Informatiebeveiliging in ziekenhuizen:

de gevaren van social engineering & het creëren van awarness

Master Thesis
Informatiekunde

Auteur:	Danny Hamelink
Afstudeerbegeleiders:	Dr. Luca Consoli & Prof. dr. ir. Theo van der Weide
Universiteit:	Radboud Universiteit Nijmegen
Afstudeernummer:	140 IK

Colofon

Auteur:	Danny Hamelink
Studentnummer:	s0624675
Opleiding:	Informatiekunde
Afstudeernummer:	140 IK
Afstudeeropdracht:	Informatiebeveiliging in ziekenhuizen: de gevaren van social engineering & het creëren van awareness.
Universiteit:	Radboud Universiteit Nijmegen Comeniuslaan 4 6525 HP Nijmegen Postbus 9102 6500 HC Nijmegen Telefoon: (024) 3616161 Fax: (024) 3564606 Internet: www.ru.nl
Faculteit:	Faculteit der Natuurwetenschappen, Wiskunde & Informatica (FNWI) Heyendaalseweg 135 6525 AJ Nijmegen Postbus 9010 6500 HC Nijmegen Telefoon: (024) 3653341 (Algemene informatie) Telefoon: (024) 3652094 (Informatica en Informatiekunde) Fax: (024) 3652888
Instituut:	Onderwijsinstituut voor Informatica en Informatiekunde
Afstudeerbegeleider:	Dr. Luca Consoli
Afstudeerbegeleider:	Prof. dr. ir. Theo van der Weide
Plaats, datum:	Nijmegen, januari 2010
Versie, status:	1.1, definitief

Voorwoord

Geachte lezer,

Voor u ligt de eindversie van mijn scriptie '*Informatiebeveiliging in ziekenhuizen: de gevaren van social engineering & het creëren van awareness*', welke het resultaat is van mijn afstudeeronderzoek ter afsluiting van de master Informatiekunde aan de Radboud Universiteit Nijmegen.

Dit afstudeeronderzoek is uitgevoerd voor het onderwijsinstituut voor Informatica en Informatiekunde, dat onderdeel is van de faculteit der Natuurwetenschappen, Wiskunde en Informatica binnen de Radboud Universiteit Nijmegen. Nu mijn studie Informatiekunde is afgerond, kan ik met veel voldoening terugkijken op deze periode. Deze scriptie is het eindresultaat van deze periode, waarin verslag wordt gedaan van mijn afstudeeronderzoek.

Graag wil ik via deze weg een aantal mensen bedanken die mij hebben geholpen en ondersteund in het uitvoeren van dit onderzoek om zo tot het gewenste resultaat te komen. Bij deze wil ik dan ook allereerst mijn twee afstudeerbegeleiders, dr. Luca Consoli en prof. dr. ir. Theo van der Weide, bedanken voor hun vakkundige begeleiding van het onderzoekstraject en voor het geven van commentaar en advies op inhoudelijke aspecten. Tevens wil ik ook graag de personen bedanken die tijd hebben vrijgemaakt om mij te woord te staan middels een interview. Zonder de inbreng van deze personen had deze scriptie niet hetzelfde resultaat kunnen hebben. Helaas kan ik in deze scriptie niet iedereen persoonlijk bedanken, vanwege de afgesproken anonimiteit, maar ik kan niets anders zeggen dan dat zonder hun hulp dit onderzoek niet tot stand zou zijn gekomen en tevens ook niet succesvol zou zijn afgerond. Hiervoor nogmaals mijn hartelijke dankbetuiging.

Dan rest mij niet veel anders meer dan u veel leesplezier toe te wensen.

Nijmegen, januari 2010

Danny Hamelink

Samenvatting (abstract)

In de informatiebeveiliging van een organisatie wordt de mens als de zwakste schakel gezien. Ondanks de technische beveiligingen is de mens achter de computer nog steeds uiterst kwetsbaar en dit komt omdat het gedrag van de mens invloed heeft op de informatiebeveiliging van een organisatie. De mens is immers eenvoudig beïnvloedbaar, door gebruik te maken van sociale en communicatieve vaardigheden. Dit wordt gezien als social engineering en is een methode dat door hackers of andere kwaadwillenden kan worden gebruikt om mensen te beïnvloeden om zo informatie te verzamelen die anders nooit zou worden prijsgegeven. Mensen hebben namelijk van nature om zich behulpzaam op te stellen, tot bijna op het naïeve af. Onbewust wordt er ingegaan op een vraag of een verzoek en wordt er iemand aangezet tot het afgeven van bedrijfsgegevens of het verrichten van bepaalde handelingen. Omdat de beveiligingstechniek bijna perfect is, kan social engineering een grote dreiging vormen voor organisaties of instellingen. Hackers of andere kwaadwillenden moeten dus andere manieren zien te vinden om aan informatie te komen en social engineering is hierin één van de betere manieren.
Bij het tegengaan van social engineering is er één belangrijk aandachtspunt: het creëren van een veiligheidsbewustzijn bij mensen dat zijzelf het grootste risico vormen in de informatiebeveiliging. Bewustwording is namelijk de maatregel tegen het voorkomen van diefstal van belangrijke informatie middels social engineering. Dit is ook het onderwerp dat centraal staat in dit afstudeeronderzoek. In dit onderzoek, dat is toegespitst op de ziekenhuizen in Nederland, is geprobeerd om vast te stellen of social engineering een gevaar vormt voor de ziekenhuizen. Ziekenhuizen werken namelijk met privacygevoelige en medische gegevens waarvan de patiënt verwacht dat er zorgvuldig mee wordt omgegaan en dat deze informatie niet aan derden wordt meegegeven of op straat komt te liggen. Daarbij is ook gekeken naar hoe het staat met het veiligheidsbewustzijn van informatiebeveiliging bij ziekenhuizen wanneer er sprake is van social engineering.

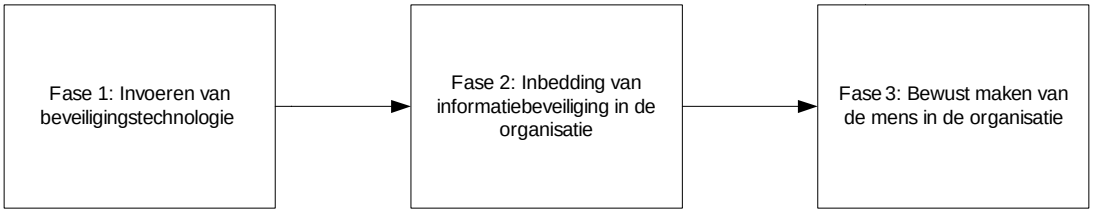
Inhoudsopgave

1. Introductie

In dit hoofdstuk zal de aanleiding en het doel van deze scriptie worden beschreven. Eerst volgt er een inleiding van dit onderzoek, gevolgd door de aanleiding en relevantie van dit onderzoek. Vervolgens wordt de probleemstelling met bijbehorende doelstelling toegelicht, die zich zal vertalen in een onderzoeksvraag met bijbehorende deelvragen. Tot slot wordt de opbouw van de scriptie beschreven door middel van een leeswijzer.

1.1 Inleiding

Informatiebeveiliging houdt zicht op en beschermt de levenscyclus van informatie, van de aanmaak en opslag van gegevens tot de distributie en het gebruik van die informatie. Medewerkers van organisaties zijn steeds vaker onderweg en maken gebruik van allerlei informatie technologische middelen zoals laptops, PDA's en het opslaan van informatie op USB-sticks. Hierdoor is het mogelijk dat derden zich toegang kunnen verschaffen tot cruciale bedrijfsinformatie. Informatiebeveiliging is daardoor een cruciaal punt in een organisatie en kan worden gespiegeld aan een drietal schakels, ook wel fases genoemd: techniek, organisatie en de mens.



Figuur 1: De levenscyclus van informatiebeveiliging

De eerste fase houdt in dat de techniek van de informatiebeveiliging wordt ingevoerd, zowel de digitale beveiliging als de fysieke beveiliging. Vandaag de dag is dit bij veel organisaties in goede handen bij de IT-afdeling. De tweede fase is het zorgen voor een goed informatie beveiligingsbeleid dat wordt uitgevoerd en nageleefd door de organisatie. De derde is de belangrijkste fase,maar tegelijkertijd ook de zwakste fase in de informatiebeveiliging van een organisatie, namelijk de mens. Ondanks de technische beveiligingen is de mens achter de computer nog steeds uiterst kwetsbaar en dit komt omdat informatiebeveiliging inspeelt op het gedrag van mensen. De mens is immers eenvoudig beïnvloedbaar, door gebruik te maken van sociale en communicatieve vaardigheden [KANT07]. Mensen hebben van nature om zich behulpzaam op te stellen, tot bijna op het naïeve af. Onbewust wordt er ingegaan op een vraag of een verzoek en wordt er iemand aangezet tot het afgeven van bedrijfsgegevens of het verrichten van bepaalde handelingen.

Een belangrijke bedreiging voor een organisatie is het begrip identiteitsfraude. Bijna alle bedrijven werken met informatie die persoonlijk van aard is en waarvan men niet wil dat deze informatie in de verkeerde handen valt. Diefstal van gegevens kan langs tal van wegen maar één van de beste manieren om aan cruciale gegevens te komen is via social engineering.

Social engineering kan in het kort worden omschreven als het verkrijgen van informatie door het menselijke aspect van beveiliging te gebruiken. De mens is de schakel in de beveiliging om aan informatie te komen en wordt veelvuldig misbruikt om mensen informatie afhandig te maken. Er is geen firewall of een beleid dat een aanval van social engineering kan herkennen omdat simpelweg het stellen van vragen niet verboden is en mensen nu eenmaal geneigd zijn antwoorden op vragen te geven. Omdat de beveiligingstechniek bijna perfect is, is social engineering nog nooit zo dreigend geweest als op dit moment. Hackers moeten dus andere manieren zien te vinden om aan informatie te komen en social engineering is hierin één van de betere manieren.

Om social engineering of andere methoden om diefstal in het kader van identiteitsfraude te voorkomen is er één belangrijk aandachtspunt: het creëren van een besef bij mensen dat zijzelf het grootste risico vormen in de informatiebeveiliging. Bewustwording is namelijk de maatregel tegen het voorkomen van diefstal van belangrijke gegevens zoals bijvoorbeeld voor identiteitsfraude. Mensen moeten bewust zijn van de risico's en weten hoe om te gaan met informatie en vooral de beveiliging van deze informatie [KOOT05].

1.2 Aanleiding van het onderzoek

Er zijn een drietal aanleidingen die ten grondslag liggen aan het uitvoeren van dit onderzoek.

- Binnen de zorgsector is informatie van essentieel belang en er wordt meer en meer gebruik gemaakt van technologie. Laptops en handheld computers worden steeds meer de standaard en heeft als voordeel dat er direct toegang is tot een enorme hoeveelheid informatie. De keerzijde is dat er meer uitdagingen zijn op het gebied van informatiebeveiliging. Personeel, specialisten of andere medewerkers houden zich vaak bewust of onbewust niet aan de beveiligingsvoorschriften en brengen hiermee vertrouwelijke informatie in gevaar [MEDI09]. Hackers of andere kwaadwillenden kunnen hier van profiteren en proberen toegang te krijgen tot deze vertrouwelijke en gevoelige informatie.

- Er is al op vele manieren onderzoek gedaan door verschillende auteurs naar het fenomeen social engineering. Deze onderzoeken richten zich voornamelijk op een begripsbepaling van social engineering en hoe hackers social engineering aanvallen inzetten om aan informatie te komen. Waar in de verschillende onderzoeken niet de nadruk op wordt gelegd is de andere kant van het verhaal, namelijk of social engineering een gevaar kan vormen voor specifieke organisaties of instellingen.

- De derde aanleiding is voornamelijk een persoonlijke aanleiding. Het intrigeert mij hoe makkelijk mensen om de tuin kunnen worden geleid en voor iemand anders hun karretje kunnen worden gespannen. Er zal een bewustwording moeten worden gecreëerd en mensen moet beginnen in te zien dat zij het grootste gevaar vormen in de informatiebeveiliging.

1.3 Relevantie van het onderzoek

Het digitaal vastleggen, raadplegen en uitwisselen van privacygevoelige, medische gegevens is bij zorginstellingen zoals ziekenhuizen sterk toegenomen, zoals bijvoorbeeld in het elektronisch patiëntendossier (EPD). Deze digitalisering brengt uiteraard nieuwe beveiligingsvraagstukken met zich mee en specifieke normen moeten zorginstellingen ondersteunen bij het risicoloos omgaan met digitale informatie. Aandachtspunt hierbij is het risicobewustzijn binnen de zorginstellingen dat sterk verbeterd dient te worden [CBP08]. Hackers maken meer en meer gebruik van social engineering aanvallen dan dat ze gebruik maken van technische aanvallen zoals bijvoorbeeld virussen. Dit komt omdat bij veel bedrijven en zorginstellingen de technische maatregelen uitstekend in orde zijn en hierdoor de hacker gedwongen is om zijn heil te zoeken in psychologische trucjes om aan informatie te komen. De mens vormt hierin de belangrijkste schakel omdat mensen simpelweg eenvoudig beïnvloedbaar zijn. Het EPD kan daardoor een ideale bron zijn om aan vertrouwelijke en gevoelige informatie te komen.

In Amerika blijkt dat informatiebeveiliging binnen de zorgsector ook nog sterk voor verbetering vastbaar is [HERZ10]. De Electronic Medical Records (EMR), in Nederland is dit het EPD, zijn vandaag de dag voor hackers interessanter om aan informatie te komen dan bijvoorbeeld credit cards. Credit cards waren vroeger voor hackers een ideale manier om informatie van personen te verzamelen om op deze manier gebruik te kunnen maken van identiteitsfraude. Maatregelen hiertegen hebben dit doen afnemen en is de focus verlegd naar de EMR. Een EMR bevat een identiteit met medische informatie en dankzij de digitalisering en de langzame toepassing van processen en technologie om deze informatie te beschermen, is een EMR voor hackers een goede bron om aan informatie voor bijvoorbeeld identiteitsfraude te komen [BAIL10].

1.4 De probleemstelling en doelstelling

Probleemstelling

Social engineering is een onderwerp waar al de nodige artikelen over zijn geschreven. Er zijn verschillende tools voor hackers om op een doordachte manier aan gegevens te komen om zo voor persoonlijk gewin te gebruiken. Veel organisaties en instellingen hebben allerlei regelgevingen opgesteld in de vorm van gedragscodes omtrent informatiebeveiliging en de omgang hiermee. Uit een onderzoek in 2008 is gebleken dat Nederlandse bedrijven en dan met name de medewerkers van die bedrijven, laks omgaan met belangrijke en vertrouwelijke informatie van de organisatie zelf en tevens ook met bescherming van persoonlijke gegevens van klanten [FELLO08]. De uitkomst uit dit onderzoek is dat werknemers hier zelf verantwoordelijk voor zijn. Zo worden er bijvoorbeeld fraudegevoelige documenten zomaar in de prullenbak gegooid, zonder deze eerst te vernietigen. Bij veel bedrijven lijkt het er dus op dat medewerkers zicht niet bewust zijn van een goede informatiebeveiliging en dat zijzelf hierin vaak de zwakste schakel zijn. Medewerkers denken dat dit hen toch niet zal overkomen en dat vertrouwelijke informatie niet kan worden gestolen uit de prullenbakken en afvalcontainers van organisaties.

Dit is ook het geval bij ziekenhuizen, waar de informatiebeveiliging niet aan de gewenste norm voldoet. Dit kwam aan het licht in een onderzoek [CBP08] dat in 2008 uitgevoerd is door het College bescherming persoonsgegevens en de Inspectie voor de gezondheidszorg naar de informatiebeveiliging in ziekenhuizen. Het besef dat informatiebeveiliging staat of valt met de organisatie van de informatiebeveiliging en het gedrag van medewerkers, leek in de meeste ziekenhuizen niet voldoende aanwezig. De conclusie was dat veel ziekenhuizen niet voldeden aan de NEN 7510 norm, de informatie beveiligingsnorm voor de zorgsector. Ziekenhuizen werken met allerlei gevoelige en vertrouwelijke informatie en er mag verwacht worden dat zij tegenover haar patiënten verantwoordelijk met deze informatie omgaat. Ook is in dit onderzoek naar voren gekomen dat de onderzochte ziekenhuizen zich niet voldoende bewust zijn van de risico's van social engineering en in sommige gevallen was men zelfs geheel onbekend met het begrip social engineering.

Doelstelling

De doelstelling van dit onderzoek is om vast te stellen of ziekenhuizen een gevaar lopen wanneer het te maken krijgt met social engineering en hoe het gesteld is met het veiligheidsbewustzijn ten opzichte van informatiebeveiliging en de gevaren van social engineering in ziekenhuizen. Hackers die zich bezighouden met social engineering zijn zeer inventief in het vinden van nieuwe ideeën om aan belangrijke en vertrouwelijke informatie van ziekenhuizen te komen. De vraag is of ziekenhuizen zich er van bewust zijn dat zij een potentieel doelwit vormen voor hackers of andere kwaadwillenden om via social engineering aanvallen dit te bewerkstelligen. De uitkomst van dit onderzoek zal aantonen in hoeverre social engineering een gevaar voor een ziekenhuis vormt en of ziekenhuizen een veiligheidsbewustzijn hebben voor de informatiebeveiliging van het ziekenhuis wanneer er sprake is van social engineering. Tevens zal duidelijk moeten worden of ziekenhuizen beschermd zijn tegen social engineering, wat ze er tegen kunnen doen en hoe social engineering kan worden voorkomen.

Onderzoeksvraag

Kan social engineering een gevaar voor een ziekenhuis vormen, hoe is het gesteld met het veiligheidsbewustzijn van informatiebeveiliging bij ziekenhuizen wanneer er sprake is van social engineering en hoe kan dit veiligheidsbewustzijn worden versterkt?

De deelvragen om de onderzoeksvraag te kunnen beantwoorden zijn:

1. Wat wordt er verstaan onder het begrip informatiebeveiliging en wat is de rol van de mens hierin?
2. Wat wordt er bedoeld met social engineering, welke aanvallen zijn er en hoe kunnen deze worden herkend en tegengegaan?
3. Wat word er verstaan onder het begrip veiligheidsbewustzijn?
4. Welke factoren spelen een rol in het hebben en creëren van een veiligheidsbewustzijn?
5. Is er sprake van een veiligheidsbewustzijn ten opzichte van informatiebeveiliging en social engineering bij ziekenhuizen en wat doet het ziekenhuis om het veiligheidsbewustzijn van medewerkers te vergroten?
6. Zijn ziekenhuizen zich bewust van de gevaren van social engineering en zijn ziekenhuizen bestand tegen de verschillende soorten aanvallen van social engineering?

1.5 Methode

De hoofdvraag zal beantwoord worden met behulp van de 6 opgestelde deelvragen. De deelvragen worden in deze paragraaf uiteengezet in een onderzoeksdoel, een deelproduct en de gebruikte methode.

Deelvraag 1

1. Wat wordt er verstaan onder het begrip informatiebeveiliging en wat is de rol van de mens hierin?

Deelvraag 1	
Onderzoeksdoel	Het doel van deze deelvraag is om duidelijkheid te krijgen over het begrip informatiebeveiliging. Er moet een duidelijke formulering zijn van dit begrip om misverstanden te voorkomen. Ook moet de rol van de mens hierin duidelijk zijn. Zij zijn de belangrijkste maar tevens ook de zwakste schakel in de informatiebeveiliging.
Deelproduct	Het deelproduct zal een begripsbepaling zijn van het onderwerp veiligheidsbewustzijn. Tevens zal dit resulteren in een overzicht wat de rol van de mens hierin is.
Methode	Om tot een begripsbepaling en de informatie te komen, is er gebruikt gemaakt van een literatuurstudie. Door middel van aanwezige artikelen en literatuur is er achterhaald hoe de verhouding tussen mens en informatiebeveiliging is en hoe de mens de informatiebeveiliging in gevaar kan brengen.

Tabel 1: Onderzoeksdoel, deelproduct en methode van deelvraag 1

Deelvraag 2

2. Wat wordt er bedoeld met social engineering, welke aanvallen zijn er en hoe kunnen deze worden herkend en tegengegaan?

Deelvraag 2	
Onderzoeksdoel	De tweede deelvraag heeft als doel om een begripsbepaling te geven van social engineering om zo duidelijkheid te scheppen over wat social engineering nu precies inhoudt voor mensen die hier nog nooit van gehoord hebben. Het tweede doel is om duidelijkheid te krijgen van social engineering aanvallen die hackers gebruiken om zo in kaart te brengen hoe men zich het best kan wapenen tegen deze aanvallen.
Deelproduct	Het deelproduct is een begripsbepaling van social engineering en een overzicht van social engineeringaanvallen die in de praktijk zijn voorgekomen. Ook moet duidelijk worden welke maatregelen genomen moeten worden om social engineering aanvallen tegen te gaan.
Methode	De begripsbepaling van social engineering vond plaats door middel van een literatuurstudie. Literatuur en case studies uit de praktijk hebben ervoor gezorgd dat social engineering aanvallen achterhaald en beschreven zijn.

Tabel 2: Onderzoeksdoel, deelproduct en methode van deelvraag 2

Deelvraag 3 & 4

3. Wat word er verstaan onder het begrip veiligheidsbewustzijn?
4. Welke factoren spelen een rol in het hebben en creëren van een veiligheidsbewustzijn en hoe kan dit bewustzijn worden versterkt?

Deelvraag 3 & 4	
Onderzoeksdoel	Deze twee deelvragen hebben als doel om een begripsbepaling te geven van veiligheidsbewustzijn en welke factoren van invloed zijn op het creëren van een veiligheidsbewustzijn en het versterken van het bewustzijn. Duidelijk moet worden in hoeverre deze factoren van invloed zijn, op welke manieren en in welke mate.
Deelproduct	Dit deelproduct resulteert in een beschrijving van het begrip veiligheidsbewustzijn met daarbij de mogelijke factoren die invloed hebben op het creëren van een veiligheidsbewustzijn. Ook worden de methoden weergegeven die er zijn in hoe een bewustzijn versterkt kan worden.
Methode	De methode die gebruikt is, is een literatuurstudie, samen met case studies uit de praktijk. Hieruit is afgeleid welke factoren een rol spelen in het creëren van een veiligheidsbewustzijn.

Tabel 3: Onderzoeksdoel, deelproduct en methode van deelvragen 3 & 4

Deelvraag 5 & 6

5. Is er sprake van een veiligheidsbewustzijn ten opzichte van informatiebeveiliging en social engineering en wat doet het ziekenhuis aan het veiligheidsbewustzijn van medewerkers?
6. Zijn ziekenhuizen zich bewust van de gevaren van social engineering en zijn ziekenhuizen bestand tegen de verschillende soorten aanvallen van social engineering ?

Deelvraag 5 & 6	
Onderzoeksdoel	Het doel van deze twee laatste deelvragen is om te onderzoeken op welke manieren ziekenhuizen omgaan met het informatie beveiligingsbeleid van het ziekenhuis en hoe dit wordt nageleefd door de andere medewerkers. Tevens zal moeten blijken in welke mate er een bewustzijn is van de gevaren van social engineering en of social engineering een gevaar kan zijn voor een ziekenhuis.
Deelproduct	Dit deelproduct resulteert in een inzicht dat zal aangeven hoe bewust een ziekenhuizen omgaan met informatiebeveiliging en de gevaren van social engineering. Het geeft een beeld weer dat zal aantonen of ziekenhuizen een doelwit kunnen zijn voor hackers om via social engineering aan informatie te komen.
Methode	De methode die gebruikt hiervoor gebruikt is, is een empirisch onderzoek door middel van semi-gestructureerde interviews met open vragen. In totaal zijn vijf experts op het gebied van informatiebeveiliging van vijf verschillende ziekenhuizen geïnterviewd.

Tabel 4: Onderzoeksdoel, deelproduct en methode van deelvragen 5 & 6

1.6 Leeswijzer

De inhoud van deze scriptie kan worden verdeeld in een tweetal delen: een theoretisch gedeelte en een empirisch gedeelte. Het theoretische gedeelte omvat de hoofdstukken 2, 3 en 4. Het empirische gedeelte, de interviews, staat beschreven in hoofdstuk 5. In de tabel op de volgende pagina staat een overzicht van de verschillende hoofdstukken die in deze scriptie voorkomen.

Theoretische gedeelte	Hoofdstuk 1	In het eerste hoofdstuk wordt de aanleiding, relevantie en de probleemstelling en doelstelling van het onderzoek beschreven. Dit resulteert in een onderzoeksvraag met bijbehorende deelvragen. Tot slot wordt de gehanteerde methode beschreven.
	Hoofdstuk 2	In hoofdstuk 2 komt het begrip informatiebeveiliging aan bod en wordt er tevens kort ingegaan op informatiebeveiliging in de zorg en wat de rol van de mens in informatiebeveiliging is.
	Hoofdstuk 3	Hoofdstuk 3 gaat over het onderwerp social engineering. In dit hoofdstuk zal social engineering ruim aan bod komen en zullen alle aspecten die bij social engineering komen kijken, worden besproken.
	Hoofdstuk 4	Hoofdstuk 4 beschrijft het begrip informatiebeveiliging awareness en word tevens ook besproken hoe een goed en effectief informatiebeveiliging awareness programma eruit hoort te zien.
Empirisch gedeelte	Hoofdstuk 5	Hoofdstuk 5 beslaat het empirische gedeelte van dit onderzoek. In dit hoofdstuk worden de gehouden interviews besproken en geanalyseerd aan de hand van de theorie uit de hoofdstukken 2, 3 en 4. Tot slot volgt er een conclusie met aanbevelingen.
	Hoofdstuk 6	In hoofdstuk 6 worden de deelvragen en de onderzoeksvraag beantwoordt.

Tabel 5: Leeswijzer van deze scriptie

Opmerking vooraf

In deze scriptie komen de begrippen informatiebeveiliging awareness, awareness, veiligheidsbewustzijn en bewustzijn voor. In het kader van deze scriptie worden met deze begrippen hetzelfde bedoeld: het creëren van een awareness (bewustzijn) in de informatiebeveiliging.

2. Informatiebeveiliging en de rol van de mens

In dit hoofdstuk wordt uiteengezet wat informatiebeveiliging precies is, welke aspecten hierbij van belang zijn, wordt er kort ingegaan op informatiebeveiliging in zorginstellingen en hoe het menselijk aspect kan worden gerelateerd aan informatiebeveiliging.

2.1 Waarom Informatiebeveiliging

Informatiebeveiliging is tegenwoordig voor ieder bedrijf, instelling, instituut of onderneming van essentieel belang om waardevolle informatie te beschermen en de continuïteit te waarborgen. De beschikbaarheid van informatie en informatiesystemen is voor veel ondernemingen een belangrijke succesfactor geworden. Informatie- en communicatietechnologie neemt daardoor een steeds strategischere rol in binnen organisaties [CAPG02].
Zo ook binnen de zorgsector en met name binnen ziekenhuizen, waar in deze thesis het onderzoek zich op zal richten. De kwaliteit van dienstverlening in de zorgsector is een zaak van groot belang, soms zelfs van levensbelang. Om patiënten het gewenste niveau van dienstverlening te kunnen bieden, is het noodzakelijk dat zorgverleners op ieder moment over betrouwbare informatie kunnen beschikken. Tegelijkertijd is het van belang dat gevoelige informatie niet in handen van ongeautoriseerde partijen valt om de privacy van de patiënt te beschermen [NEN7510]. Het goed beveiligen van deze informatie heeft dus een hoge prioriteit.

2.2 Een begripsbepaling van informatiebeveiliging

Er bestaan talloze definities van het begrip informatiebeveiliging. In de Code voor Informatiebeveiliging (CvIB), en dan met name in het ISO 27001 certificaat wordt informatiebeveiliging als volgt omschreven:

> *Informatiebeveiliging wordt gedefinieerd als het waarborgen van*
>
> - *Beschikbaarheid: geautoriseerde gebruikers hebben op de juiste momenten toegang tot informatie en aanverwante bedrijfsmiddelen;*
> - *Integriteit: correctheid en volledigheid van informatie en de informatieverwerking;*
> - *Vertrouwelijkheid: informatie is alleen toegankelijk voor degenen die hiervoor zijn geautoriseerd.*

In het Besluit voorschrift informatiebeveiliging van de Rijksdienst wordt informatiebeveiliging als volgt gedefinieerd:

> *Het proces van het vaststellen van de vereiste betrouwbaarheid van informatiesystemen in termen van vertrouwelijkheid, beschikbaarheid en integriteit alsmede het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen.*

Zo zijn er nog vele verschillende definities die op details verschillen. Wat in iedere definitie terugkomt, zijn de termen beschikbaarheid, integriteit en vertrouwelijkheid. Zij zorgen voor de betrouwbaarheid van de informatie binnen het vakgebied van de informatiebeveiliging en worden ook wel de betrouwbaarheidsaspecten genoemd.

Beschikbaarheid (Availability)	Waarborgen dat geautoriseerde gebruikers op de juiste momenten tijdig toegang hebben tot informatie en aanverwante bedrijfsmiddelen.
Integriteit (Integrity)	Het waarborgen van de correctheid en de volledigheid van informatie en verwerking
Vertrouwelijkheid (Confidentiality)	Waarborgen dat informatie alleen toegankelijk is voor degenen die hiertoe geautoriseerd zijn

Tabel 6: De betrouwbaarheidsaspecten van informatiebeveiliging

Deze aspecten zijn vooral bekend onder de Engelse afkorting CIA: confidentiality, integrity en availability.

Naast de bovenstaande drie aspecten zijn er nog een drietal beveiligingsproblemen die met informatiebeveiliging verbonden zijn.

Geheimhouding (Secrecy)	Informatie uit handen van onbevoegde gebruikers houden
Authenticatie (Authentication)	Bepalen met wie je spreekt alvorens vertrouwelijke informatie te zenden of een zakelijke transactie af te sluiten
Niet-loochening (Non-repudiation)	Het belang om achteraf toegang en transacties te kunnen verifiëren

Tabel 7: Extra betrouwbaarheidsaspecten van informatiebeveiliging

In de verschillende definities van informatiebeveiliging die er zijn, worden deze drie aspecten niet opgenomen omdat geheimhouding en authenticatie vaak worden gezien als vertrouwelijkheid en niet-loochening als integriteit [TANE03].

Een goede en naar mijns inziens volledige definitie van informatiebeveiliging luidt als volgt:

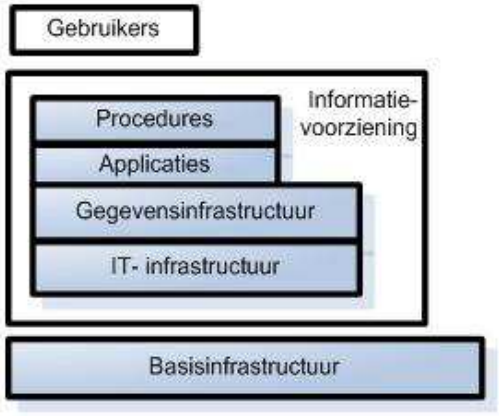
Informatiebeveiliging is het proces van het vaststellen van de vereiste beveiligingsrichtlijnen , maatregelen en procedures (zowel technisch als niet-technisch) met betrekking tot informatie en informatievoorziening ter waarborging van de vertrouwelijkheid , integriteit en beschikbaarheid van de informatievoorziening

Informatievoorziening [OVER07] wordt omschreven als:

> *Het geheel van IT-infrastructuur , gegevensinfrastructuur , applicaties en organisaties , dat tot doel heeft om te voorzien in de informatiebehoefte van de processen van een organisatie . De informatievoorziening kan ook beschouwd worden als de verzameling informatiesystemen van een organisatie*

.

Informatievoorziening (zie ook figuur 2) is het geheel van activiteiten dat voor een bedrijf moet worden uitgevoerd om iedereen de informatie te verstrekken die nodig is om toegewezen functies te vervullen. De basisinfrastructuur (gebouwen, elektriciteitsvoorziening) en gebruikersprocedures maken geen deel uit van de informatievoorziening maar zijn wel noodzakelijk voor het functioneren van de informatievoorziening [LOOI04].

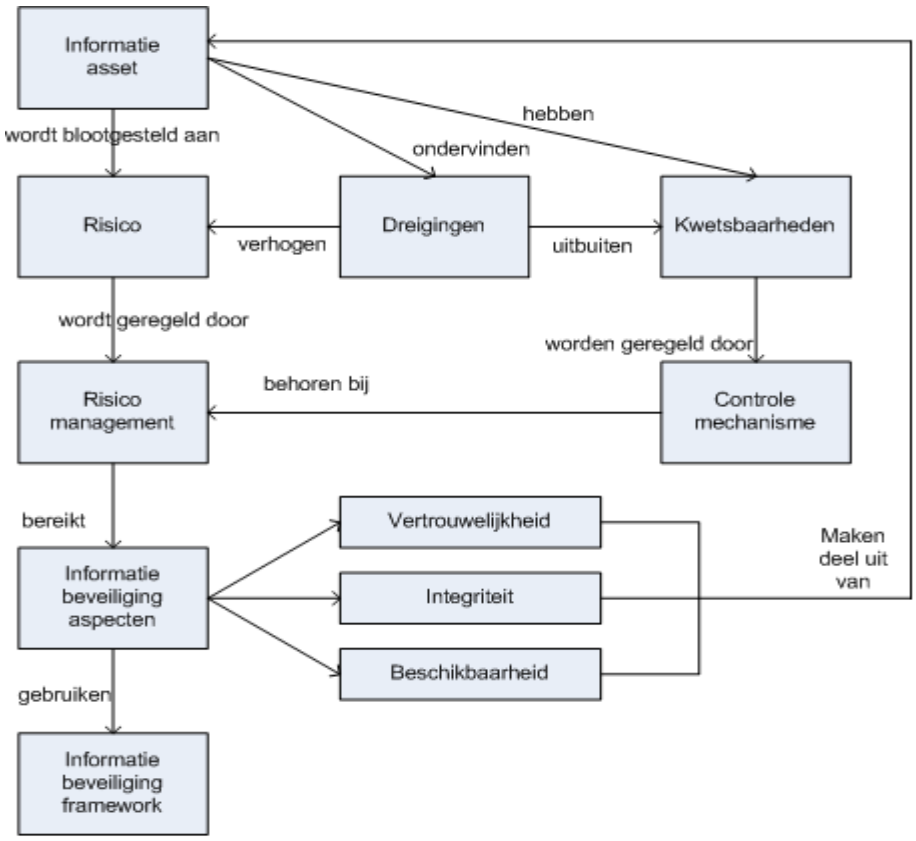


Figuur 2:De componenten van informatievoorziening

Vaak wordt bij informatiebeveiliging alleen aandacht geschonken aan technische maatregelen zoals virusscanners en firewalls. Veel organisaties zien onder andere virussen, hackers en spyware als de grootste bedreiging voor de organisatie omdat deze technisch van aard zijn en hierdoor de nadruk vooral op de technische maatregelen ligt. De technische maatregelen zijn dan ook bij de meeste organisaties goed geregeld omdat men bewust is van de gevaren. Echter omvat de informatiebeveiliging meer dan enkel de technische maatregelen. Zaken als het beleid van de organisatie, de fysieke beveiliging en medewerkers spelen een voorname rol in de informatiebeveiliging maar worden door veel organisaties en instellingen vaak niet als zodanig erkend.

2.2.1 Informatiebeveiligingsframework

Hoe informatiebeveiliging te werk gaat, kan schematisch worden weergegeven in het framework op de volgende pagina



Figuur 3: Het informatiebeveiligingsframework (Bron: Course Security in Organisations van P. van Rossum)

Een informatie asset dat moet voldoen aan de informatie beveiligingsaspecten kan worden blootgesteld aan een bepaald risico. Deze asset kan een bepaalde kwetsbaarheid hebben en last hebben van één of enkele dreigingen. Deze dreigingen verhogen het risico die de asset loopt door de kwetsbaarheden van diezelfde asset uit te buiten. De kwetsbaarheden worden geregeld door de opgestelde controle mechanismen die bij het risico management horen om zo de risico's te elimineren. In het framework op de volgende pagina komen de volgende begrippen aan bod:

Informatie asset	(een stuk) waardevolle informatie of infrastructuur.
Kwetsbaarheid	De zwakheid van een informatie asset dat kan worden uitgebuit door één of meerdere dreigingen.
Dreiging	Een manier om een kwetsbaarheid uit te buiten.
Controle mechanisme	Technisch, organisatorisch of rechtsgeldig mechanisme om toegang te regelen.
Risico	De mogelijkheid van verlies van een informatie asset.
Risico management	Het identificeren van risico's en het vaststellen van beheersmaatregelen.

Tabel 8: Begrippen van informatiebeveiliging

2.2.2. Informatiebeveiliging: bedreigingen & maatregelingen

Bij informatiebeveiliging zijn de begrippen bedreiging, kwetsbaarheid en risico van groot belang. De betrouwbaarheid van informatie is niet iets dat uit zichzelf ontstaat en de informatievoorziening staat onder constante druk van potentiële bedreigingen. Deze bedreigingen kunnen de betrouwbaarheid en de betrouwbaarheidsaspecten sterk in twijfel trekken. In hoeverre de informatievoorziening gevoelig is voor bedreigingen, hangt samen met de kwetsbaarheid van de informatievoorziening van een bepaalde bedreiging.

Een bedreiging is een proces of een gebeurtenis dat de kwetsbaarheid van een informatievoorziening (of een asset) kan uitbuiten. Bedreigingen kunnen worden onderverdeeld in menselijke dreigingen en niet-menselijke dreigingen [PVIB08]. Menselijke bedreigingen kunnen weer worden opgesplitst in opzettelijke en onopzettelijke dreigingen. Mensen kunnen opzettelijke schade toebrengen aan een informatievoorziening van een organisatie of instelling door verschillende redenen. Meestal heeft het te maken met oorzaken van buitenaf (misbruik en criminaliteit) zoals diefstal, inbraak en hacking. Ook sabotage is een vaak voorkomende dreiging, bijvoorbeeld een medewerker die ontslagen wordt en als wraak data vernietigd of steelt. Er kan ook schade worden toegebracht door onopzettelijk foutief handelen door gebruikers, beheerders of gasten. Hier kan dan bijvoorbeeld worden gedacht aan een USB-stick waarop onbedoeld een virus staat en die vervolgens in een computer wordt gestopt en zodoende het netwerk wordt geïnfecteerd. Er zijn ook niet-menselijke bedreigingen wat vaak invloeden van buitenaf zijn zoals een aardbeving, blikseminslag, waterschade of stormschade.

In [OVER07] wordt een overzicht gegeven van algemene type bedreigingen bij de drie betrouwbaarheidsaspecten:

Aspect	Kenmerk	Bedreiging	Voorbeeld van bedreiging
Beschikbaarheid	Tijdigheid	Vertraging	Overbelasting van infrastructuur
	Continuïteit	Uitval	Defect in infrastructuur
Integriteit	Correctheid	Wijziging	Ongeautoriseerd wijzigen van gegevens
	Volledigheid	Verwijdering Toevoeging	Ongeautoriseerd wissen van gegevens Ongeautoriseerd toevoegen van gegevens
	Geldigheid	Veroudering	Gegevens niet up-to-date houden
	Authenticiteit	Vervalsing	Frauduleuze transactie
	Onweerlegbaarheid	Verloochening	Ontkennen bepaald bericht gestuurd te hebben
Vertrouwelijkheid	Exclusiviteit	Onthulling Misbruik	Afluisteren van netwerk; hacking privé gebruik

Tabel 9: Aspecten en kenmerken van betrouwbaarheid en daaraan gerelateerde bedreigingen

Bij het aspect beschikbaarheid zijn de bedreigingen vooral de vertraging bij en uitval van informatiesystemen waardoor informatie niet meer tijdig en op het juiste moment beschikbaar is. Het aspect integriteit heeft vooral te maken met bedreigen die te maken hebben met de correctheid en volledigheid van informatie. Informatie behoort altijd correct en volledig te zijn ingevoerd. Wanneer dit niet het geval is, komt de integriteit van informatie in gevaar en kunnen er voor organisaties vervelende situaties ontstaan. Het aspect vertrouwelijkheid heeft als grootste bedreigingen vooral misbruik van informatie en het niet juist omgaan met informatie. Deze bedreigingen ontstaan vooral wanneer er niet vertrouwelijk door de bevoegde personen met informatie wordt omgegaan.

Door het treffen van beveiligingsmaatregelen is het mogelijk om de bedreigingen te verminderen. Een manier om beveiligingsmaatregelen in te delen is op de manier waarop ze gerealiseerd worden [OVER07]:

- Organisatorische maatregelen;
- Logische maatregelen;
- Fysieke maatregelen.

Organisatorische maatregelen zijn maatregelen die betrekking hebben op de organisatie als geheel, zoals het beveiligingsbeleid, richtlijnen en procedures. Enkele voorbeelden van organisatorische maatregelingen zijn: opleiding en voorlichting om het beveiligingsbewustzijn (awareness) te verbeteren en een portier bij de hoofdingang om de toegang te bewaken.

Logische maatregelen zijn maatregelen die geprogrammeerd zijn in programmatuur. Voorbeelden zijn login- en wachtwoordauthenticatie en digitale handtekeningen in elektronische post.

Fysieke maatregelen zijn maatregelen die gebaseerd zijn op apparatuur of andere materiële zaken. Voorbeelden zijn noodstroomvoorzieningen en sloten tegen ongewenste toegang.

De informatiebeveiliging richt zich op de aspecten beschikbaarheid, integriteit en vertrouwelijkheid. Elke beveiligingsmaatregel richt zich dus op één of meerdere van deze aspecten. Organisatorische maatregelen richten zich op beschikbaarheid en vertrouwelijkheid, logische maatregelen richten zich op integriteit en vertrouwelijkheid, en fysieke maatregelen hebben de focus op beschikbaarheid en vertrouwelijkheid.

2.3 Belangrijke aspecten van informatiebeveiliging

In een artikel van Basie von Solms en Rossouw von Solms [SOLM04] worden de tien belangrijkste aspecten van informatiebeveiliging uiteengezet. Deze tien aspecten zijn van essentieel belang wanneer een organisatie een plan voor informatiebeveiliging implementeert. Deze aspecten gelden ook voor een bestaand plan wanneer blijkt dat er problemen zijn bij de uitvoering van dit plan en de effectiviteit die hierbij komt kijken. Wanneer één van deze aspecten wordt genegeerd of niet naar behoren wordt uitgevoerd, kan dit voor serieuze problemen zorgen in een organisatie met betrekking tot de veiligheid van informatie. Het betreft de volgende tien aspecten:

1. **De verantwoordelijkheid van informatiebeveiliging ligt bij het bestuur van de organisatie.**

   Informatiebeveiliging is een belangrijk onderdeel geworden van het topmanagement van een organisatie. Bij hen ligt de verantwoordelijkheid om ervoor te zorgen dat alle informatie assets veilig zijn en dat er maatregelen zijn genomen om deze veiligheid te waarborgen.

2. **De bescherming van informatie is een organisatorische kwestie en niet een technische kwestie.**

   Problemen die gerelateerd zijn aan informatiebeveiliging kunnen niet alleen door technische middelen worden opgelost. Bij veel organisaties komt het nog voor dat het management denkt dat alleen technologie nodig is om problemen op te lossen en daardoor deze zaken laat afhandelen door de technische afdeling. Zonder de juiste ondersteuning van het management op organisatorisch gebied, worden de informatie beveiligingsproblemen niet goed afgehandeld en zullen dus blijven terugkomen

3. **Informatiebeveiliging is een mutidimensionele discipline.**

   Informatiebeveiliging is een multi dimensionele discipline, waarbij alle dimensies in acht moeten worden genomen om een veilige omgeving te creëren voor de informatie assets van een organisatie. Enkele dimensies die van belang zijn: Organisatorische dimensie, ethische dimensie, awareness dimensie, technische dimensie en personeelsdimensie.
   De meeste van deze dimensies zijn van een niet technische aard, wat dus relateert aan het tweede aspect. Al deze dimensies moeten in acht worden genomen bij het creëren en ontwikkelen van een informatiebeveiligingsplan omdat geen enkele dimensie op zijn eigen een geschikte oplossing zal vormen.

4. **Een informatiebeveiligingsplan moet worden gebaseerd op het identificeren van risico's.**

   Het doel van informatiebeveiliging is om middelen te verzorgen die de risico's verminderen die geassocieerd zijn met de informatie resources van de organisatie. Wanneer het voor organisaties niet duidelijk is wat precies de potentiële gevaren zijn, wordt er geld uitgegeven aan dreigingen die misschien niet vaak zullen voorkomen en worden daardoor dreigingen genegeerd die een grotere impact op de organisatie kunnen hebben wanneer deze dreigingen voorkomen. Het is daarom essentieel dat een organisatie een risicoanalyse moet hebben in het beveiligingsbeleid.

5. **Internationale best practices spelen een belangrijke rol in de informatiebeveiliging.**

   Een groot aantal dreigingen voor de beveiliging van informatie, de risico's die dit met zich meebrengen en de maatregelen tegen deze dreigingen zijn vaak allemaal hetzelfde voor alle organisaties. Wanneer organisaties hun ervaringen op dit gebied hebben gedocumenteerd, kunnen deze gedocumenteerde ervaringen door andere organisaties worden gebruikt. Waarom iets doen wat anderen al gedaan hebben? Deze ervaringen kunnen worden toegepast en er kan veel van worden geleerd.

6. **Een informatie beveiligingsbeleid is essentieel.**

   Een juist informatie beveiligingsbeleid is de basis voor elk succesvol informatie beveiligingsplan. Een dergelijk beleid is het startpunt waarop alle andere standaarden en procedures moeten worden gebaseerd. Ook moet een informatie beveiligingsbeleid kort (3, 4 pagina's) en ondertekend zijn door de CEO, zodat duidelijk is dat het management achter alle informatie beveiligingsaspecten staat. Dit is de meest zichtbare manier waarop het management hun ondersteuning laten zien tegenover informatiebeveiliging in de organisatie.

7. **Naleving en controle van informatiebeveiliging is essentieel.**

   Het heeft geen nut om een informatie beveiligingsbeleid te hebben, als het niet mogelijk is om naleving en controle te hebben op het beleid. Iedere informatie beveiligingsmanager moet via technische en niet-technische middelen het informatie beveiligingsbeleid kunnen controleren en naleven

8. **Een juiste structuur voor de informatiebeveiliging is essentieel.**

   Een organisatie moet een geschikte structuur voor informatiebeveiliging hebben om een informatie beveiligingsplan succesvol te kunnen maken. Een dergelijke structuur heeft te maken met de manier waarop informatiebeveiliging is georganiseerd en gestructureerd in een organisatie.

9. **De belangrijkheid van informatiebeveiliging awareness onder gebruikers.**

   Wanneer er geen awareness programma bestaat, zullen medewerkers minder bewust zijn van de gevaren die de organisatie ondervindt en de schade die het daardoor zal krijgen. Medewerkers kunnen daardoor ook minder snel verantwoordelijk worden gehouden voor problemen, wanneer ze niet weten wat de problemen precies zijn en wat ze moeten doen om de problemen tegen te gaan.

10. **Ervoor zorgen dat informatiebeveiliging managers hun verantwoordelijkheden kunnen uitvoeren door ze de juiste infrastructuur en middelen aan te bieden.**

    Vaak wordt een informatiebeveiliging manager aangesteld waarvan verwacht wordt dat deze persoon alles alleen uitvoert en oplost. Dit is niet mogelijk vanwege de complexiteit en de multi-dimensionele aard van informatiebeveiliging. Wanneer informatiebeveiliging managers realiseren dat ze hun werk niet voldoende kunnen uitvoeren, wordt de organisatie aan diverse dreigingen blootgesteld omdat het beveiligingsplan niet naar behoren wordt uitgevoerd.

Het creëren van een geschikt informatie beveiligingsprogramma heeft vaak te maken met het gebruiken van het gezonde verstand. Helaas wordt dit vaak hevig onderschat en genegeerd omdat niet gerealiseerd wordt hoe essentieel deze aspecten zijn.

2.4 Informatiebeveiliging in zorginstellingen

In de zorgsector draait het vooral om het verlenen van zorg, maar gaat er tevens veel informatie in deze sector om. In de meeste gevallen gaat het om vertrouwelijke informatie die bovendien correct, op het juiste moment en op de juiste plek beschikbaar moet zijn. Hoewel de behoefte aan informatie uitwisseling in de zorgsector groeit (denk aan de verschillende zorgverleners en verschillende locaties), gaat de beveiliging van informatie vaak hierin niet mee. De digitalisering van patiënten gegevens neemt een grote vlucht (Elektronisch Patiënten Dossier) waardoor de informatiebeveiliging voor de patiëntveiligheid van groot belang is [WOLT05].

2.4.1 Het belang van een goede informatiebeveiliging in ziekenhuizen

Informatiebeveiliging in de zorg is een heet hangijzer en is vooral sinds de invoering van de NEN 7510 norm een belangrijk aandachtspunt voor ziekenhuizen. Het digitaal, vastleggen, raadplegen en uitwisselen van privacygevoelige medische gegevens is bij zorginstellingen zoals ziekenhuizen sterk toegenomen, denk hierbij aan het Elektronisch Patiënten Dossier

(EPD) of het cliëntendossier. De digitalisering van medische gegevens maakt het mogelijk snel een volledig beeld te krijgen van patiënten. Dit komt de kwaliteit van de zorg uiteraard ten goede. Onvoldoende aandacht voor informatiebeveiliging kan leiden tot schade aan de beschikbaarheid, integriteit en de vertrouwelijkheid van die gegevens. Daardoor kan de zorg van patiënten in gevaar komen, ontstaat negatieve publiciteit voor de zorginstellingen en verdwijnt het vertrouwen bij andere zorgverleners en patiënten. Inadequate informatiebeveiliging kan dus uiteindelijk negatieve effecten hebben op het imago van het ziekenhuis of zelfs leiden tot sancties. Daarnaast kunnen problemen met elektronische gegevens leiden tot onnodige of zelfs verkeerde behandelingen, met als gevolg onnodige extra kosten en risico's. Tot slot zorgt dit voor weinig vertrouwen van medici en verplegend personeel in digitale medische gegevens [VLIE09].

Ziekenhuizen zijn zich ervan doordrongen dat informatiebeveiliging alle aandacht verdient. Beschikbaarheid, integriteit en vertrouwelijkheid zijn hierbij de sleutelbegrippen (Zie hoofdstuk 2, paragraaf 2.2). ICT-systemen moeten beschikbaar zijn wanneer dat is afgesproken en de integriteit en vertrouwelijkheid van die informatie moet zijn gewaarborgd. Informatiebeveiliging is een continu proces en vraagt niet om een eenmalige actie. De organisatie is immers niet statisch, er doen zich doorlopend wijzigingen voor in de processen en daarmee in de informatievoorziening [HEAD08]. Informatie is één van de primaire zaken waar een ziekenhuis mee te maken heeft. Bij bijna alles komt informatie kijken en die informatie is nodig om de patiënt de juiste zorg te kunnen bieden. De beveiliging van die informatie is dus een zeer belangrijk aandachtspunt.

Dat informatiebeveiliging voor ziekenhuizen van essentieel belang is, blijkt ook wel uit de drie onderstaande berichten.

Virus legt ziekenhuis Hoorn plat
Woensdag,17:53 doorRedactie
Een nog onbekend virus heeft vandaag het Westfries Gasthuis in Hoorn grotendeels platgelegd . Vanochtend kwam het ziekenhuis met het bericht dat er zich een computerstoring had voorgedaan. "Er wordt hard gewerkt om de situatie onder controle te krijgen . Onze eerste zorg gaat uit naar de meest kwetsbare patiënten ", zo is op de website van het ziekenhuis te lezen . Daar stond ook dat (poliklinische) afspraken mogelijk kwamen te vervallen en ook het uitstellen van klinische opnames werd geopperd . Via de website zou het ziekenhuis patiënten op de hoogte houden, maar verdere updates zijn niet verschenen .

Via de media laat het ziekenhuis weten dat het om een computervirus gaat . Daardoor worden in de operatiekamers alleen spoedbehandelingen uitgevoerd en beperken de poliklinieken zich tot patiënten die acute zorg nodig hebben . Opgeslagen patiëntgegevens zouden geen risico lopen .

Vaker
Dit jaar zijn al meerdere ziekenhuizen door malware besmet geraakt . In januari was het raak bij het Albert Schweitzer ziekenhuis in Dordrecht. In maart liep een Maastrichts ziekenhuis een virusinfectie op.

Bron: www.security.nl 20-10-10

Virus infecteert Maastrichts ziekenhuis
17-03-2010,16:44 doorRedactie
Gisterenmiddag zijn nog een onbekend aantal computersystemen van het academisch ziekenhuis Maastricht (aZM) door een virus getroffen. Het gaat hier volgens het ziekenhuis mogelijk om een nieuw virus. De infectie beïnvloedde het functioneren van verschillende servers, waardoor bepaalde systemen ook niet meer naar behoren werkten. Het ziekenhuis spreekt zelfs van "ernstige hinder."

De patiëntenzorg zou niet in gevaar zijn geweest en vindt gewoon doorgang. "Zij het dat op sommige afdelingen de vertraging wel merkbaar is en de wachttijden kunnen uitlopen." Geplande operaties gaan gewoon door.

Virus-killer
Volgens het ziekenhuis is er inmiddels "een zogeheten virus-killer geïnstalleerd." Daarnaast zijn er noodprocedures in gang gezet om het netwerk zo min mogelijk te belasten en het primair beschikbaar te houden voor de directe patiëntenzorg. "Er wordt hard gewerkt aan het verhelpen van het probleem en alles is erop gericht de overlast voor de patiënten tot een minimum te beperken. Indien u toch overlast mocht ervaren, bieden wij u onze excuses hiervoor aan."

Eind januari wist de Conficker worm de systemen en apparatuur van het Albert Schweitzer ziekenhuis in Dordrecht te infecteren. De worm zorgde ervoor dat het ziekenhuisinformatiesysteem (SAP), het elektronisch medicatievoorschrijfsysteem, het elektronisch patiëntendossier en diverse kantoortoepassingen op PC 's niet meer functioneerde.

Bron: www.security.nl 17-03-10

Worm legt elektronisch patiëntendossier plat
24-01-2010,17:02 doorRedactie
De Conficker worm heeft vorige week het Albert Schweitzer in Dordrecht geïnfecteerd, waardoor onder andere het elektronisch patiëntendossier niet meer werkte. In totaal had het ziekenhuis zeker vijf dagen lang met computerstoringen te maken. De worm zorgde ervoor dat het ziekenhuisinformatiesysteem (SAP), het elektronisch medicatievoorschrijfsysteem, het elektronisch patiëntendossier en diverse kantoortoepassingen op PC 's niet meer functioneerde. De overlast voor werknemers bestond uit het niet kunnen inloggen of meermalen opnieuw moeten inloggen op systemen, het geen gebruik kunnen maken van draadloze netwerken en het trager werken van apparatuur, zo meldt Het Kompas.

De juistheid en volledigheid van gegevens zouden niet in gevaar zijn geweest, wat ook voor het primaire zorgproces in het ziekenhuis geldt. Zowel de ICT-afdeling van het ziekenhuis, leverancier van antivirussoftware en de afdeling Klinische Fysica /Medische Techniek hebben zich op het verwijderen van de worm en verhelpen van de storingen gestort. Sinds 23 oktober 2008 is er een patch beschikbaar die het Windows -lek dicht waardoor de worm zich weet te verspreiden. Conficker kan daarnaast ook machines via Autorun en gedeelde netwerkmappen infecteren.

Bron: www.security.nl 24-01-10

Deze dreigingen geven duidelijk weer hoe belangrijk de beschikbaarheid, integriteit en vertrouwelijk van informatie is voor een ziekenhuis. Een virus kan er dus blijkbaar voor zorgen dat de beschikbaarheid wordt aangetast waardoor operaties niet kunnen worden uitgevoerd en in feite het ziekenhuis plat komt te liggen. Dit geeft des te meer het belang aan van een goede informatiebeveiliging bij ziekenhuizen.

2.4.2 Norm voor informatiebeveiliging in de zorg

De Nederlandse norm voor informatiebeveiliging in de zorg definieert informatiebeveiliging als volgt [WEL04]:

> *Een stelsel van maatregelen om verstoringen in de zorgvuldige en doelmatige informatievoorziening te voorkomen en eventuele schade als gevolg van desondanks optredende verstoringen te beperken. Het doel is om patiënten het gewenste niveau van dienstverlening te kunnen bieden en om de privacy van de patiënt, de zorgverlener en van de zorginstelling te beschermen.*

Deze definitie wordt omschreven in de Nederlandse Code voor Informatiebeveiliging (vanaf nu afgekort tot CViB) en wordt als internationale standaard gebruikt in de meeste organisaties. De huidige Nederlandse code is afgeleidt van de Britse informatiebeveiliging standaard, de British Standard (BS) 7799, als een samenbundeling van 'best business practices' (publicaties op basis van ervaring over hoe bepaalde aspecten van informatiebeveiliging het beste kunnen worden geregeld) voor informatiebeveiliging. Deze BS 7799 is later als ISO/IEC 17799 internationale standaard voor informatiebeveiliging gepubliceerd. De CViB is een leidraad voor praktische informatiebeveiliging. Het biedt een antwoord op de vraag naar praktische hulpmiddelen voor beveiliging van informatie in computers en netwerken. De CViB geeft handvaten voor bedrijven om op gemeenschappelijke basis een beveiligingsbeleid te ontwikkelen, maatregelen te selecteren, de nodige plannen op te stellen, en zo tot beveiliging op maat te komen [OVER05].
Bert-Jaap Koops concludeert dat de CViB voor het overgrote deel correct is vanuit Nederlands juridisch oogpunt en de eisen die gesteld worden aan informatiebeveiliging. Maar belangrijker dan de (in)correctheid van de CViB is de concretisering ervan. De algemene bepalingen moeten worden vertaald naar de praktijksituatie. Voor een goed overzicht in de wettelijke vereisten voor de informatiebeveiliging van een organisatie blijft voorop staan wat de CViB zelf al aangeeft: 'Er dient deskundig advies over specifieke juridische eisen te worden ingewonnen bij de juridische adviseurs van de organisatie of bij gekwalificeerde juristen' [KOOP03]. De CViB is een formeel geaccepteerde ISO standaard (ISO17799:2000), en bestaat uit twee delen. Deel 1 bevat een logische verzameling van beveiligingsdoelstellingen en maatregelen (afkomstig van 'best business practices') ten aanzien van beveiligingsgerelateerde onderwerpen. Deel 2 omvat de beschrijving van eisen die worden gesteld aan de werking van het 'Information Security Management System' (ISMS). Dit systeem draagt zorg voor de beheersing van het totale informatiebeveiligingsproces. De 127 individuele normen en 36 beheersdoelstellingen die gelden voor het ISMS zijn één op één terug te voeren naar de 'best business practices' zoals die verwoord zijn in deel 1, maar dan normatief geformuleerd [CVIB00].

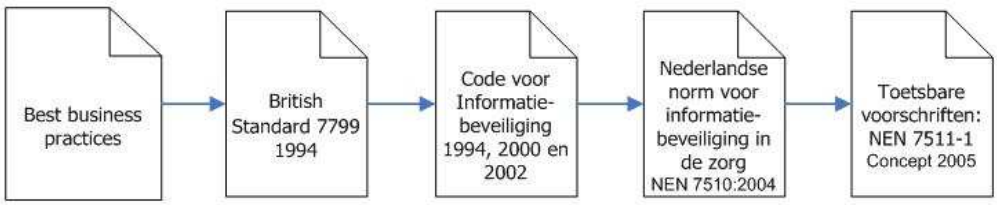
2.4.3 NEN 7510

Doordat er in de zorgsector niet tot nauwelijks gebruik werd gemaakt van de Code voor Informatiebeveiliging, is er voor de zorgsector in Nederland een aangepaste versie van de Code opgesteld, de NEN 7510. De norm NEN 7510 gaat specifiek over de informatiebeveiliging binnen de zorgsector. In de NEN 7510 wordt informatiebeveiliging omschreven als:

Het waarborgen van de beschikbaarheid, integriteit en vertrouwelijkheid van alle informatie die benodigd is om verantwoorde zorg te kunnen bieden.

Naast het borgen van deze kwaliteitscriteria vereist deze norm ook dat de informatiebeveiligingsmaatregelen op controleerbare wijze, zowel wat bedrijfsprocesniveau als onderliggende infrastructuur betreft, zijn ingericht, voordat er sprake is van adequate informatiebeveiliging. De NEN 7510 geeft richtlijnen en uitgangspunten voor het bepalen, instellen en handhaven van maatregelen die een organisatie in de gezondheidszorg dient te treffen ter beveiliging van de informatievoorziening [ON2I09].

De Nederlandse norm voor informatiebeveiliging in de zorg is van toepassing op alle zorginstellingen werkzaam in de gezondheidszorg, ongeacht de aard en de omvang van het bedrijfsproces. Er is door de NEN (Nederlands Normalisatie-instituut) gewerkt aan definitieve toetsbare voorschriften voor de NEN 7510. Er zijn door de NEN in mei 2005 drie varianten (NEN 7511-1,NEN 7511-2 en NEN 7511-3) uitgegeven. Ieder voorschrift heeft een specifiek toepassingsgebied en geven een nadere uitwerking van de NEN 7510 met een voorschrijvend, toetsbaar karakter voor complexe organisaties, samenwerkingsverbanden en solopraktijken in de zorg [NEN7510].
Door naleving van de norm NEN 7510, in combinatie met het toetsbare voorschrift uit de NEN 7511, wordt voldaan aan een passende beveiliging die is vereist voor een betrouwbare en veilige omgang met gegevens in de zorg [WOLT05]. In figuur 3 is de totstandkoming van normen voor informatiebeveiliging schematisch weergegeven:



Figuur 4: Totstandkoming van normen voor informatiebeveiliging.

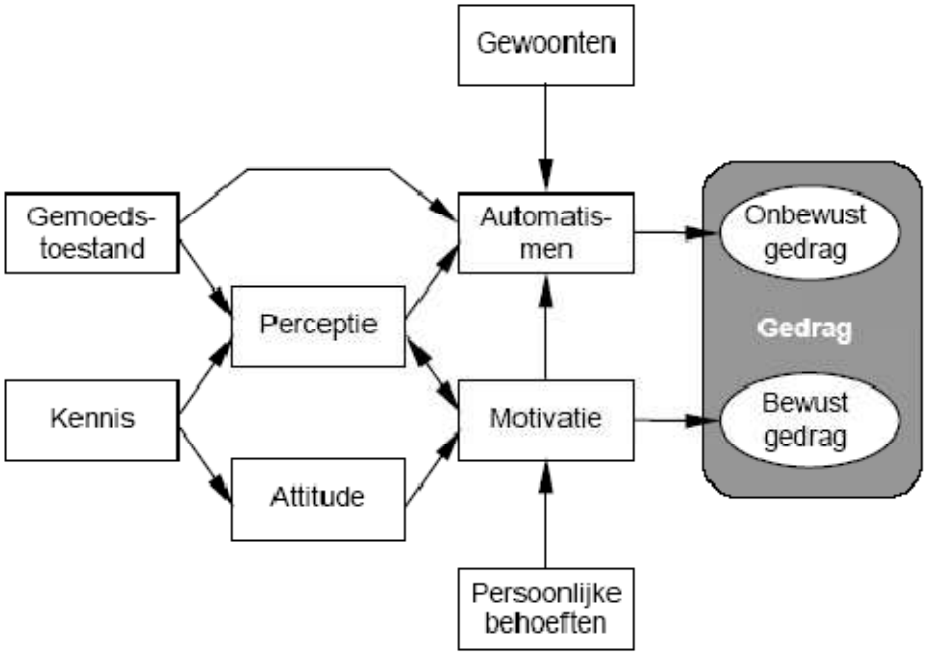
2.4.4 Toepassing van de NEN 7510 in ziekenhuizen

In 2008 is er door het college bescherming persoonsgegevens (CBP) en de inspectie voor de gezondheidszorg (IGZ) onderzoek gedaan naar de informatiebeveiliging in 20 ziekenhuizen [CBP08]. In veel zorginstellingen wordt het gebruik van ICT steeds belangrijker en wordt het gebruik van ICT ook enorm uitgebreid. Dit was voor het CBP en de IGZ aanleiding om onderzoek te doen naar de manier waarop ziekenhuizen in Nederland omgaan met de beveiliging van hun informatie. Het doel van het onderzoek was om een beeld te krijgen van de stand van zaken van de implementatie van de NEN 7510 norm bij ziekenhuizen in het algemeen. De belangrijkste uitkomsten uit dit onderzoek waren dat er op technisch gebied al veel verbeterd is, maar dat medewerkers zich nog steeds onvoldoende bewust zijn van de risico's dat het gebruik van ICT in ziekenhuizen met zich meebrengt. Ook werd duidelijk dat wat de NEN 7510 norm betreft, de meeste ziekenhuizen ten tijde van het onderzoek in 2008 niet aan deze norm voldoen en dat daardoor de informatiebeveiliging in ziekenhuizen niet in orde was.

2.5 Informatiebeveiliging en de menselijke factor

De menselijke kant van informatiebeveiliging staat steeds meer in de belangstelling. Technische beveiligingsmaatregelen, zoals firewalls of virusscanners, functioneren goed, maar zijn kennelijk niet voldoende om het scala van beveiligingsrisico's af te dekken. Men gaat er veelal vanuit dat de menselijke factor voldoende wordt afgedekt door het toewijzen van taken en verantwoordelijkheden aan medewerkers. Toch treden er aan de lopende band beveiligingsincidenten op, waarvan het merendeel terug te voeren is op menselijk falen. In het algemeen worden menselijke aspecten ernstig onderschat. Verschillende factoren zoals zelfbewustwording en het gedrag van mensen spelen hierbij een rol. Zelfbewustwording, in het Engels wordt dit aangeduid met awareness, komt later in deze thesis uitgebreid aan bod. In deze paragraaf zal kort het gedrag van mensen in relatie tot informatiebeveiliging worden besproken [SPRU04].

Om de beveiliging van informatie tegen menselijke fouten tegen te gaan, is het nodig om inzicht te hebben in menselijk gedrag. Volgens het Van Dale woordenboek omschrijft gedrag zich als de manier waarop iemand zich gedraagt. Met andere woorden: het gedrag van een persoon is alles wat die persoon zegt of doet. Gedrag wordt enerzijds bepaald door de persoonlijke karakteristieken van de persoon in kwestie. En anderzijds door de omgeving, die een bepaald gedrag mogelijk maakt, stimuleert of zelfs afdwingt. Gedrag bestaat uit twee componenten, namelijk onbewust en bewust gedrag. Dit is weergeven in de onderstaande figuur 4 [OVER07].



Figuur 5: Onbewust en bewust gedrag en de factoren die daarbij een rol spelen

Onbewust gedrag wordt gekenmerkt door automatische handelingen (automatismen), die gebaseerd zijn op gewoonten. Het al dan niet activeren van gewoonten wordt beïnvloed door de gemoedstoestand van de betreffende persoon en anderzijds diens perceptie van de omgeving.

Bewust gedrag bestaat uit handelingen die willens en wetens uitgevoerd worden. Hierbij speelt de motivatie een bepalende rol. Op basis van de perceptie van de omgeving en de attitude ten opzichte van de daarin mogelijke handelingen, kan de persoon ervoor kiezen om de desbetreffende handelingen uit te voeren. In dat geval is er sprake van intrinsieke motivatie: de motivatie komt vanuit de persoon zelf, zonder dat er sprake is van beloning. Het kan ook zijn dat de persoon in kwestie de handelingen pas uitvoert als hij ervan overtuigd is dat daar mogelijk profijt uit volgt. In dat geval is er sprake van extrinsieke motivatie: de motivatie ontstaat pas als er sprake is van beloning [SPRU04].

Niet al het gedrag is even wenselijk, mensen maken namelijk fouten. Er kan onderscheidt gemaakt worden tussen fouten die in het onbewuste gedrag gemaakt worden en fouten die in het bewuste gedrag gemaakt worden:

Gedrag	**Fouten**	**Omschrijving**
Onbewust	Uitglijders	Fouten die ontstaan doordat iemand een handeling ‘op de automatische piloot’ uitvoert, terwijl de situatie juist om een andere handeling vraagt.
	Afdwalingen	Situaties waarin een benodigde handeling niet uitgevoerd wordt
Bewust	Vergissingen	Dit zijn bewuste handelingen waarin een benodigde handelingen niet uitgevoerd wordt.
	Overtredingen	Dit is een verzamelterm voor handelingen waarbij bewust regels of voorschriften genegeerd worden.

Tabel 10: Onderscheid tussen fouten in bewust en onbewust gedrag

Daarnaast kun je ook nog spreken van overtredingen te goeder trouw en overtredingen met boze opzet. Overtredingen te goeder trouw zijn onder te verdelen in incidentele overtredingen en structurele overtredingen. Incidentele overtredingen zijn overtredingen die begaan worden omdat men vindt dat ‘het werk erom vraagt’.Structurele overtredingen zijn overtredingen die begaan worden omdat de van toepassing zijnde regels onduidelijk of ondeugdelijk zijn. Overtredingen met boze opzet zijn criminele overtredingen die strafbaar zijn: diefstal, fraude, hacking, etc [OVER07].

2.6 Conclusie

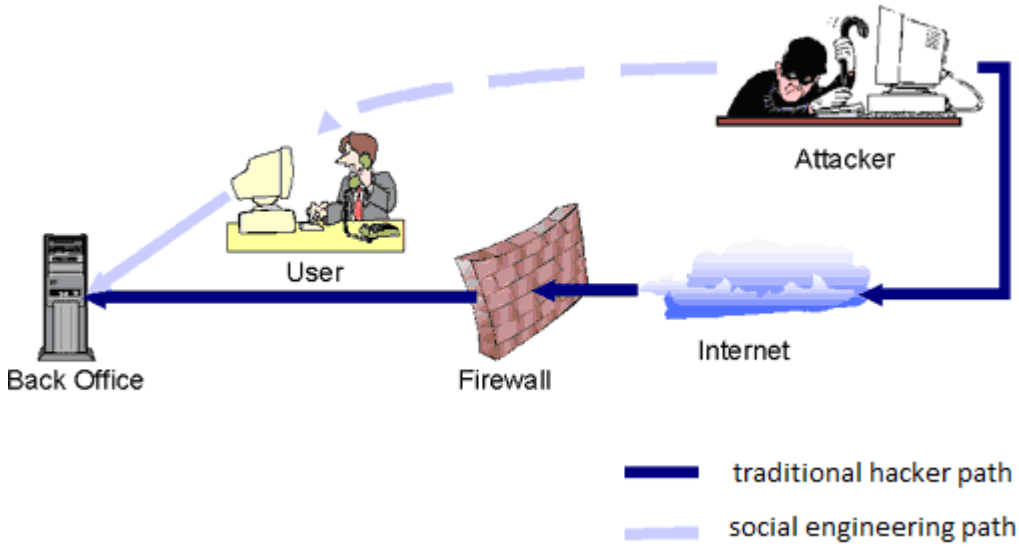
Informatiebeveiliging is voor iedere organisatie van essentieel belang om waardevolle informatie te beschermen en de continuïteit te waarborgen. Informatiebeveiliging zou dan ook ten allen tijde deel moeten uitmaken van interne controle mechanismen, die de processen, operaties en transacties van de organisatie beschermen. Deze controle mechanismen moet een medewerker zich eigen maken zodat de organisatie niet wordt blootgesteld aan kwetsbaarheden door toedoen van deze medewerker. Informatiebeveiliging moet in feite routinematig handelen worden voor medewerkers, zoals het ook routine is voor mensen in het privéleven om bijvoorbeeld de auto op slot doen wanneer je deze verlaat.
Informatiebeveiliging moet voorkomen dat er ernstige fouten worden gemaakt, dat er onveilige situaties ontstaan of dat er misbruik van informatie wordt gemaakt. Informatiebeveiliging is dus tegenwoordig voor ieder bedrijf, instelling, instituut of onderneming van essentieel belang om waardevolle informatie te beschermen en de continuïteit te waarborgen.

3. Social Engineering

In dit hoofdstuk zal het onderwerp social engineering uitgebreid aan bod komen. Er zal worden besproken wat social engineering precies is, wat het doel van social engineering is en hoe het proces van social engineering eruitziet. Vervolgens worden de psychologische factoren bij social engineering geanalyseerd, worden de verschillende social engineering aanvallen uiteengezet en worden deze aanvallen door middel van een attack tree geanalyseerd. Tot slot wordt in de laatste paragraaf van dit hoofdstuk beschreven hoe social engineering kan worden tegengegaan.

3.1 Wat is social engineering

Social engineering is een heel breed en ruim begrip en is een verzamelnaam voor een methode dat op basis van communicatie tussen aanvaller (social engineer) en doelwit voorkomt. Het doel is om ongeautoriseerde toegang tot informatie te krijgen via misleiding en is een serieuze dreiging voor de meeste beveiligde netwerken. Het is niet makkelijk om een organisatie te verdedigen tegen social engineeringaanvallen omdat social engineers de zwakste schakel in een organisatie uitbuiten, namelijk de mens [ALLE06]. Er worden naar manieren of middelen gezocht om op technologie of software gebaseerde systemen te kraken door de mensen te manipuleren die toegang tot de informatie of het gewenste systeem hebben. De onderstaande figuur geeft weer hoe de social engineer mensen gebruikt om de gewenste informatie te krijgen. De social engineer gebruikt sociale vaardigheden in plaats van traditionele hack- software en/of hardware om toegang te krijgen tot het doelwit [HINE02].



Figuur 6: De aanpak van social engineering

Er zijn talloze definities over social engineering in de literatuur te vinden. Hieronder worden enkele van deze definities weergegeven. Kevin Mitnick is één van de bekendste veroordeelde hackers die gebruik maakte van social engineering en is tegenwoordig adviseur in de beveiligingsbranche. In 2002 heeft Mitnick een boek uitgebracht waarin hij zijn ervaringen beschrijft die hij als hacker heeft opgedaan. In zijn boek, The Art of Deception, beschrijft hij social engineering als volgt:

> *"Social Engineering uses influence and persuasion to deceive people by convincing them that the social engineer is someone he is not, or by manipulation. As a result, the social engineer is able to take advantage of people to obtain information with or without the use of technology"*

Het Institute of Social Engineering gebruikt de volgende definitie:

> *"het gebruik van je sociale vaardigheden om andere mensen te bewegen tot het doen van dingen die ze anders niet gedaan zouden hebben".*

Andere voorkomende definities zijn:

> *"Social engineering is the 'art' of utilizing human behavior to breach security without the participant (or victim) even realizing that they have been manipulated."* [GULA03]
>
> *"…the art and science of getting people to comply with your wishes." [ALLE06]*
>
> *"Social Engineering - A euphemism for non-technical or low-technology means - such as lies, impersonation, tricks, bribes, blackmail, and threats - used to attack information systems."* [ALLE06]

Alle definities beschrijven min of meer hetzelfde, social engineering probeert het zwakste punt (de menselijke factor) in een organisatie uit te buiten om informatie te verkrijgen. De definitie die in dit onderzoek gebruikt zal worden is de defintie zoals die door Mitnick is opgesteld:

"Social Engineering uses influence and persuasion to deceive people by convincing them that the social engineer is someone he is not , or by manipulation. As a result, the social engineer is able to take advantage of people to obtain information with or without the use of technology"

Deze definitie kan mijns inziens worden gezien als de meest volledige. Het geeft het psychologische aspect goed weer dat bij social engineering komt kijken. Social engineering is namelijk een vorm van hacken waar weinig tot geen technologie bij komt kijken maar zich vooral richt op het psychologische aspect van hacken, mensen beïnvloeden en overtuigen om ze dingen te laten doen die ze anders niet zouden doen.

3.1.1 Het doel van social engineering

Omdat beveiligingstechnologieën steeds beter en beter worden, wordt het daardoor steeds moeilijker om technische kwetsbaarheden uit te buiten en richten hackers en andere kwaadwillenden zich daardoor op het menselijke element. Het kraken van de 'menselijke firewall' is vaak makkelijker en bevat minder risico als het goed wordt uitgevoerd. Social engineering baseert zich op het feit dat mensen zich niet bewust zijn van de waarde van informatie die ze bezitten en gaan daardoor in de meeste gevallen achteloos met de beveiliging van die informatie om. De menselijke factor is altijd de zwakste schakel in de informatiebeveiliging [LACE09].

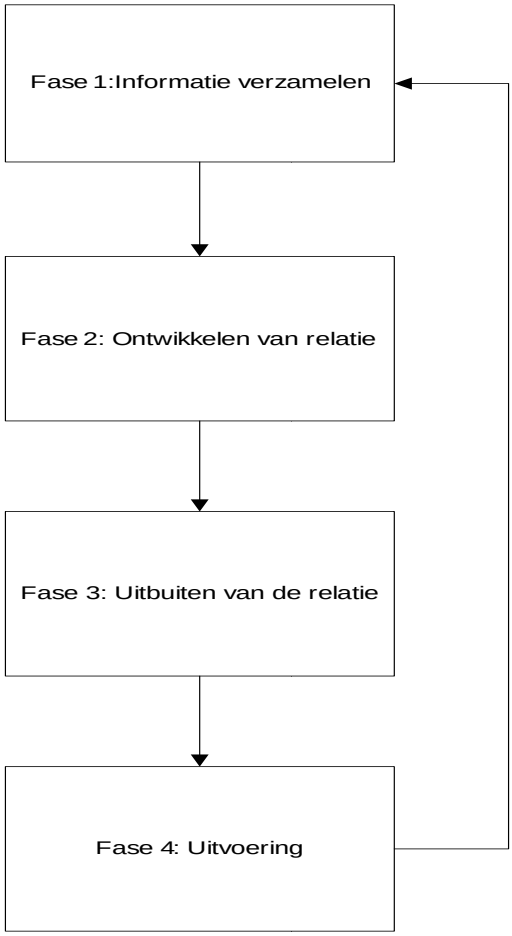
Het doel van social engineering is om iemand (het doelwit) te doen misleiden in het verstrekken van waardevolle informatie of toegang te krijgen tot die informatie of resource. Social engineering gaat daarbij uit van de kwaliteiten van de menselijke aard, zoals:

- *De wens om behulpzaam te zijn*: de meeste mensen willen graag behulpzaam zijn en dit kan leiden tot het weggeven van te veel informatie.
- *Het vertrouwen op mensen*: de menselijke aard is om mensen te vertouwen totdat bewezen wordt dat dit niet het geval is.
- *De angst om in de problemen te komen*: veel mensen zijn bang om in de problemen te komen bij het uitvoeren van hun werk.
- *De bereidheid om de 'kantjes ervan af te lopen'*: mensen kunnen som lui zijn door belangrijk materiaal rond te laten slingeren zodat iedereen dit kan zien.

Een hacker die gebruik maakt van social engineering (een social engineer) speelt in op deze eigenschappen van de mens om zo tot het uiteindelijke doel te komen: het verkrijgen van de gewenste informatie. De zwakheden van de mens worden eerst geprobeerd om bloot te leggen alvorens er andere manier geprobeerd zullen worden zoals het kraken van wachtwoorden. Waarom alle moeite nemen in het plaatsen van een trojan horse wanneer een simpel telefoontje naar een medewerker je toegang geeft tot het gewenste gebruikersnaam met wachtwoord [PELT05].

3.1.2 Het proces van social engineering

Hoewel social engineering op verschillende manieren kan worden uitgevoerd, bestaat er volgens Gartner [HINE05] een proces waaruit een aanval van social engineering is opgebouwd. Dit proces bestaat uit vier fases die worden uitgevoerd in een social engineeringaanval en elke fase is afhankelijk van de vervulling en het succes van de vorige fase. Het social engineeringproces bestaat uit de volgende 4 fases: Informatie verzamelen, ontwikkelen van een relatie, uitbuiten van de relatie en de uitvoering van de aanval om het doel te bereiken Een schematische weergave is in onderstaande figuur te vinden.



Figuur 7: Het proces van social engineering [HINE05]

Fase 1: Informatie verzamelen

Deze fase bestaat uit verschillende methoden die kunnen worden gebruikt om een grote hoeveelheid informatie te verkrijgen over het doelwit. De methode die gebruikt wordt is afhankelijk van diverse factoren (bijvoorbeeld is het doelwit een persoon of een organisatie). Het ultieme doel van deze fase is om zoveel mogelijk informatie te verzamelen over het doelwit om een relatie en vertrouwen te kunnen ontwikkelen in de volgende fase. Voorbeelden van informatie dat verzameld kan worden zijn: namen van medewerkers, een telefoonlijst, e-mail adressen en de structuur van een organisatie.

Fase 2: Ontwikkelen van een relatie

In de tweede fase wordt er door de social engineer contact met het doelwit gezocht. Met de verzamelde informatie zal er vervolgens geprobeerd worden om een relatie gebaseerd op vertrouwen op te bouwen met het doelwit. Het zit in de menselijke aard om iemand te vertrouwen die goed is ingelicht, veel van de omgeving afweet en die dezelfde interesses delen. Dit geldt ook voor iemand die behulpzaam, vriendelijk en hoffelijk overkomt. Door een

relatie te ontwikkelen, positioneert de social engineer zichzelf in een positie van vertrouwen dat vervolgens kan worden uitgebuit.

Fase 3: Uitbuiten van de relatie

Wanneer het contact gemaakt is, kan de social engineer het vertrouwen uitbuiten of de vertrouwensrelatie verbeteren door in te spelen op de emoties van het doelwit. Het doelwit kan dan worden gemanipuleerd door de social engineer (die inmiddels helemaal vertrouwd wordt), om informatie weg te geven of een actie uit te voeren dat normaal nooit zal gebeuren. Deze aanval kan het einde van de aanval zijn of het begin van de volgende fase.

Fase 4: Uitvoering

Wanneer de gewenste informatie verkregen is, gebruikt de social engineer deze informatie om zijn doelstelling te bereiken. Als de verkregen informatie gebruikt wordt om een stap dichter bij het ultieme doel te komen, zal de social engineer terugkeren naar het begin van het proces totdat het ultieme gewenste doel bereikt wordt.

Zoals de pijl in figuur 7 aangeeft, kan het proces een aantal keer herhaald worden totdat de social engineer alle informatie verzameld heeft die nodig is. Op deze manier kan alle informatie verzameld worden die nodig is om de aanval uit te voeren [ALLE06].

3.2 Psychologische factoren bij social engineering

De social engineer gebruikt zijn invloed en overtuiging om mensen te misleiden om aan informatie te komen. Om social engineering te kunnen begrijpen is het nodig om de psychologische factoren die bij social engineering komen kijken op een rijtje te zetten. In deze paragraaf zal worden beschreven welke eigenschappen het menselijk gedrag heeft en welke psychologische technieken de social engineer kan gebruiken om zijn doel te bereiken.

3.2.1 Psychologische eigenschappen van het menselijk gedrag

Ieder mens bezit een aantal eigenschappen waar de social engineer probeert op in te spelen bij het uitvoeren van een social engineeringaanval. Robert Cialdini [CIAL01] geldt als een expert op dit gebied en volgens hem zijn er zes basis psychologische eigenschappen die het menselijk gedrag sturen. Deze eigenschappen worden in deze subparagraaf uiteengezet.

1. **Autoriteit**
   De kracht van de druk van autoriteit kan een zeer krachtige vorm zijn in het beïnvloeden van mensen. De social engineer probeert het gewenste resultaat te halen door het doelwit te laten denken dat hij of zij met een autoritair persoon te maken heeft. De gehoorzaamheid naar autoriteit is vaak iets wat beloond wordt en het is daardoor natuurlijk om naar personen met autoriteit te luisteren. Mensen reageren

vaak kwetsbaar op autoriteit en hier kan handig op ingespeeld worden omdat de kans op medewerking groot is wanneer mensen met symbolen (bijvoorbeeld kleding, titels) van autoriteit te maken krijgen.

2. **Commitment en consistentie**

Het consistentie eigenschap is erg effectief in het leiden van menselijk gedrag. Deze eigenschap zegt dat na het maken van een keuze (commitment) of het innemen van een standpunt, er persoonlijke druk ontstaat om vasthoudendheid te tonen aan die commitment. Bijna alle mensen gedragen zich op een consistente manier in de meeste situaties die voorkomen in iemands leven. De persoon wiens woorden en daden niet overeenkomen wordt gezien als een verward en onbetrouwbaar individu. Terwijl een persoon die consistentie toont in zijn manier van leven gezien wordt als een persoon met veel sterkte en intelligentie. Een andere reden waarom consistentie een aantrekkelijke eigenschap voor mensen is, is dat het de complexiteit van het leven vereenvoudigt. Consistent gedrag maakt het mogelijk om mentale energie te sparen door niet telkens moeilijke beslissingen te hoeven nemen de hele dag.

3. **Sympathie**

Een persoon accepteert eerder een verzoek van iemand wanneer die persoon sympathiek overkomt. Mensen zeggen graag ja tegen personen wanneer ze die persoon daadwerkelijk kennen en ook graag mogen en sympathie voor hebben. Een social engineer zal een doelwit proberen te manipuleren door sympathie te kweken waardoor de social engineer in een goede positie komt om het verzoek succesvol af te ronden.

Er zijn een aantal factoren die van invloed zijn op het krijgen van sympathie voor een persoon. Fysieke aantrekkelijkheid is hierin een belangrijke factor. Aantrekkelijke mensen worden gezien als sympathiek, kunnen mensen vaak beter overtuigen en worden vaker zelf geholpen. Een andere factor is gelijksoortigheid. Mensen houden graag van mensen die een gelijkenis in gedrag, achtergrond, meningen en persoonlijkheden hebben. De derde factor is lof. Iemand die veel complimenten geeft aan anderen wordt vaak ook erg sympathiek en aardig gevonden. Herkenning is ook een factor. Mensen houden graag van dingen die bekend voorkomen. De vijfde en laatste factor is associatie. Mensen associëren zichzelf graag met positieve dingen en dit kan beïnvloed worden door bijvoorbeeld positief nieuws te brengen. Al deze factoren verhogen de kans op het krijgen van een succesvol antwoord op een verzoek.

4. **Reciprocation**

Reciprocation (in het Nederlands betekent dit wisselwerking) is één van de meest effectieve manieren in het beïnvloeden van mensen. Sociale interactie is vaak gebaseerd op het feit dat als iemand iets geeft, dan wordt van die andere persoon verwacht dat die ook iets teruggeeft. Dit is wat reciprocation inhoudt. Als iemand een gunst verleent aan een ander persoon, voelt die persoon zich vaak verplicht om iets terug te geven. Deze eigenschap is zeer effectief omdat het diepgeworteld in onze maatschappij zit. Niemand mag een persoon die alleen aanneemt en vervolgens niets teruggeeft.

Reciprocation kan zeer succesvol zijn omdat een kleine eerste gunst vaak ervoor zorgt dat er grotere gunsten voor terugkomen. Dit komt omdat de meeste mensen het niet fijn vinden om een soort van schuld te hebben. Niemand houdt van een persoon die alleen neemt en niets teruggeeft. Een social engineer weet dit en kan hier handig gebruik van maken.

5. **Schaarste**
   De schaarste eigenschap zorgt ervoor dat mensen meer waarde hechten aan zaken of mogelijkheden die moeilijk te verkrijgen zijn. Een voorbeeld hierbij is de 'deadline' tactiek. Een verkoper probeert iets te verkopen aan een klant wat nog maar enige tijd geldig is. De bedoeling is om de klant geen tijd te geven om na te denken en er toe te dwingen om het product aan te schaffen.

   De kracht van deze eigenschap ligt ook in het feit dat wanneer bepaalde mogelijkheden minder beschikbaar voor mensen zijn, er bepaalde vrijheden verloren gaan en mensen verliezen niet graag vrijheden die al in bezit zijn. Ook worden meer dingen als waardevol gezien die nog maar sinds kort moeilijk te verkrijgen zijn dan dingen die al geruime tijd moeilijk te verkrijgen zijn.

6. **Sociale zekerheid**
   De eigenschap van sociale zekerheid zegt dat in een gegeven situatie er gekeken wordt naar het gedrag van anderen om uit te vinden wat er precies gedaan moet worden. Als veel mensen hetzelfde doen, wordt dit vaak gezien als het enige juiste. Sociale zekerheid is effectief en invloedrijk wanneer er wordt voldaan aan twee specifieke condities. De eerste conditie is onzekerheid. Als een persoon zich onzeker voelt, wordt er door die persoon eerder naar het gedrag van anderen gekeken om te zien wat het beste is om te doen. De tweede conditie is gelijkwaardigheid. Mensen volgen eerder het gedrag van anderen wanneer deze mensen gelijkenis vertonen met henzelf.

Naast deze eigenschappen zijn er in de verschillende literatuur nog een aantal eigenschappen te vinden die het menselijk gedrag sturen, deze eigenschappen worden hieronder uiteengezet.

7. **Behulpzaamheid**
   Het ligt in de menselijke aard om behulpzaam te willen zijn. Social engineers zijn hiervan op de hoogte en kunnen dit in hun voordeel gebruiken door het doelwit te laten denken dat ze in een bepaalde situatie behulpzaam zijn [SIEG09].

8. **Nieuwsgierigheid**
   Nieuwsgierig zijn is iets wat mensen altijd al van nature zijn geweest en motiveert mensen vaak om een actie te ondernemen. Een social engineer kan hier op inspelen en de interesse van een doelwit proberen te wekken. Het doelwit zal dit niet kunnen weerstaan en gaat dan in de meeste gevallen ook in op het vooropgestelde plan van de social engineer [JORD05].

9. **Hebzucht**
   Hebzucht is een eigenschap dat mensen enorm kwetsbaar voor manipulatie maakt. Een social engineer kan een doelwit iets in het vooruitzicht stellen wat moeilijk te negeren valt. Het doelwit heeft vaak moeite om weerstand tegen dit verzoek te bieden vanwege de hoge beloning die het doelwit in het vooruitzicht wordt gesteld [JORD05].

10. **Onverschilligheid**
    Onverschilligheid heeft te maken heeft te maken met de nonchalance en onwetendheid van de mens. In sommige gevallen maakt het de mens helemaal niet uit wat er in de directe omgeving gebeurt en worden de geldende regels genegeerd. Een social engineer kan hier dan natuurlijk handig op inspelen en is het niet moeilijk om informatie afhandig te maken [JORD05].

11. **Angst**
    Angst is een eigenschap waar heel goed op valt in te spelen door social engineers. Als mensen een bepaald verzoek krijgen, is men geneigd om het verzoek uit te voeren omdat er angst is voor maatregelen wanneer het verzoek niet goed wordt uitgevoerd [JORD05].

12. **Schuldgevoel**
    Een schuldgevoel hebben is een eigenschap van de mens dat niet prettig aanvoelt. Mensen kunnen er vaak niet tegen als ze zien dat mensen op de één of andere manier problemen hebben of ergens aan onder doorgaan. Een social kan een doelwit ervan overtuigen dat als het verzoek niet wordt ingewilligd, het doelwit grote problemen zal krijgen waardoor er een schuldgevoel ontstaat [JORD05]

3.2.2 Psychologische technieken van een social engineer

De social engineer heeft een aantal technieken ter beschikking die gebruikt kunnen worden bij een social engineeringaanval. Deze technieken zijn psychologisch van aard en hebben het doel om te misleiden en te manipuleren. Een social engineer kan meerdere technieken combineren bij een aanval.

1. **Vriendelijkheid**
   Een effectieve techniek dat helpt om aan informatie te komen is door vriendelijk te zijn. Mensen geven eerder informatie weg als ze het idee hebben dat ze die persoon kennen en mogen en daardoor het gevoel hebben een vriend te zijn tegenover die persoon. Het speelt in op de eigenschap van de mens dat hij graag gemogen wilt worden en hierdoor hulpvaardiger word [GOPA10].

2. **Flirten**
   Flirten is een techniek dat handig inspeelt op het ego van de mens. Door avances te maken richting het doelwit kan er een situatie ontstaan waarbij er een bepaalde vorm van seksuele spanning ontstaat waardoor de social engineer deze situatie kan uitbuiten [GRAN01].

3. **Vleierij**
   Net als flirten speelt ook vleierij in op het ego van de mens. Door veelvuldig complimenten uit te delen wordt er een situatie gecreëerd waarin mensen geneigd zijn om vanwege de complimenten iets terug te willen doen of geven. De social engineer kan hier dan handig op inspelen en vervolgens uit buiten [GRAN01].

4. **Intimidatie**
   Intimidatie is een techniek dat gebruikt wordt om mensen te intimideren (bang te maken) om zo een bepaalde handeling uit te voeren zoals het weggeven van informatie. Een social engineer kan zich voordoen als een persoon met autoriteit en een bepaald verzoek indienen. De primaire reactie is dan vaak om in te stemmen met het verzoek vanwege de oncomfortabele situatie die er op dat moment dan is [GOPA10] .

5. **Diffusion of responsability**
   Mensen hebben de neiging om eerder te voldoen aan een verzoek wanneer ze het idee hebben dat er meerdere mensen verantwoordelijk zijn en niet alleen zijzelf. Een social engineer kan dit uitbuiten door te doen geloven dat bij het uitvoeren van een actie de verantwoording niet alleen bij hemzelf ligt, maar ook bij andere medewerkers. Hierdoor voldoen mensen eerder aan een verzoek van de social engineer [GOPA10].

6. **Afleiding**
   Deze techniek richt zich op de zwakheid van de mens dat het vaak maar op één ding kan concentreren. Een social engineer kan deze zwakheid uitbuiten door voor afleidingen te zorgen. Als een doelwit is afgeleid kan een social engineer makkelijker de gewilde informatie afhandig maken [GOPA10].

7. **Urgentie**
   Een social engineer kan er bij een doelwit voor zorgen dat er een vorm van onrust ontstaat wanneer bepaalde informatie niet snel wordt verstrekt waardoor er negatieve consequenties kunnen ontstaan voor het doelwit. Hierdoor kan het doelwit een onjuiste beslissing nemen in het voordeel van de social engineer [REDM06].

8. **Overbelasting**
   Deze techniek zorgt ervoor dat een doelwit met zoveel informatie wordt verstrekt, dat vervolgens deze informatie niet meer effectief kan worden verwerkt. Het doelwit kan de ‘overload’ aan informatie niet aan en de social engineer maakt hier gebruik van door het doelwit over te halen om te voldoen aan een verzoek [REDM06]

9. **Morele plicht**
   Mensen willen vaak datgene doen wat juist is. Mensen willen een teamspeler zijn en hun collega’s helpen. Wanneer een social engineer een verzoek doet aan het doelwit waarbij een klein beetje de regels moeten worden gebroken, om zo bijvoorbeeld een collega te kunnen helpen, dan kan het doelwit besluiten om hieraan te voldoen [REDM06].

10. **Directe benadering**
    Dit is waarschijnlijk de meest risicovolle techniek dat een social engineer kan gebruiken. De social engineer vraag gewoon simpelweg zonder een omweg wat hij daadwerkelijk wilt. Soms stemt het doelwit hiermee in maar in de meeste gevallen wordt dit geweigerd omdat het argwaan opwekt [REDM06].

3.2.3 De relatie tussen de psychologische eigenschappen en technieken

De in de subparagraaf 3.2.2 uiteengezette psychologische technieken kunnen de in subparagraaf 3.2.1 beschreven psychologische eigenschappen van de mens beïnvloeden. Een social engineer kan die technieken gebruiken om de psychologische eigenschappen van de mens uit te buiten voor eigen gewin. In de onderstaande tabel 11 worden deze relaties weergegeven. In deze tabel (en ook in tabel 12 op pagina 47) zijn de technieken flirten en vleierij ondergebracht bij vriendelijkheid. Deze drie technieken spelen in op dezelfde eigenschappen en verschillen in feite niet veel van elkaar. Bij alle drie de technieken wordt ingespeeld op het ego van de mens door vriendelijk te zijn met als doel een vriendschappelijke band met iemand op te bouwen.

Eigenschappen / Technieken	Autoriteit	Commitment & consistentie	Sympathie	Reciprocation	Schaarste	Sociale zekerheid	Behulpzaamheid	Nieuwsgierigheid	Hebzucht	Onverschilligheid	Angst	Schuldgevoel
Vriendelijkheid			X	X			X	X				
Intimidatie	X	X									X	X
Diffusion of responsability						X						
Afleiding							X	X	X	X		
Urgentie	X				X						X	
Overbelasting	X	X									X	
Morele plicht			X	X			X					X
Directe benadering							X	X		X	X	

Tabel 11: Psychologische technieken in relatie met de psychologische eigenschappen

De techniek vriendelijkheid (en dus ook flirten en vleierij) speelt vooral in op de eigenschappen sympathie, reciprocation , behulpzaamheid en nieuwsgierigheid. Deze eigenschappen worden vaak alleen beïnvloed bij mensen wanneer zij op een positieve manier benaderd worden in plaats van op een negatieve manier zoals door intimidatie.

Intimidatie speelt in op eigenschappen die te maken hebben met autoriteit, angst en schuldgevoel. Dit komt omdat er een oncomfortabele situatie ontstaat wanneer gebruik gemaakt wordt van intimidatie.

Diffusion of responsability is een techniek dat vooral inspeelt op sociale zekerheid omdat er bij deze techniek naar het gedrag van anderen wordt gekeken om een verzoek uit te voeren. Afleiding is een techniek dat met name zal voorkomen bij behulpzaamheid, nieuwsgierigheid,

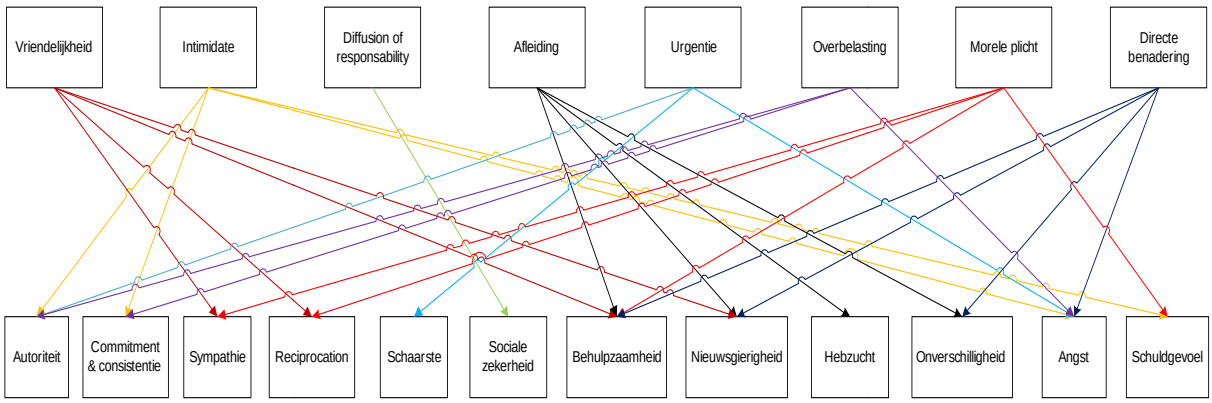
hebzucht en onverschilligheid. Door mensen af te leiden met iets kan er bijvoorbeeld een vorm van nieuwsgierigheid of behulpzaamheid worden opgewekt.

Urgentie kan gerelateerd worden aan autoriteit, schaarste en angst. Als een persoon inspeelt op de eigenschap autoriteit door middel van de techniek urgentie en een verzoek neerlegt met de eis dat er snel op gereageerd dient te worden, kan het slachtoffer dit verzoek moeilijk negeren en is daardoor dus kwetsbaar omdat hij of zij denkt te maken te hebben met een persoon die veel macht bezit. Dit geldt ook voor de techniek overbelasting. Door een verzoek bij iemand neer te leggen en die persoon vervolgens met informatie te overladen en tegelijkertijd in te spelen op de eigenschap autoriteit, is die persoon geneigd om te voldoen aan het verzoek. Overbelasting speelt ook in op commitment & consistentie en angst. Door iemand met informatie te overladen kan die persoon in de verleiding worden gebracht om niet meer zo vasthoudend te zijn, en kan hierdoor een andere keuze maken of een handeling verrichten dan dat die persoon normaal doet.

De techniek morele plicht wordt gebruikt om een ander persoon te overtuigen om datgene te doen wat in zijn of haar gevoel juist is. Hierdoor wordt ingespeeld op de eigenschappen sympathie, reciprocation, behulpzaamheid en schuldgevoel omdat deze eigenschappen te maken hebben met de aard van de mens om een ander persoon te helpen.

De techniek directe benadering speelt bijna alleen in op de eigenschappen behulpzaamheid, nieuwsgierigheid, onverschilligheid en angst. Dit is afhankelijk van wat voor informatie de social engineer wil en op welke manier dit aan het doelwit wordt gevraagd. Deze eigenschappen zijn het makkelijkst beïnvloedbaar bij een persoon en dus het best te gebruiken bij directe benadering.

In de onderstaande figuur zijn de relaties tussen de technieken en eigenschappen nog eens op een andere manier visueel weergegeven.



Figuur 8: Psychologische technieken in relatie met de psychologische eigenschappen

3.3 Social engineering tactieken

Er zijn twee categorieën waaronder alle social engineering tactieken (aanvallen) kunnen worden geclassificeerd: op computer (technologie) gebaseerde tactieken of op mensen gebaseerde tactieken. Beide methoden hebben met elkaar overeen dat de social engineer eerst een achtergrond onderzoek uitvoert voordat er wordt begonnen met de aanval [ARTH10].

Op computer gebaseerde tactieken

In de technische of op computer gebaseerde social engineering tactieken, vertrouwt de social engineer op technologie om het doelwit te misleiden. Het doelwit krijgt informatie aangeleverd van de social engineer dat nodig is om het doel van de aanval te vervullen. Dit kan bijvoorbeeld worden gedaan door valse pop-ups die als doel hebben om ervoor zorgen dat het doelwit informatie prijsgeeft. Een voorbeeld is dat er aan het doelwit gevraagd wordt om een gebruikersnaam met wachtwoord te geven voor authenticatie. De gebruikersnaam en wachtwoord dat door het doelwit wordt vertrekt, wordt dan vervolgens naar de social engineer gestuurd. De social engineer is dan nu in staat om met deze informatie het netwerk en het computersysteem binnen te dringen.

Op mensen gebaseerde tactieken

De andere aanpak van social engineering, de op mensen gebaseerde aanpak, is vaak de meest simpele en populairste methode van een social engineering aanval. Deze aanpak is simpelweg gebaseerd op misleiding via menselijke interactie. Deze vorm van aanvallen zijn succesvol vanwege het grote voordeel dat de social engineer krijgt door de onwetendheid en de neiging van mensen om behulpzaam te zijn. Dit gebeurt door middel van verschillende vormen van misleiding, zoals onder andere vriendelijkheid, imitatie en door autoriteit te tonen [ARTH10].

Social engineers gebruiken veel verschillende tactieken om anderen te overtuigen en te beïnvloeden om zo hun doel te bereiken. In de twee volgende subparagrafen worden de meest voorkomende tactieken op een rijtje gezet.

3.3.1 Op mensen gebaseerde social engineeringstactieken

Op mens gebaseerde tactieken die veel gebruikt worden zijn impersonation, dumpster diving, shoulder surfing, piggybacking en reverse social engineering. In deze subparagraaf zullen de genoemde tactieken worden beschreven met per tactiek een overzicht van wat het doel van de tactiek is, welke voorbereiding vereist is, op welke psychologische eigenschap er kan worden ingespeeld en welke techniek de social engineer kan gebruiken.

1. **Impersonation**
   Impersonation (imitatie) is de meest gebruikte techniek door social engineers om mensen te misleiden. Het komt erop neer dat een social engineer zich voordoet als iemand anders. Er wordt door de social engineer een karakter gecreëerd en speelt vervolgens een rollenspel om de gewenste informatie te verkrijgen. De rollen die de social engineer kan aannemen zijn o.a. een klusjesman, een manager of een vertrouwde derde partij [SIEG09].

Doel	De social engineer doet zich voor als een ander persoon om een vertrouwensrelatie op te bouwen om zodoende toegang en/of informatie te krijgen.
Voorbereiding	Informatie verzamelen over het doelwit en de rol die wordt aangenomen moet goed worden voorbereidt.
Eigenschap	Afhankelijk van de rol die de social engineer aanneemt kunnen op alle eigenschappen worden ingespeeld.
Techniek	Afhankelijk van de rol die de social engineer aanneemt kunnen alle technieken gebruikt worden.

2. **Dumpster diving**
   Een andere populaire methode is het doorzoeken van afval, ook wel bekend als dumpster diving. Veel informatie kan worden verzameld door afval te doorzoeken. Informatie dat eigenlijk vernietigd had moeten worden omdat het vertrouwelijke en gevoelige informatie bevat, eindigt vaak bij het afval en is dus een goede bron voor social engineers om aan informatie te komen [ALLE06].

Doel	Het verkrijgen van informatie door het afval van het doelwit te doorzoeken.
Voorbereiding	Lokaliseren waar het afval van het doelwit zich bevindt.
Eigenschap	Onverschilligheid.
Techniek	Afleiding.

3. **Shoulder surfing**
   Shoulder surfing is een techniek dat neerkomt op het ongemerkt observeren van het doelwit om door middel van ‘spionage’ aan informatie te komen. Het is mogelijk om aan een gebruikersnaam met wachtwoord te komen door simpelweg over de schouder mee te kijken wanneer dit in een computersysteem wordt ingevoerd [ALLE06].

Doel	Het verkrijgen van informatie door ongemerkte observatie van het doelwit.
Voorbereiding	De social engineer moet ervoor zorgen dat er geen argwaan is wanneer hij zich in de buurt van het doelwit bevindt.
Eigenschap	Behulpzaamheid, nieuwsgierigheid, hebzucht, onverschilligheid.
Techniek	Afleiding.

4. **Piggybacking**

Piggybacking is één van de meest effectieve manieren om jezelf toegang te verschaffen tot een organisatie of een afgeschermde ruimte. Een social engineer doet zich voor als een medewerker en loopt een beveiligd gebouw binnen door iemand te volgen die toegang tot het gebouw heeft. Een voorbeeld hiervan is dat de social engineer zich voordoet als een medewerkers en zich buiten bij een groepje mensen aansluit die staan te roken. Wanneer deze mensen naar binnen gaan volgt de social engineer ze naar binnen en heeft dan geen last van fysieke beveiligingsmaatregelen [WHIT09].

Doel	Het ongemerkt binnenkomen van een gebouw of ruimte.
Voorbereiding	Er is geen speciale voorbereiding vereist.
Eigenschap	Sympathie, behulpzaamheid, onverschilligheid.
Techniek	Vriendelijkheid, flirten, vleierij, afleiding.

5. **Reverse social engineering**

Reverse social engineering is wanneer de social engineer zich voordoet als een persoon die een hoge functie bekleedt en autoriteit heeft en waar medewerkers zich toe richten als ze hulp nodig hebben. Het wordt reverse social engineering genoemd omdat het doelwit het contact initieert en niet de social engineer. Deze techniek vereist een grondig onderzoek en voorbereiding om succesvol te kunnen zijn. Reverse social engineering bestaat uit 3 fases die uitgevoerd moeten worden: sabotage (voorbereiding), marketing (uitvoering) en onderhoud. In de sabotage fase moet de social engineer ervoor zorgen dat het doelwit contact gaat leggen met de social engineer. In de volgende fase, de marketing fase, zorgt de social engineer er daadwerkelijk voor dat het doelwit contact opneemt. In de laatste fase, de onderhoudsfase, moet de social engineer ervoor zorgen dat het doelwit niets doorkrijgt en moet het probleem waarvoor het doelwit contact had opgezocht verholpen worden. Nu kan geprobeerd worden om de gewenste informatie te krijgen of er kan een vertrouwensrelatie tussen de social engineer en het doelwit worden opgebouwd [WHIT09]

Doel	Het doel van deze methode is dat het doelwit uiteindelijk de social engineer om hulp vraagt.
Voorbereiding	Deze methode vereist een grondige voorbereiding en gaat uit van de drie hierboven genoemde fases: sabotage, marketing en onderhoud.
Eigenschap	Autoriteit, commitment en consistentie, reciprocation, sociale zekerheid, behulpzaamheid, angst, schuldgevoel.
Techniek	Intimidatie, diffusion of responsability, overbelasting, morele plicht

3.3.2 Op computer of technologie gebaseerde social engineeringstactieken

Op computer of technologie gebaseerde tactieken die veel gebruikt worden zijn phishing, trojan horses, popup windows en baiting. . In deze subparagraaf zullen de genoemde tactieken worden beschreven met per tactiek een overzicht van wat het doel van de tactiek is, welke voorbereiding vereist is, welke psychologische eigenschap beïnvloed wordt en welke techniek de social engineer kan gebruiken.

6. **Phishing**

Phishing is de meest voorkomende vorm van online social engineering en kan op twee manieren plaatsvinden. Phishing kan worden beschouwd als een vorm van imitatie waarmee de social engineer een aanval plaatst door middel van een nagemaakte website of een valse e-mail. Phishing door middel van een valse e-mail moet ervoor zorgen dat het doelwit op de e-mail reageert door bijvoorbeeld de e-mail te beantwoorden en te voldoen aan het verzoek om een wachtwoord mee te sturen. De bekendste vorm van phising op deze manier is natuurlijk de bekende e-mail uit Nigeria waarin om geld wordt gevraagd.

De andere vorm van phishing zorgt ervoor dat het doelwit een website bezoekt die hij of zij vertrouwt maar die in werkelijkheid door de social engineer gekloond (nagemaakt) is. Deze nagemaakte website doet zich voor als de echte website, maar is dus gecreëerd door de social engineer om ervoor te zorgen dat het doelwit vertrouwelijke en gevoelige informatie op de website invoert [ALLE06].

Doel	Het doel van deze methode is het oplichten van het doelwit door een vertrouwde situatie te creëren waarbij het doelwit nietsvermoedend allerlei vertrouwelijke informatie weggeeft.
Voorbereiding	Bij deze methode gaat een grondige voorbereiding vooraf: er zal een website moeten worden gekloond of een valse e-mail worden opgesteld.
Eigenschap	Behulpzaamheid, nieuwsgierigheid, angst.
Techniek	Directe benadering

7. **Trojan Horses en andere malware**

Deze techniek heeft hetzelfde doel als phishing, maar in tegenstelling tot phishing gaat dit meestal automatisch en wordt er geen interactie van gebruikers vereist (behalve voor bijvoorbeeld het installeren van software). Een voorbeeld kan een key-logger zijn dat op het computersysteem van het doelwit wordt geïnstalleerd. Dit zorgt ervoor dat alle toetsaanslagen worden geregistreerd en verstuurd naar de social engineer. Dit is een handige manier om aan gebruikersnamen en wachtwoorden te komen [SIEG09].

Doel	De social engineer zorgt ervoor dat het doelwit niets vermoedend een trojan horse of andere malware op zijn computersysteem installeert en er hierdoor vertrouwelijke informatie in het bezit van de social engineer komt.
Voorbereiding	De social engineer moet ervoor zorgen dat het doelwit in het bezit van de trojan horse komt en deze daadwerkelijk ook zal installeren.
Eigenschap	Autoriteit, sympathie, behulpzaamheid, nieuwsgierigheid, hebzucht, onverschilligheid, angst.
Techniek	Vriendelijkheid, flirten, vleierij, intimidatie, urgentie, overbelasting, morele plicht.

8. **Popup window**
   Deze techniek zorgt ervoor dat er een popup scherm verschijnt op het computerscherm van het doelwit. Dit popup scherm kan bijvoorbeeld aangeven dat de verbinding met het netwerk verbroken is en dat het doelwit zijn of haar gebruikersnaam met wachtwoord moet invoeren om weer toegang te krijgen tot het netwerk. De social engineer krijgt dan deze informatie toegestuurd.

Doel	Het weggeven van vertrouwelijke informatie door een situatie te creëren waarbij het doelwit nietsvermoedend deze informatie invoert.
Voorbereiding	Het creëren van een natuurlijke situatie op het computersysteem van het doelwit.
Eigenschap	Onverschilligheid.
Techniek	Directe benadering.

9. **Baiting**
   Baiting is een techniek dat op specifieke plekken spullen achterlaat die door het doelwit als interessant kunnen worden gezien en vervolgens wordt meegenomen om het op de werkplek te bekijken. In de meeste gevallen zijn dit cd-roms of USB-sleutels die vooraf geprogrammeerd zijn. Zodra deze cd-roms of USB-sleutels door het doelwit worden gebruikt zal het programma zich activeren en gelijk alle wachtwoorden opzoeken en versturen naar de social engineer [WHIT09].

Doel	Het verkrijgen van vertrouwelijke informatie door middel van het neerleggen van spullen op een specifieke plaats die door het doelwit als zodanig interessant worden gezien dat het wordt meegenomen en op de werkplek wordt bekeken.
Voorbereiding	Het vooraf infecteren van een USB-sleutel of een andere informatiedrager met een programma dat ervoor zorgt wanneer het geopend wordt dat het alle gewenste informatie naar de social engineer opstuurt. Daarnaast zal een geschikte plek moeten worden gekozen om de USB-sleutel neer te leggen. Bijvoorbeeld bij de auto van het doelwit of bij het koffieapparaat.
Eigenschap	Nieuwsgierigheid, hebzucht, onverschilligheid.
Techniek	Afleiding

3.3.3 Social engineering tactieken in relatie met eigenschappen en technieken

De negen social engineeringstactieken kunnen in relatie met de psychologische eigenschappen van de mens en de technieken die door de social engineer worden gebruikt schematisch worden weergegeven. In de vorige subparagraaf is per social engineeringstactiek de eigenschap vermeld waarop door de social engineer wordt ingespeeld en welke techniek door de social engineer wordt gebruikt. In de tabellen en figuren op de volgende pagina's wordt dit nog eens schematisch herhaald.

In onderstaande tabel 12 is te zien welke technieken door de social engineer kunnen worden gebruikt ter ondersteuning bij de social engineeringtactieken.

Technieken / Tactieken	Vriendelijkheid	Intimidatie	Diffusion of responsability	Afleiding	Urgentie	Overbelasting	Morele plicht	Directe benadering
Impersonation	X	X	X	X	X	X	X	X
Dumpsterdiving				X				
Shoulder surfing				X				
Piggybacking	X			X				
Reverse social engineering		X	X			X	X	
Phishing								X
Trojan horses	X	X			X	X	X	
Popup window								X
Baiting				X				

Tabel 12: Social engineeringstactieken in relatie met de psychologische technieken van de social engineer

Bij impersonation kunnen alle technieken worden gebruikt, afhankelijk van welke rol de social engineer aanneemt. Speelt de social engineer de rol van helpdeskmedewerker,dan zal de techniek vriendelijkheid worden gebruikt en als de rol van een autoritair persoon wordt aangenomen zal door middel van intimidatie geprobeerd worden om bepaalde informatie te verkrijgen.

Dumpsterdiving is een tactiek dat gebruikt maakt van afleiding. Door de het doelwit af te leiden kan de social engineer het afval doorzoeken. Dit geldt ook voor shoulder surfing, door het doelwit af te leiden kan geprobeerd worden om mee te kijken en op deze manier aan inlognamen en wachtwoorden te komen.

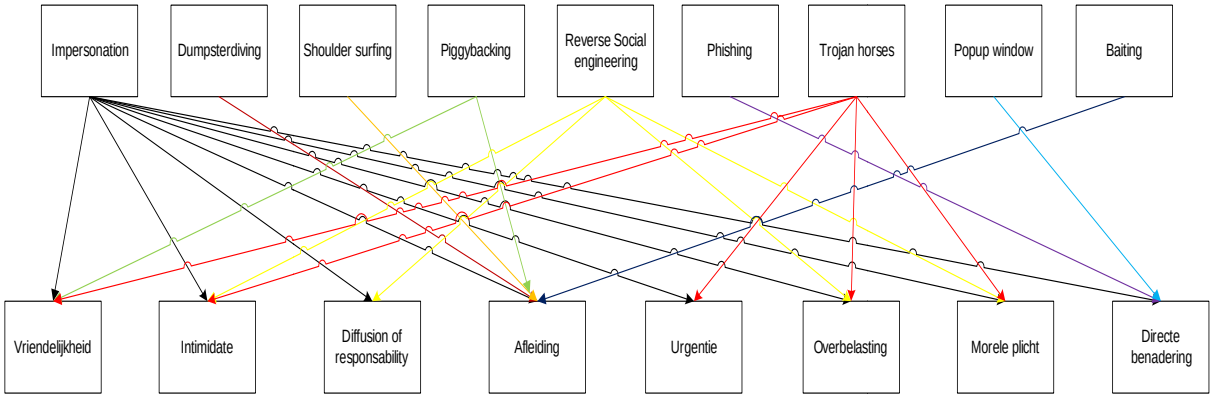
Piggybacking maakt vooral gebruik van vriendelijkheid en afleiding. Ongemerkt een gebouw binnen komen kan door vriendelijk te zijn en je voordoen als een medewerker of door voor afleiding te zorgen en vervolgens naar binnen te glippen.

Phishing en popup windows maken gebruik van de techniek directe benadering. Een doelwit wordt via een valse website en e-mail benaderd door de social engineer om een handeling uit te voeren. Dit geldt ook voor een popup window waarbij zonder omweg wordt gevraagd om een wachtwoord opnieuw in te voeren. Deze twee tactieken kunnen alleen gebruikt worden in combinatie met directe benadering en niet met andere technieken. Dit is vanwege het feit dat de andere technieken psychologisch van aard zijn en phishing en popup windows op computer of technologie gebaseerde tactieken zijn en hierdoor niet vatbaar zijn voor de meer psychologische technieken.

Bij trojan horses kunnen wel andere technieken gebruikt worden omdat de social engineer ervoor moet zorgen dat het doelwit de trojan horse op zijn of haar computersysteem zal installeren. Dit kan bijvoorbeeld gedaan worden door het vriendelijk te vragen of door middel van intimidatie.

Bij baiting kan met name gebruik worden gemaakt van afleiding. Door het doelwit af te leiden kan de social engineer ervoor zorgen dat het doelwit de vooraf neergelegde USB-sleutel opmerkt en deze vervolgens zal meenemen naar de werkplek om te kijken wat er op staat.

In de figuur 9 op de volgende pagina zijn de relaties tussen de social engineering tactieken en de psychologische technieken op een andere manier visueel weergegeven om zo de relatie te verduidelijken.



Figuur 9: Social engineering tactieken in relatie met de psychologische technieken

In de onderstaande tabel 4 is te zien welke eigenschappen beïnvloed kunnen worden door welke tactieken. Deze social engineering tactieken beïnvloeden de eigenschappen niet rechtstreeks maar via de technieken die bij de social engineering tactieken horen. Uiteraard bestaat er dan indirect wel een relatie tussen de tactieken en eigenschappen. Als bijvoorbeeld de tactiek dumsperdiving het best kan worden uitgevoerd via de techniek afleiding, dan wordt met het afleiden van een persoon ingespeeld op de eigenschap onverschilligheid. Dan moet er uiteraard wel een relatie bestaan tussen de tactiek dumpsterdiving en de techniek afleiding, tussen afleiding en de eigenschap onverschilligheid, alsmede ook een relatie met dumpsterdiving en onverschilligheid. Dit geldt dan voor alle tactieken, technieken en eigenschappen.

Eigenschappen / **Tactieken**	**Autoriteit**	**Commitment & consistentie**	**Sympathie**	**Reciprocation**	**Schaarste**	**Sociale zekerheid**	**Behulpzaamheid**	**Nieuwsgierigheid**	**Hebzucht**	**Onverschilligheid**	**Angst**	**Schuldgevoel**
1. Impersonation	X	X	X	X	X	X	X	X	X	X	X	X
2. Dumpsterdiving										X		
3. Shoulder surfing							X	X	X	X		
4. Piggybacking			X				X			X		
5. Reverse social engineering	X	X		X		X	X				X	X
6. Phishing							X	X			X	
7. Trojan horses	X		X				X	X	X	X	X	
8. Popup window										X		
9. Baiting								X	X	X		

Tabel 13: Social engineeringstactieken in relatie met de psychologische eigenschappen van de mens

Impersonation is een tactiek die net zoals op alle technieken, ook op alle gedefinieerde eigenschappen kan inspelen, afhankelijk van de rol die de social engineer zich aanmeet. Als de social engineer de rol van helpdesk medewerker aanneemt en contact opneemt met het doelwit met de vraag om een wachtwoord door te geven omdat de helpdesk dit wachtwoord voor iets nodig heeft, wordt er ingespeeld op de eigenschappen behulpzaamheid en onverschilligheid. Behulpzaamheid omdat de mens van nature behulpzaam is en onverschilligheid omdat het doelwit denkt daadwerkelijk met de helpdesk te maken heeft en hierdoor een nonchalante houding heeft en verder niet nadenkt over mogelijke gevolgen.

Dumpsterdiving heeft te maken met de onverschilligheid van de mens. Veel mensen denken niet na over wat voor waardevolle informatie ze weggooien zonder dit eerst te vernietigen.

Bij piggybacking en shoulder surfing zijn vooral de eigenschappen behulpzaamheid en onverschilligheid kwetsbaar.

Bij reverse social engineering wordt door de social engineer vaak een autoritair persoon gespeeld waardoor de eigenschappen autoriteit en angst beïnvloedbaar zijn.

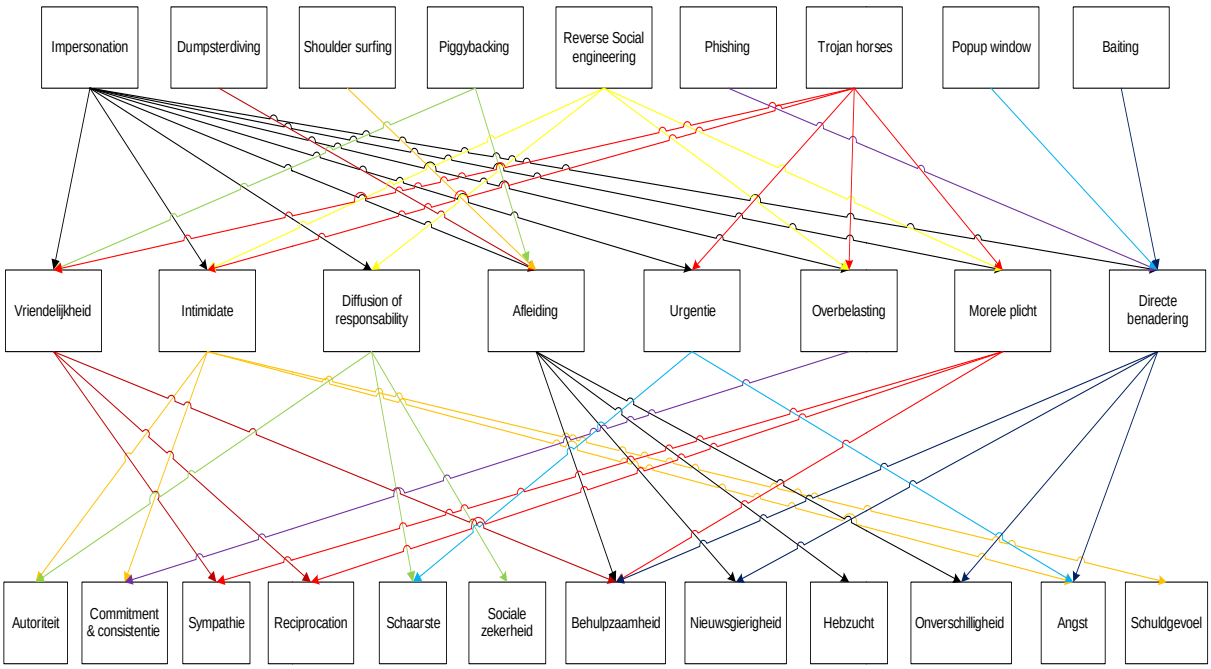
Phishing, trojan horses en popup windows spelen onder andere in op commitment en consistentie (als mensen gevraagd worden om een wachtwoord in te voeren in een voor hen vertrouwde applicatie of website, wordt dit meestal ook gedaan) en onverschilligheid. Mensen zijn heel vaak nonchalant en ontwetend wanneer via technologie wordt gevraagd om een handeling te verrichten.

De eigenschappen die bij baiting een rol spelen zijn nieuwsgierigheid, hebzucht en onverschilligheid. Als mensen een USB-sleutel vinden zijn mensen heel erg nieuwsgierig naar wat voor informatie er op die USB-sleutel bevindt. Mensen denken niet na over de gevolgen die het kan hebben wanneer er een gevonden en dus geen vertrouwde USB-sleutel in een computersysteem wordt gestoken.

In de onderstaande figuur 10 zijn de relaties tussen de social engineering tactieken en de psychologische eigenschappen op een andere manier visueel weergegeven om zo de relatie te verduidelijken.

Figuur 10: Social engineering tactieken in relatie met de psychologische eigenschappen

In figuur 11 is een totaal overzicht te zien van de relaties tussen de tactieken, technieken en eigenschappen.



Figuur 11: Relaties tussen social engineering tactieken, technieken en psychologische eigenschappen

3.4 Risicoanalyse door middel van attack trees

Nu in de vorige paragraaf de bedreigingen zijn uiteengezet die social engineering met zich meebrengen, is het verstandig om deze bedreigingen systematisch in kaart te brengen. Een manier om dit te doen is door gebruik te maken van attack trees. Deze term werd door Bruce Schneier in zijn artikel geïntroduceerd [SCHN99]. Attack trees verzorgen een formele, methodische manier om de beveiliging van systemen te beschrijven en geeft tegelijkertijd een helder beeld van de mogelijkheden van de aanvaller. Bij deze methode wordt er gekeken vanuit het oogpunt van de aanvaller: de aanvaller wil een bepaald doel bereiken (weergegeven in de wortel van de boom) en het doel kan op meerdere manieren bereikt worden (een nieuwe vertakking in de boom). Bovenin de boom (bij de wortel), bevindt zich het hoofddoel en er onder (bij de takken) staan de doelen die nodig zijn om het hoofddoel te halen (bij deze methode wordt de boom van boven naar onder gelezen). Een boogje bij een vertakking betekent dat alle doelen bereikt moeten worden. Als er geen boogje staat hoeven niet alle doelen bereikt te worden maar kan er een keuze tussen de doelen gemaakt worden.

Het voordeel van de attack tree methode is dat het gaat om een semi-formele methode. De boom drukt een formele relatie tussen verschillende aanvallen uit, maar de aanvallen zelf zijn uitgedrukt in natuurlijke taal. Hierdoor kan de gebruiker zelf bepalen welke mate van detaillering geschikt is. Een ander groot voordeel is dat tijdens het ontwikkelen van de attack tree, bijna onmiddellijk wordt nagedacht over eventuele maatregelen die de aanval kunnen keren [MAUW06]. Attack trees hebben een simpele hiërarchische structuur waardoor er snel

door de boom kan worden genavigeerd. Ook is het concept van attack trees snel en eenvoudig te begrijpen waardoor verschillende personen voordeel van een attack tree kunnen hebben of er zelf aan kunnen bijdragen. De simpele visuele representatie van de mogelijke bedreigingen maakt het gemakkelijk om een duidelijk beeld te krijgen van de situatie en kan de boom snel en eenvoudig worden uitgebreid wanneer er zich nieuwe dreigingen voordoen. Nog een ander voordeel is de herbruikbaarheid van takken (of delen ervan). Sommige situaties hebben namelijk te maken met dezelfde dreigingen, waardoor het herbruiken van takken kan resulteren in een vermindering van de kosten [OPEL05].

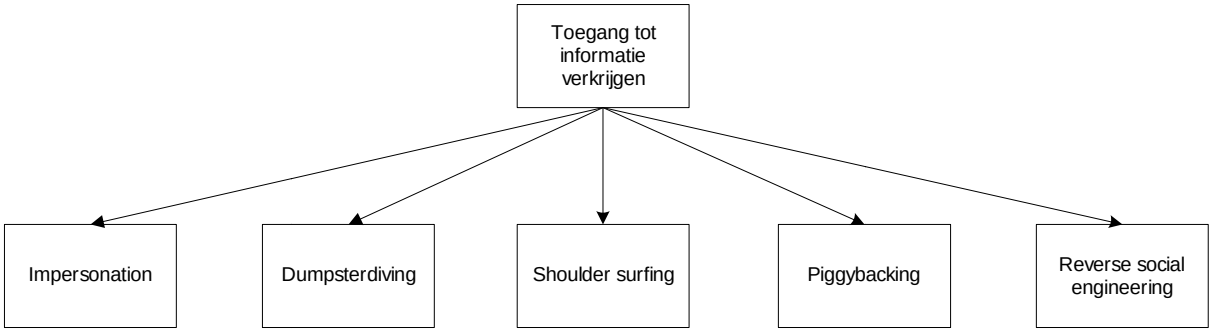
Wanneer eenmaal een concrete boom is opgesteld, kunnen er ook nog attributen worden toegewezen aan de verschillende doelen waardoor er berekeningen kunnen plaatsvinden om zodoende de veiligheid van het doel te berekenen. Een voorbeeld hiervan is om de attributen mogelijk en onmogelijk toe te wijzen, zodat snel eenvoudig kan worden gezien welke aanval het makkelijkst is om uit te voeren. Andere voorbeelden van attributen zijn: de kosten van een aanval, wel of geen speciaal gereedschap nodig, risico voor de aanvaller, additionele impact voor de verdediger, etc [MAUW05].

Attack trees zijn dus een uitstekend hulpmiddel om de bedreigingen van social engineering weer te geven. Door de aanvallen van social engineering te visualiseren kan snel en eenvoudig worden gezien waar de kwetsbaarheden en pijnpunten zitten van een organisatie als er een social engineering aanval plaatsvindt. De negen social engineeringstactieken uit de vorige paragraaf zijn het uitgangspunt van de attack tree aangezien dit de aanvallen zijn die een social engineer zal inzetten.

Er is gekozen om de boom op te splitsen in op mensen gebaseerde tactieken en op computer of technologische gebaseerde tactieken (net zoals gedaan is in paragraaf 3.3). Dit is gedaan omdat anders de boom wel heel erg onoverzichtelijk is. Ook is er voor gekozen om de boom op te delen per social engineering tactiek. De boom moet dus wel als één geheel worden gezien maar vanwege de overzichtelijkheid zijn de negen tactieken opgesplitst. Voor elke social engineeringstactiek is er dus een aparte boom en wordt er beschreven wat de tactiek inhoudt, welke dreigingen er zijn (en ook hoe groot de dreiging is) en welke bescherming nodig is.

3.4.1 Attack tree van de op mensen gebaseerde tactieken

Het eerste (bovenste) deel van de boom ziet er als volgt uit:



Figuur 12: Bovenste deel van de attack tree van de op mensen gebaseerde social engineeringstactieken

Het hoofddoel van social engineering is zoals beschreven in paragraaf 3.1.1 het verkrijgen van de gewenste informatie. Dit is het hoofddoel en bevindt zich dan ook bij de wortel van de boom. Dit hoofddoel kan dan bereikt worden door de 5 takken eronder (de social engineering tactieken).

3.4.1.1 Impersonation

De attack tree van de impersonation tactiek wordt als volgt weergegeven:

Figuur 13: Attack tree van de impersonation tactiek

Impersonation is een social engineering aanval die onder social engineers populair is. Deze aanval kan via de telefoon of face-to-face plaats vinden. De aanval via de telefoon uitvoeren is veel minder riskant dan je fysiek voordoen als iemand anders. Je hebt immers direct contact met je doelwit waardoor de kans groter is dat de aanval niet zal slagen. Het doelwit kan sneller achterdochtig worden wanneer de aanval bijvoorbeeld niet goed wordt uitgevoerd. Via de telefoon is het mogelijk om snel de verbinding te verbreken. Wanneer het gaat om informatie

zoals wachtwoorden of ander niet-tastbare informatie wordt de aanval vaak telefonisch uitgevoerd. Wanneer de gewenste informatie wel tastbaar is, zal de aanval meestal op een directe manier, via een face-to-face gesprek, plaatsvinden

De social engineer meet zich een bepaalde rol aan, bijvoorbeeld die van een manager. Informatie over het doelwit verzamelen kan op een aantal manieren. De meest voorkomende manier is om op het internet op zoek te gaan naar relevante informatie. Op veel websites van bedrijven kan informatie over personen worden gevonden, denk hierbij aan telefoonnummers en e-mailadressen. Daarnaast kan op sociale netwerken zoals hyves en facebook veel privé informatie worden ingewonnen dat door social engineers kan worden gebruikt in hun aanval. Andere manieren om aan informatie te komen is via derden (via collega's bijvoorbeeld) of via de social engineeringaanval dumpsterdiving (zie verderop in deze paragraaf). Deze laatste twee manieren zullen minder snel gebruikt worden om aan informatie te komen omdat het meer voorbereiding vereist en veel complexer is. Ook gaan er meer tijd en kosten aan vooraf dan wanneer er naar informatie op internet wordt gezocht.
Om vervolgende de gewenste informatie te krijgen kan de social engineer het doelwit opbellen en zich hierbij voordoen als een manager van een bepaalde afdeling. Door gebruik te maken van intimidatie en daarna vervolgens autoriteit uit te stralen en daadkrachtig over te komen is het doelwit geneigd om de gevraagde informatie te verstrekken. Vooral wanneer dit bijvoorbeeld gedaan wordt met een bepaalde vorm van urgentie. Als de social engineer het doelwit laat geloven dat de gewenste informatie snel verkregen moet worden (dit werkt vooral met intimidatie en de bijbehorende autoritaire uitstraling), is de kans groter dat het doelwit de informatie aan de social engineer zal meegeven.

Afhankelijk van de rol die de social engineer aanneemt, kan gekozen worden welke aanpak het beste is: door simpelweg gewoon vriendelijk te zijn en het te vragen of door intimidatie en de informatie op te eisen. De aanpak van directe benadering is ook een mogelijkheid maar heeft vaak de minste kans van slagen omdat de social engineer het doelwit zonder bepaalde techniek benadert en gewoon om de gewenste informatie vraagt.

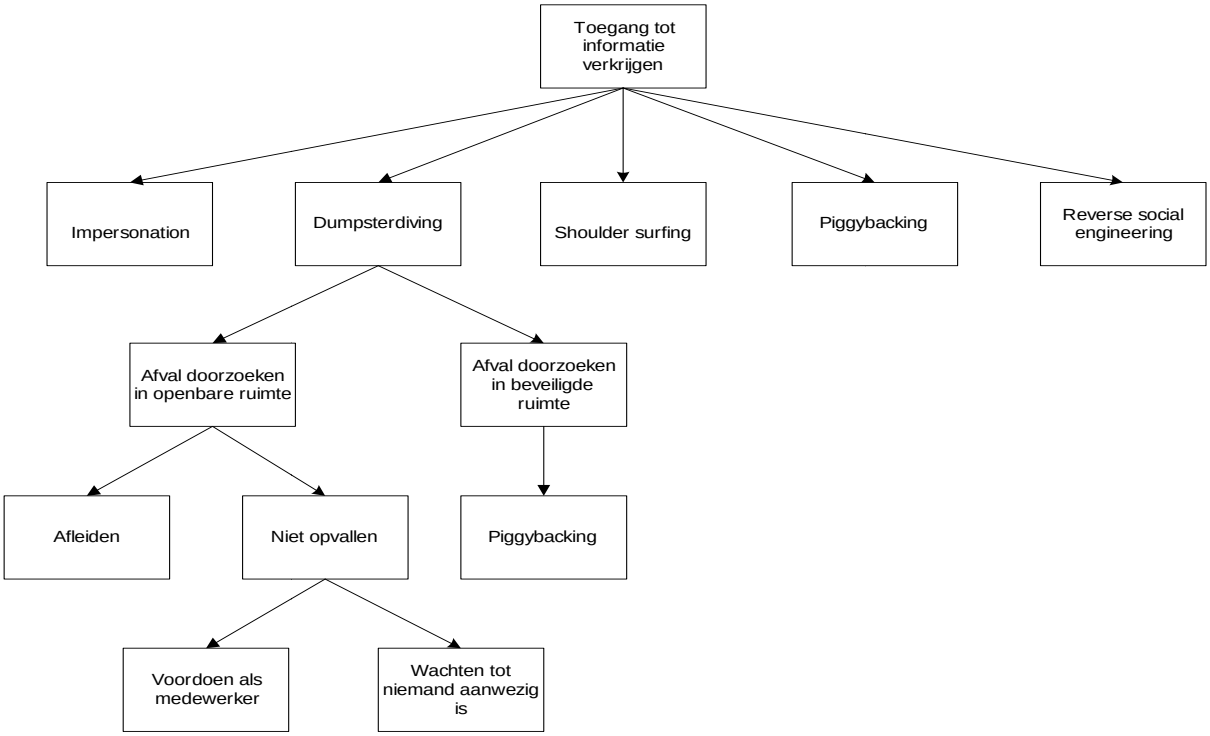
Dreiging
Deze tactiek is een methode die door social engineers vaak gebruikt wordt. Er gaat een grote dreiging van uit omdat deze tactiek relatief makkelijk is uit te voeren, de social engineer geen specialistische kennis hoeft te bezitten en er geen hoge kosten aan verbonden zitten. Wel kan het een zeer tijdrovende klus zijn omdat er namen en telefoonnummers achterhaald moeten worden en de social engineer zal zich moeten inleven in de rol die hij of zij moet gaan spelen. Wat deze tactiek nog meer dreigend maakt is het feit dat als het bij medewerker A niet lukt om de gewenste informatie afhandig te maken, het gewoon bij medewerker B kan worden geprobeerd. Mocht het nog steeds geen succes opleveren, dan kan het bij medewerker C worden geprobeerd. Deze tactiek kan net zo lang worden uitgevoerd tot een medewerker de informatie weggeeft. Er zijn immers vaak genoeg medewerkers om het bij te proberen. Daarnaast is er bij medewerkers nog een dreiging die van groot belang is, namelijk de laksheid in het omgaan met informatie. Zoals eerder in dit hoofdstuk beschreven, zijn er een aantal psychologische eigenschappen die mensen bezitten. Onverschilligheid is er één van en de nonchalance en onwetendheid van mensen in het omgaan met informatie ie iets wat bij veel mensen aardig zit ingebakken. Social engineers weten dit en spelen hierop in waardoor er een grote kans van slagen voor deze tactiek is.

Bescherming
Medewerkers zullen zorgvuldig met de informatie moeten omgaan. Hoewel voor deze tactiek geen specifieke maatregelen zijn, kan er wel voor gezorgd worden dat de kans van slagen van de impersonation tactiek miniem is. Het belangrijkste is om een bewustzijn bij medewerkers te kweken. Het belang van veiligheid van informatie moet duidelijk zijn en dat moet uiteindelijk resulteren in het veilig omgaan met informatie en dus niet zomaar deze informatie aan derden verstrekken. Een veiligheidsbewustzijn hebben is de allerbelangrijkste maatregel in de informatiebeveiliging, weten wat te doen met informatie en misschien vooral wat niet te doen met bepaalde informatie.
Wat ook altijd aanwezig moet zijn is een helder en duidelijk informatie beveiligingsbeleid waarin wordt aangegeven hoe moet worden omgegaan met (gevoelige en vertrouwelijke) informatie en wat de consequenties zijn wanneer informatie wordt weggegeven. Zo kan een maatregel zijn wanneer er om bepaalde informatie door een persoon wordt gevraag om deze persoon is eerst terug te bellen voordat de informatie wordt verstrekt. Zo kan worden gecheckt om te kijken of deze persoon daadwerkelijk is wie hij of zij zegt te zijn. Ook nummer herkenning kan bij het tegengaan van deze tactiek helpen.
Een medewerkers zal dus nooit zomaar informatie moeten weggeven zonder de zekerheid te hebben dat de persoon die om de informatie vraagt, de persoon is die hij of zij zegt te zijn. Ook al is die persoon nog zo vriendelijk of intimiderend, zonder absolute zekerheid te hebben over de identiteit van deze persoon, moet bepaalde informatie nooit aan derden worden verstrekt.

Kortom, het belangrijkste is om medewerkers bewust te maken van de eigen verantwoordelijkheid in het omgaan met informatie die vertrouwelijk en gevoelig van aard kan zijn. Dit is overigens niet iets wat alleen voor deze tactiek geldt, maar is een maatregel die eigenlijk voor alle social engineeringstactieken van belang is. Maar dit is een aspect dat in het volgende hoofdstuk uitgebreid belicht wordt.

3.4.1.2 Dumpster diving

De attack tree van de dumpster diving tactiek wordt als volgt weergegeven:



Figuur 14: Attack tree van de dumpster diving tactiek

Het doorzoeken van afval is een handige methode om aan informatie te komen. Vaak wordt informatie niet vernietigd wanneer het wordt weggegooid, terwijl het een kleine moeite is om een papierversnipperaar te gebruiken. Social engineers weten dit en gokken erop dat bij veel organisaties informatie niet vernietigd wordt. Afval kan zich bij organisaties op twee plekken bevinden: in een afgesloten (beveiligde) ruimte of in een ruimte dat voor iedereen toegankelijk is (openbare ruimte). Als een organisatie de containers met afval in een openbare ruimte plaatst is het een koud kunstje om deze te doorzoeken. De social engineer kan dan voor afleiding kiezen om ervoor te zorgen dat er ongehinderd naar informatie kan worden gezocht of door simpelweg niet op te vallen. Dit is mogelijk door je bijvoorbeeld voor te doen als een medewerker en vervolgens op zoek te gaan naar informatie. Een andere optie is om te wachten totdat niemand aanwezig en dan vervolgens op zoek te gaan naar informatie. Wanneer afvalcontainers zich in een afgesloten ruimte bevinden, zal de social engineer eerst toegang tot deze ruimte moeten krijgen. Dit kan door middel van piggybacking. De attack tree van piggybacking staat verderop beschreven in deze paragraaf. Als vervolgens toegang tot de afgesloten ruimte is verkregen via piggybacking, gelden de mogelijkheden uit de attack tree die er zijn omtrent het doorzoeken van afval in een openbare ruimte.

Dreiging

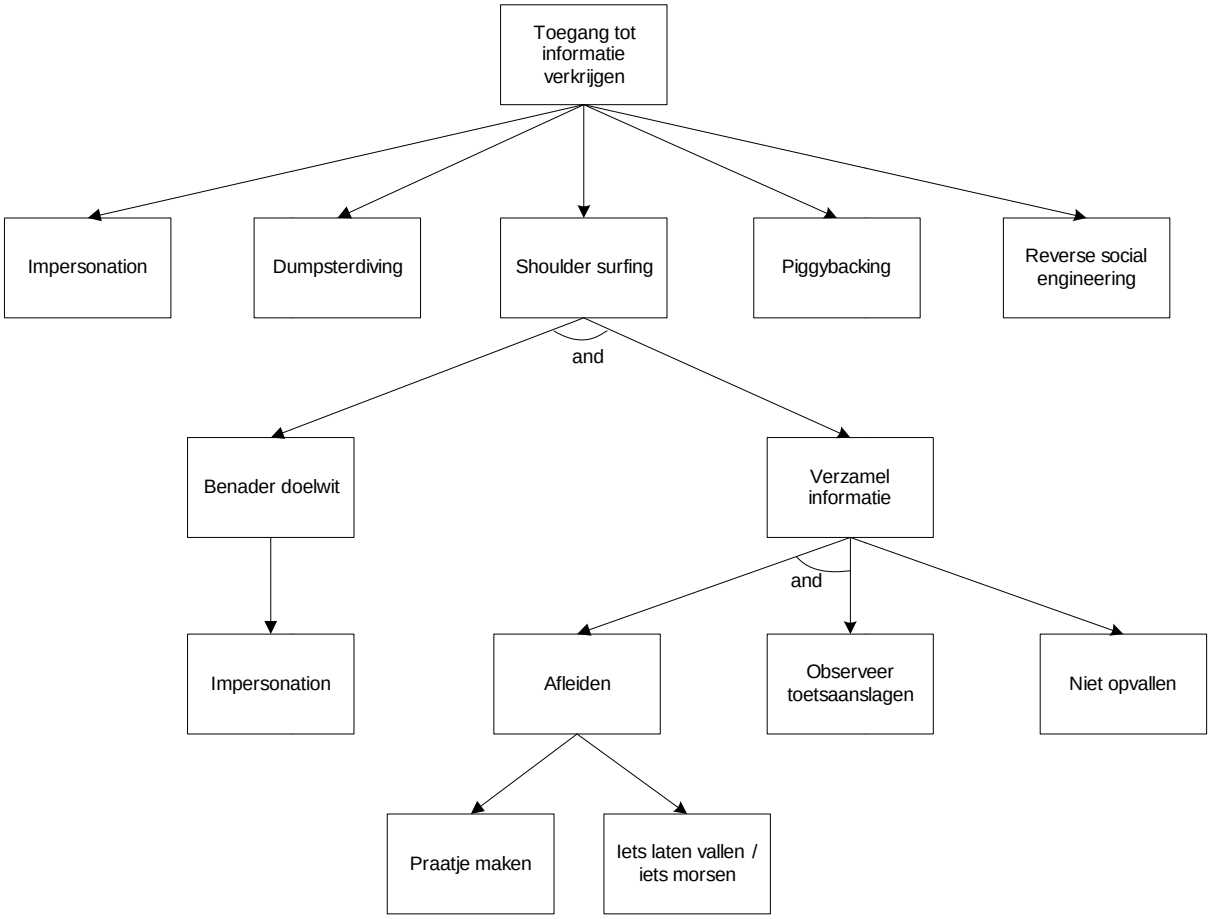
De dreiging van deze aanval zit hem in het feit dat met informatie vaak nonchalant wordt omgegaan. Vertrouwelijke en gevoelige informatie moet natuurlijk altijd vernietigd worden voordat het wordt weggegooid. Dit wordt niet altijd gedaan waardoor er de kans is dat deze informatie in verkeerde handen valt. Toch lijkt deze aanval geen al te grote kans van slagen te hebben omdat er redelijk wat moeite gedaan moet worden om toegang tot die informatie te

krijgen. Daarnaast weet de social engineer niet of er daadwerkelijk informatie tussenzit die van belang kan zijn en of die informatie wel of niet vernietigd is.

Bescherming
Deze aanval kan redelijk eenvoudig worden tegengegaan door afvalcontainers altijd in afgesloten ruimtes neer te zetten en informatie te allen tijde te vernietigen. Dit is ook iets wat in het informatie beveiligingsbeleid te allen tijde moet worden opgenomen. Een extra maatregel kan ook zijn om het afval te laten ophalen door gespecialiseerde vernietigingsbedrijven.

3.4.1.3 Shoulder surfing

De attack tree van de shoulder surfing tactiek wordt als volgt weergegeven:



Figuur 15: Attack tree van de shoulder surfing tactiek

Door informatie te verkrijgen via shoulder surfing moet het doelwit benaderd worden om de informatie te kunnen verzamelen. Het benaderen kan gedaan worden door bijvoorbeeld de impersonation aanval toe te passen en een rol aan te nemen van bijvoorbeeld een collega. Het verzamelen van de informatie kan gedaan worden op twee manieren: door middel van afleiding en vervolgens het observeren van de toetsaanslagen . Het afleiden van het doelwit is mogelijk door een conversatie te starten of door iets te laten vallen. De andere manier is door niet op te vallen en daardoor de informatie te verzamelen. Shoulder surfing is een methode dat vaak gebruikt wordt om een wachtwoord te achterhalen.

Dreiging

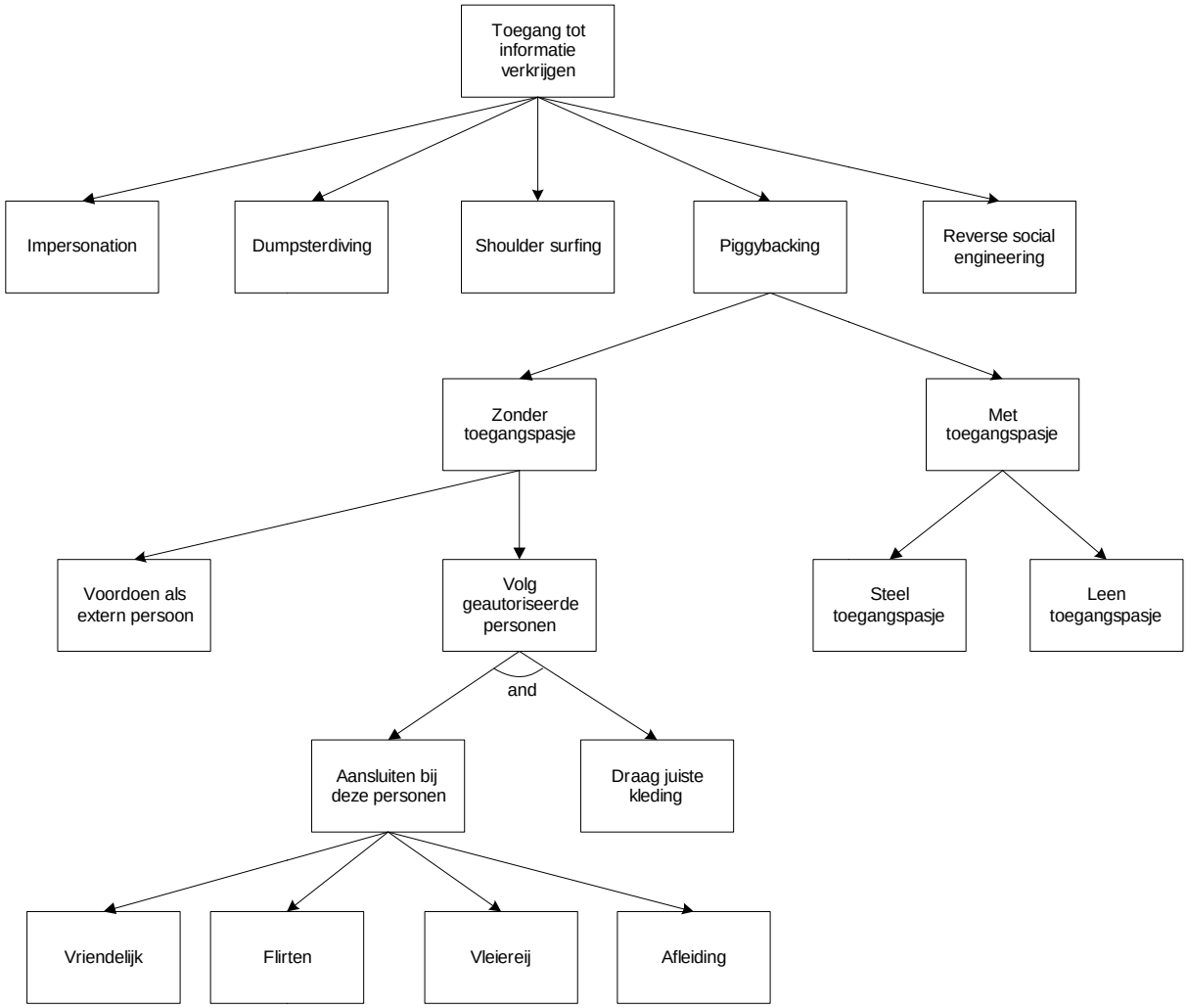
Deze aanval lijkt net als dumpster diving geen al te grote dreiging te hebben. De social engineer is van te veel factoren afhankelijk. Zo zal de social engineer in direct contact moeten komen met zijn slachtoffer door middel van de impersonation aanval. Hierdoor is er een groter risico om door de mand te vallen en tevens moet de social engineer er ook voor zien te zorgen dat het doelwit niet oplet bij het invoeren van het wachtwoord.

Bescherming

De bescherming tegen deze aanval is lastig. De oplettendheid en de bewustwording van het doelwit is van grote invloed bij deze aanval.

3.4.1.4 Piggybacking

De attack tree van de piggybacking tactiek wordt als volgt weergegeven:



Figuur 16: Attack tree van de piggybacking tactiek

Piggybacking zorgt ervoor dat de social engineer toegang tot een gebouw of ruimte krijgt om op zoek te gaan naar informatie. In de meeste gevallen heeft de social engineer geen toegangspasje om een gebouw binnen te kunnen gaan. Een manier om dan toch binnen te geraken is om geautoriseerde personen te volgen die wel toegang hebben. Een effectieve manier om dit te doen is wanneer medewerkers terugkomen van een lunch of als medewerkers buiten met een groepje staan te roken. De social engineer probeert dan binnen te komen door zich bij deze personen op te houden en aan te sluiten wanneer deze personen het gebouw binnengaan. Daarbij is het van belang dat de social engineer kleding draagt waaruit blijkt dat hij of zij in het gebouw hoort te zijn. Een andere manier voor een social engineer is om je voor te doen als een extern persoon. Hierbij kan gedacht worden aan een persoon die de brandblussers komt vervangen of een persoon die de frisdrankautomaten komt bijvullen. Hierdoor kan de social engineer ook vrij toegang tot een gebouw krijgen.

Dreiging

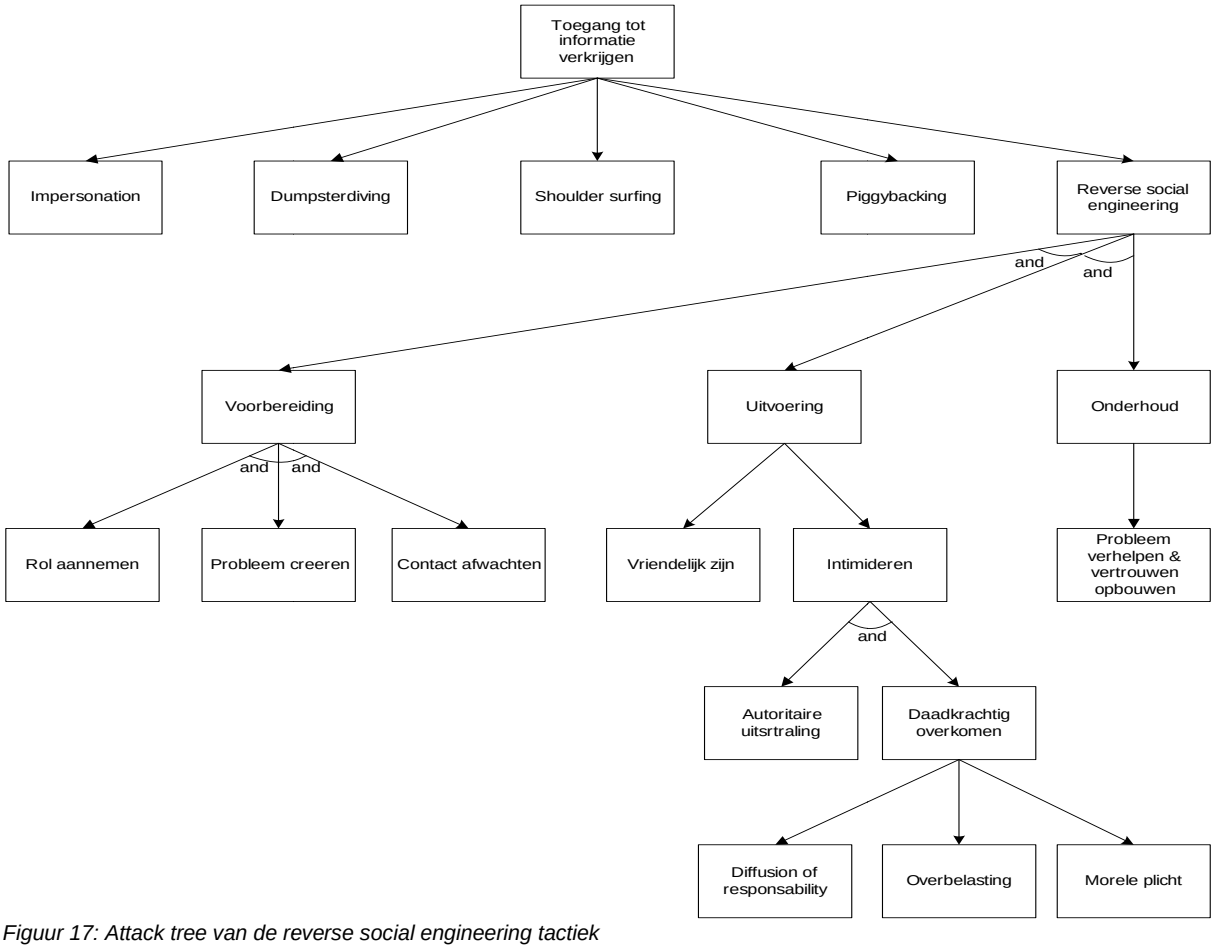
Het doel van deze aanval is om in een gebouw binnen te komen en vrij te kunnen bewegen om zo op zoek te gaan naar informatie. Deze aanval heeft een vrij grote dreiging. Het is vaak

niet moeilijk om voor een bedreven social engineer toegang tot een gebouw te krijgen. Wanneer de social engineer zich in het gebouw bevindt kan hij of zij op zoek gaan naar informatie zoals wachtwoorden die op bureaus rondslingeren of op computerschermen zitten geplakt.

Bescherming
Het is mogelijk om je tegen deze aanval te beschermen, hoewel het moeilijk is en ook weer van factoren afhankelijk is. Medewerkers moeten er op geducht zijn om niet zomaar iemand mee naar binnen te laten gaan. Zeker niet als deze persoon geen identificatiepasje heeft en waarvan met het idee heeft dat hij of zij niet in het gebouw behoort te zijn. Ook moet er voor gezorgd worden dat personen die in het gebouw iets komen doen, altijd door een medewerker worden begeleidt en niet alleen worden gelaten. Ook de bewustwording van medewerkers speelt hierin een grote rol. Nooit wachtwoorden opschrijven en rond laten slingeren en mensen aanspreken waarvan je vermoedt dat ze er niet horen te zijn.

3.4.1.5 Reverse social engineering

De attack tree van de reverse social engineering tactiek wordt als volgt weergegeven:



Figuur 17: Attack tree van de reverse social engineering tactiek

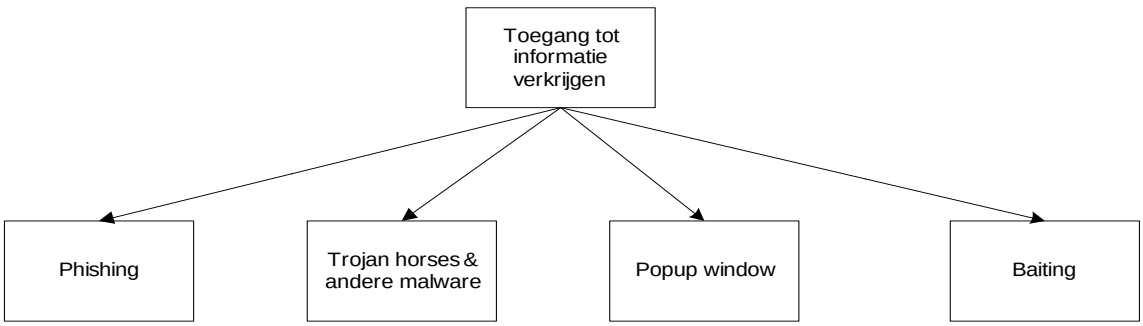
Bij reverse social engineering initieert het doelwit het contact en niet de social engineer. Om dit te bereiken moet de social engineer zich goed voorbereiden. De social engineer zal een rol moeten aannemen en een passend probleem moeten creëren. Dit probleem moet ervoor zorgen dat het doelwit contact opneemt met de social engineer die zich dan voordoet als de rol die hij of zij zich eerder heeft aangemeten. Wanneer het doelwit contact zoekt met de social engineer begint de uitvoering van deze tactiek. Het doelwit neemt contact met de social engineer op om het probleem te verhelpen. De social engineer kan dan kiezen (afhankelijk van de rol die wordt gespeeld) om vriendelijk te zijn of intimiderend. In de meeste gevallen zal de keuze op intimidatie vallen omdat de social engineer vaak de rol bekleedt van een hoge manager. Wanneer het contact gelegd is, start de onderhoud van deze tactiek en wordt het probleem verholpen en wordt er eventueel een vertrouwensrelatie opgebouwd met het doelwit.

Dreiging
De dreiging van deze aanval lijkt niet al te groot. Er gaat heel veel voorbereiding in deze aanval zitten en de social engineer is enorm afhankelijk van het doelwit om deze aanval te laten slagen. Als het de social engineer namelijk niet lukt om contact met het doelwit te krijgen, zal deze aanval niet slagen. Wanneer het echter wel lukt om deze aanval op te zetten en te laten slagen, dan is de dreiging een stuk hoger aangezien het doelwit de social engineer dan vertrouwt. Er kan dan sprake zijn van een vertrouwensrelatie tussen de social engineer en het doelwit, wat kan leiden tot nog grotere schade.

Bescherming
De bescherming van deze aanval is volledig afhankelijk van het veiligheidsbewustzijn van het doelwit. Wanneer dit niet aanwezig is en het doelwit onverschillig en nonchalant omgaat met de informatie, zijn er geen maatregelen om deze aanval tegen te gaan.

3.4.2 Attack tree van op technologie of computer gebaseerde tactieken

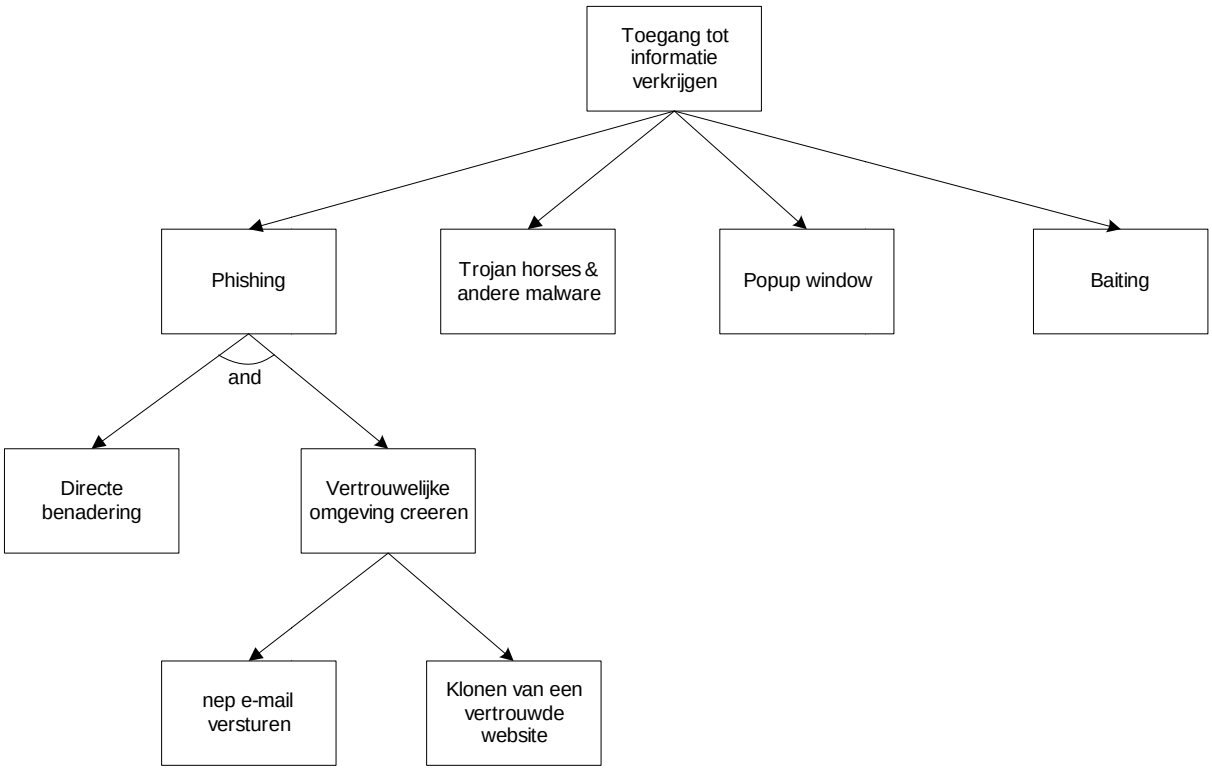
Het eerste (bovenste) deel van de boom ziet er als volgt uit:



Figuur 18: Bovenste deel van de attack tree van de op technologie of computer gebaseerde social engineeringstactieken

3.4.2.1 Phishing

De attack tree van de phishing tactiek wordt als volgt weergegeven:



Figuur 19: Attack tree van de phishing tactiek

Een phising aanval kan op twee manieren plaatsvinden, door middel van een valse e-mail of via een gekloonde website. Een phishing aanval via een gekloonde website moet ervoor zorgen dat er een situatie ontstaat dat door het doelwit als vertrouwelijk wordt ervaren en er daardoor voor zorgt dat het doelwit informatie invoert op de website en dus in handen van de social engineer terecht komt. Een phishing aanval via een valse e-mail is een eenvoudigere methode dan het klonen van een website. Deze valse e-mail moet ervoor zorgen dat de boodschap van de e-mail door het doelwit voor waar wordt aangenomen en ook vertrouwt. Wanneer dit het geval is, is het mogelijk dat het doelwit op de e-mail reageert en zijn of haar wachtwoord prijsgeeft.

Bedreiging

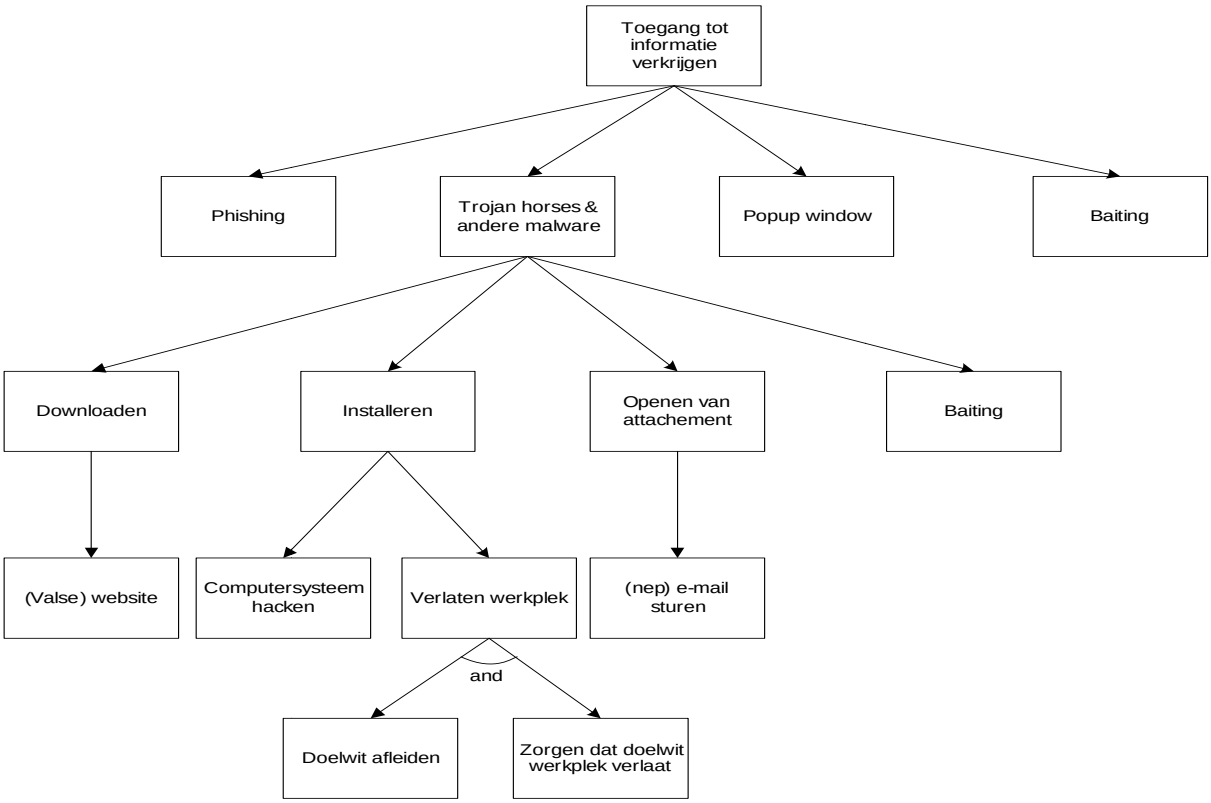
Een social engineeringsaanval door middel van phishing heeft een grote dreiging. Als een social engineer er in slaagt om een website perfect na te maken en er tegelijk ook voor kan zorgen dat het doelwit op de nagemaakte website terecht komt, is de kans heel goot dat het doelwit inlogt op deze website en dus informatie (wachtwoord) prijsgeeft. Ook bij phishing door middel van een valse e-mail is de dreiging groot. Hoewel de kans van slagen minder is, blijft er wel een grote dreiging bestaan. Dit komt met name omdat met deze aanval heel veel mensen tegelijk kunnen worden benaderd. Stel dat een bedrijf met meer dan 100 medewerkers

allemaal een valse e-mail ontvangen (zogenaamd van de helpdesk) met daarin de vraag of ze het wachtwoord van hun account willen terug mailen. Er hoeft maar één medewerker te zijn die dit gelooft en de e-mail beantwoord met daarin het wachtwoord van zijn of haar account. De schade kan dan aanzienlijk zijn omdat slechts één persoon zich niet bewust is van het gevaar.

Bescherming
Ook de bescherming tegen deze aanval is sterk afhankelijk van het veiligheidsbewustzijn van de mens. Het informatie beveiligingsbeleid kan hierin helpen door medewerkers er op te wijzen dat er nooit om een wachtwoord zal worden gevraagd. Medewerkers moeten weten dat ze ten alle tijd hun wachtwoord nooit moeten prijsgeven.

3.4.2.2 Trojan horses & andere malware

De attack tree van de trojan horses tactiek wordt als volgt weergegeven:



Figuur 20: Attack tree van de trojan horses & andere malware tactiek

Het doel van deze tactiek is ervoor te zorgen dat informatie wordt verkregen door middel van het infecteren van het computersysteem van het doelwit door middel van een trojan horse. Dit kan gedaan worden op een viertal manieren. Het doelwit kan de trojan horse downloaden van een (valse) website. De social engineer kan de trojan horse installeren door het

computersysteem te hacken of zelf te installeren wanneer het doelwit niet aanwezig is. De derde manier is via het openen van een attachement in een e-mail. De laatste manier is via baiting, wat gezien kan worden als een aparte social engineeringsaanval en hierdoor een eigen attack tree heeft (zie verderop in deze paragraaf).

Dreiging
Deze social engineeringsaanval heeft een redelijk grote dreiging omdat deze aanval op verschillende manieren kan plaatsvinden. De dreiging van deze aanval kan sterk verminderd worden wanneer de technische infrastructuur (firewall, virusscanner, etc.) goed in orde is. Dit zal de dreiging niet helemaal afvangen omdat ook de mens een rol in deze aanval speelt. Wanneer een medewerker volledig vertrouwt op de aanwezige techniek, is de kans aanwezig dat zijn of haar eigen handelingen ervoor kunnen zorgen dat de techniek helaas niet afdoende is.

Bescherming
Om te beginnen moet ervoor gezorgd worden dat de technische infrastructuur helemaal up-to-date is. Dat wil zeggen, virusscanners, firewalls, computersysteem van de medewerkers, allemaal moet dat 100% in orde zijn. Daarnaast moet er bewustwording worden gekweekt bij de mensen dat techniek alleen niet voldoende, maar dat ook zij een belangrijke rol spelen in het informatie beveiligingsproces.

3.4.2.3 Popup window

De attack tree van de trojan horses tactiek wordt als volgt weergegeven:

Figuur 21: Attack tree van de popup window tactiek

De popup window tactiek lijkt sterk op de phishing tactiek met als dat verschil dat de social engineer ervoor zorgt dat er een pup scherm op het computerscherm van het doelwit verschijnt. Net als bij phishing moet ook hier een situatie worden gecreëerd dat natuurlijk en vertrouwelijk overkomt bij het doelwit zodat nietsvermoedend informatie wordt ingevoerd en weggeven.

Dreiging
De dreiging lijkt minder groot dan bij de phishing aanval omdat het een voorbereiding vereist met veel technische kennis. De social engineer moet er namelijk voor zorgen dat op het computersysteem van het doelwit een scherm verschijnt, en wat tegelijk ook nog een natuurlijk en vertrouwelijk overkomt.

Bescherming
Het hebben en kweken van een veiligheidsbewustzijn is ook hier de grootste maatregel tegen een aanval zoals deze. Wanneer iemand met een dergelijke aanval te maken krijgen, moet er een lampje gaan branden dat er iets niet helemaal pluis is.

3.4.2.4 Baiting

De attack tree van de baiting tactiek wordt als volgt weergegeven:

Figuur 22: Attack tree van de baiting tactiek

Het verkrijgen van informatie via baiting is een tactiek dat vooral afhangt van de nieuwsgierigheid van het doelwit. De social engineer zal een digitale gegevensdrager (zoals een USB-sleutel) infecteren met bijvoorbeeld een keylogger. Vervolgens wordt deze geïnfecteerde gegevensdrager door de social engineer neergelegd op een strategische plaats (een plek waar het doelwit zeker te weten komt). Tot slot moet er door de social engineer voor worden gezorgd dat de geïnfecteerde gegevensdrager ook daadwerkelijk wordt meegenomen. De gegevensdrager moet er daardoor interessant uitzien voor het doelwit en zal het doelwit moeten worden afgeleidt zodat de gegevensdrager wordt opgemerkt.

Dreiging
Deze aanval heeft een grote dreiging omdat er een grote kans van slagen is. De mens is van nature uit erg nieuwsgierig en wanneer iemand een USB-stick ziet liggen, zit het in de aard van de mens om te willen weten wat er op staat. Hierdoor heeft deze aanval grote kans van slagen.

Bescherming
Jezelf beschermen tegen deze aanval is zeer lastig. Wanneer je een USB-stick vindt, verwacht je niet dat deze expres is neergelegd met kwade bedoelingen. Het is volkomen logisch dat mensen de USB-stick gaan bekijken om te zien of het mogelijk is om te achterhalen van wie de USB-stick is. Hier maatregelen tegen treffen is zeer lastig en dus is het moeilijk om een adequate bescherming tegen deze aanval te vinden.

3.5 Een verdediging tegen social engineering

In de vorige paragraaf is heel kort aan bod gekomen hoe je jezelf tegen social engineering kunt beschermen. In deze paragraaf wordt hier uitgebreider aandacht aan besteedt.

Om ervoor te zorgen dat een social engineer niet succesvol wordt in het verkrijgen van vertrouwelijke en gevoelige informatie, zullen er maatregelen moeten worden toegepast die de aanvallen en tactieken van de social engineer tegengaan. De typische technische hacker onderscheidt zich op één punt met de social engineer en dat is namelijk het aantal medewerkers die betrokken raken bij de aanval. In de gebruikelijke technische aanval van de hacker, worden vaak alleen de mensen van de IT afdeling betrokken, terwijl in een social engineeringaanval iedereen kan worden betrokken. Niet iedereen binnen een organisatie heeft technische kennis en is up-to-date met het bewustzijn van beveiliging. In [GRAN01] stelt Granger het volgende voor:

> *In order to be successful, organizations must make computer security part of all jobs, regardless of whether the employees use computers. Everyone in the organization needs to understand exactly why it is so crucial for the confidential information to be designated as such, therefore it benefits organizations to give them a sense of responsibility for the security of the network.*

In feite impliceert dit dat training en opleiding uiterst belangrijk zijn in de verdediging tegen social engineeringaanvallen. Eén van de belangrijkste verdedigingen tegen social engineering is om te weten wanneer je wordt aangevallen. Hoewel er geen gegarandeerde manier is om volledig een social engineering aanval tegen te gaan, kan wel het risico worden tegengegaan en geprobeerd worden om de schade zoveel mogelijk te minimaliseren. Dit komt neer op het

hebben van een veiligheidsbewustzijn (security awareness). In het volgende hoofdstuk zal dit aspect worden besproken.

3.5.1 Een verdediging tegen social engineering op meerdere niveau's

David Gragg beschrijft in [GRAG02] een methode die bestaat uit verschillende lagen om een social engineering aanval tegen te gaan. Graag beschrijft dat volgens hem de sleutel tegen die aanvallen is om de kwetsbaarheden en de dreigingen vast te stellen om vervolgens de verdediging op te bouwen tegenover die risico's. Deze verdediging moet bestaan uit zes verschillende lagen (die in deze paragraaf worden beschreven) van bescherming zodat als een social engineer er in slaagt om een laag door te dringen, er andere lagen zijn waar de aanval kan worden gestopt.

1. **Foundation level: Security policy addressing social engineering**

Een gebouw staat niet zonder een sterk en stabiel fundament. Het fundament van informatiebeveiliging is het beleid. Het beveiligingsbeleid geeft het niveau van de beveiliging van een netwerk aan. Het beleid wordt doorslaggevend wanneer het bescherming moet bieden tegen social engineering. Social engineering richt zich op mensen die moeten weten hoe ze moeten reageren op twijfelachtige verzoeken. Het beleid moet gebruikers helpen om een verzoek van een social engineer te herkennen en zich vervolgens tegen dit verzoek te kunnen verzetten. Gebruikers moeten niet in een positie gebracht worden waar ze moeten nadenken of er wel of niet informatie kan worden weggegeven. Het moet op voorhand goed gedefinieerd zijn door mensen die serieus hebben nagedacht over de waarde van informatie. Het beveiligingsbeleid moet een aantal gebieden aanduiden om een fundament te kunnen zijn in het tegengaan van social engineering. Toegang controle mechanismen voor informatie, het opzetten van accounts, het veranderen van wachtwoorden, maar ook sloten, identiteiten en het vernietigen van papier zouden onder andere moeten worden aangeduid. Het beleid moet een ingebouwde discipline hebben en moet vooral worden afgedwongen.

Het beleid tegen social engineering helpt medewerkers zich te verdedigen tegen de verschillende psychologische technieken die kunnen worden gebruikt. Het duidt ook de verantwoordelijkheid aan voor informatie of toegang dat wordt weggegeven, zodat er geen onduidelijkheid is dat het voor de gebruiker een eigen risico is om informatie of toegang weg te geven.

2. **Parameter level: Security awareness training for all users**

Wanneer het beveiligingsbeleid is opgezet en goedgekeurd, moeten alle medewerkers worden getraind in beveiligingsbewustzijn (awareness). Het beveiligingsbeleid zorgt voor richtlijnen en motivatie voor de training. Beleid waar goed over is nagedacht en vervolgens aan medewerkers is geleerd, kan het verschil maken in hoe medewerkers reageren op bepaalde verzoeken.

Medewerkers moeten weten wat voor soort informatie een social engineer kan gebruiken en welke conversaties verdacht zijn. Medewerkers moeten weten hoe ze vertrouwelijke informatie moeten herkennen en moeten ook begrijpen dat het hun verantwoordelijkheid is om het te beschermen. Alle medewerkers moeten zich bewust zijn van de signalen die in een social

engineering aanval zitten. Geen contact informatie geven, intimidatie, rare vragen en het vragen naar vertrouwelijke informatie kunnen van die signalen zijn. Ook moeten medewerkers zich ervan bewust zijn dat een goede social engineer eerst een relatie gebaseerd op vertrouwen wil opbouwen. Vervolgens zal deze relatie worden uitgebuit om allerlei waardevolle informatie te krijgen.

Er zijn een aantal elementen in de training die alle gebruikers moeten onthouden:

- **Weten wat de waarde is**: de meeste mensen onderwaarderen hun data en toegang voordat ze worden gehackt. Mensen moeten zich van te voren afvragen wat ze zouden doen als ze geen toegang meer hebben tot hun computer en dus niet meer bij hun informatie kunnen. De waarde van de informatie moet van te voren duidelijk zijn.

- **Vrienden zijn niet altijd vrienden**: Vrienden die over de telefoon allerlei vragen stellen over vertrouwelijke en gevoelige informatie, hoeven helemaal geen vrienden te zijn. Gebruikers moeten zich ervan bewust zijn dat als iemand overkomt als een vriend, dit niet betekent dat ze kunnen worden vertrouwd met bepaalde informatie.

- **Wachtwoorden zijn persoonlijk**: Social engineers kunnen met overtuigende redenen komen om gebruikers hun wachtwoord weg te geven aan compleet onbekenden. Zonder training geven mensen te snel hun wachtwoord weg.

- **Uniformen zijn goedkoop**: een social engineer kan bij een gebouw komen en zich voordoen als iemand met een legitieme reden om hier daadwerkelijk te zijn. Het aantrekken van een uniform geeft in veel gevallen toegang tot een gebouw. Het is belangrijk dat medewerkers worden getraind om iemand in uniform niet zomaar toe te laten.

3. Fortress level: Resistance training for key personnel

Niet alleen moeten alle medewerkers worden getraind in beveiligingsbewustzijn, maar het belangrijkste personeel (o.a. help desk, secretaresses, receptionistes en systeembeheerders) moet ook worden getraind in het geven van weerstand. Een goede training in weerstand zorgt ervoor dat medewerkers geen informatie weggeven die de social engineer nodig heeft. Een dergelijke training kan succesvol zijn wanneer twee essentiële eigenschappen worden meegenomen. De eerste is dat de medewerkers zich moet realiseren dat hij of zij wordt gemanipuleerd. De tweede en meest kritische eigenschap is dat medewerkers zich moeten realiseren dat ze zelf kwetsbaar voor manipulatie zijn.

4. Persistence level: Ongoing reminders

Een goede verdediging heeft regelmatig herinneringen nodig over de noodzakelijkheid van beveiligingsbewustzijn. Het trainen van mensen in weerstand bieden tegen social engineering is vaak maar effectief in een korte periode. Reguliere en creatieve herinneringen zijn nodig om mensen bewust te houden van de gevaren die er zijn in een vriendelijk telefoontje.

5. **Gotcha level: Social Engineering Land Mines (SELM)**

Social engineering land minds (SELM) zijn valstrikken die in het systeem zijn ingebouwd om een aanval bloot te stellen en te stoppen. De SELM waarschuwt het doelwit en de beveiliging van het doelwit dat er een aanval plaatsvindt waardoor er een verhoogde beveiliging optreedt. Voorbeelden van SELM zijn onder andere:

- **De persoon die alles weet:** deze persoon zorgt ervoor dat hij of zij iedereen kent die op de werkvloer rondloopt. Een social engineer aarzelt niet om een gebouw binnen te gaan en overal begint rond te kijken in de wetenschap dat hij of zij toch niet opvalt. Een persoon die dan iedereen daadwerkelijk kent kan de social engineer herkennen als een ongewilde bezoeker.

- **Gecentraliseerde security log:** het hebben van een gecentraliseerde security log kan een aanval helpen voorkomen. Wanneer een medewerkers gevraagd wordt om informatie weg te geven of een wachtwoord te veranderen, moet dit opgeslagen worden in dit systeem. Beveiligingspersoneel kan dan vervolgens actie ondernemen en de aanval stoppen, mocht het ook daadwerkelijk een aanval zijn.

- **Terugbellen:** een bekende procedure dat werkelijk helpt is het beleid dat helpdesk medewerkers en systeembeheerders toestaat om iedereen terug te bellen die een verzoek indienen om een wachtwoord te veranderen of die vraagt om bepaalde informatie. Terugbellen verifieert het telefoonnummer en zou het telefoonnummer moeten zijn die in de telefoonlijst staat van de persoon die belt.

- **In de wacht zetten:** Elk verdacht telefoontje waarin gevraagd wordt naar wachtwoorden of informatie moeten in de wacht worden gezet. De social engineer kan hierdoor zenuwachtig worden en stoppen met de aanval. Ook geeft dit de mogelijkheid voor de medewerker om na te denken.

6. **Offensive level: Incident response**

De laatste laag van verdediging is het reageren op incidenten. Er moet een goed gedefinieerd proces zijn dat een medewerker kan beginnen zodra hij of zij denkt wanneer er iets mis is. Als er geen dergelijk systeem is, zal iedere medewerker die met social engineering te maken krijgt een nieuw gevecht uitvechten. Zodra een social engineering aanval wordt ontdekt en wordt gekarakteriseerd en gecommuniceerd naar alle medewerkers, is de kans groot dat deze aanval in de toekomst niet nog een keer zal voorkomen en meteen zal worden herkend.

3.5.2 Additionele verdedigingstechnieken tegen social engineering

Naast de manier beschreven in subparagraaf 3.5.1, zijn er nog een aantal andere en aanvullende technieken om social engineering aanvallen tegen te gaan. Om een dergelijke aanval tegen te gaan, moeten medewerkers goed getraind zijn en bekend zijn met de algemene social engineering technieken. Het is belangrijk voor organisaties om een helder en sterk beveiligingsbeleid te creëren, met standaarden, processen en procedures om de dreiging van social engineering te stoppen. Een goede social engineering verdediging zou het volgende moeten bevatten [DOLA04]:

- Wachtwoorden beleid;
- Beoordelingen van de kwetsbaarheid van de organisatie;
- Classificatie van gegevens;
- Aanvaardbaar gebruiksbeleid;
- Achtergrond controles;
- Beëindiging proces;
- Reageren op incidenten;
- Fysieke beveiliging.

Wachtwoorden beleid

Toegang krijgen tot een informatiesysteem kan voor een social engineer het verschil betekenen in een geslaagde of mislukte aanval. Er moet een beleid bestaan voor het verkrijgen, creëren en veranderen van wachtwoorden. Een goed wachtwoorden beleid moet onder meer het volgende informatie bevatten:

- Geen wachtwoorden delen wanneer hier naar wordt gevraagd;
- Geen wachtwoorden opschrijven;
- Geen default wachtwoorden gebruiken;
- Methoden voor het geven van wachtwoorden;
- Het creëren van wachtwoorden;
- Periodiek veranderen van wachtwoorden;
- Uitsluiting van het informatiesysteem wanneer verkeerd wachtwoord wordt gebruik.

Medewerkers moeten zich realiseren dat een sterk wachtwoord uiterst belangrijk is. Hoe sterker het wachtwoord, hoe moeilijker te kraken of te achterhalen. Wachtwoorden mogen uiteraard ook niet worden opgeschreven. Social engineers gebruiken vaak de fysieke aanpak door op werkplekken naar opgeschreven wachtwoorden te zoeken. Er moet een strenge toezicht zijn op identiteiten van medewerkers wanneer wachtwoorden worden uitgedeeld. Er moet zekerheid zijn dat de medewerker inderdaad is wie die medewerker zegt te zijn.

Beoordeling van de kwetsbaarheid van de organisatie

Organisaties moeten periodieke beoordelingen doen over de (mogelijke) kwetsbaarheden. Zulke beoordelingen bestaan meestal uit bekende hacker tools en technieken die worden gebruikt om een netwerk bloot te stellen aan aanvallen. Door op deze manier te beoordelen kan er een accurate schatting worden gemaakt waar er problemen in organisaties zijn of kunnen voorkomen.

Classificatie van gegevens

Omdat social engineers de kennis van anderen gebruiken om aan informatie te komen, is het van belang om een data classificatie model te hebben waar alle medewerkers zich van bewust zijn. Data classificatie geeft een vorm van veiligheid aan bedrijfsinformatie. Elk niveau van data classificatie moet verschillende regels bevatten, zoals wie er toegang heeft, wij er kan bewerken en hoe de informatie kan worden gedeeld.

Een voorbeeld van een data classificatie model:

- Top Secret: Hoogst gevoelige interne documenten, die serieuze schade aan de organisatie kunnen brengen wanneer deze verloren gaan of publiekelijk worden gemaakt. Informatie dat geclassificeerd is als top secret heeft een strikte vorm van distributie en moet te allen tijde beschermd worden. Beveiliging op dit niveau is het hoogst mogelijk.

- Hoogst vertrouwelijk: informatie dat serieus de verrichtingen van een organisatie kan belemmeren wanneer deze informatie publiekelijk wordt gemaakt of in de organisatie wordt rondgedeeld. Deze informatie mag niet worden gekopieerd of worden meegenomen zonder specifieke toestemming. De beveiliging op dit niveau moet erg hoog zijn.

- Proprietary: informatie van eigendomsgebonden aard. Procedures operationele werk routines, project plannen, ontwerpen en specificaties die de manier definiëren waarop een organisatie werkt. Zulke informatie is normaliter alleen voor geautoriseerd personeel en de beveiliging op dit niveau moet hoog zijn.

- Alleen voor intern gebruik: informatie dat niet bestemd is voor gebruik buiten de organisatie en waar verlies van deze informatie zorgt voor ongemak in de organisatie en bij het management maar dat waarschijnlijk niet resulteert in financieel verlies of serieus schade toebrengt aan de geloofwaardigheid. De beveiliging is gecontroleerd maar wel normaal.

- Publieke documenten: Informatie voor het publieke domein, zoals jaarrapporten. De beveiliging op dit niveau is minimaal.

Aanvaardbaar gebruiksbeleid

Een gebruiksbeleid zorgt ervoor dat vertrouwelijke data niet gedeeld wordt en dat informatiesystemen niet misbruikt worden. Een dergelijk beleid bevat informatie over hoe een informatiesysteem gebruikt moet worden en dat informatiesystemen alleen gebruikt worden waarvoor ze bedoeld zijn.

Achtergrond controles

Social engineers gebruiken iedere methode tot hun beschikking om hun doel te bereiken. Ook door zelf te gaan werken voor de organisatie dat door de social engineer als doelwit is uitgekozen. Een achtergrond controle van medewerkers is daardoor belangrijk en een essentieel deel in de verdediging tegen social engineering. Overigens geldt dit niet alleen voor intern personeel, maar ook voor extern personeel zoals bijvoorbeeld schoonmaakpersoneel.

Beëindigingsproces

Een effectief beëindiginsproces voor het afschrikken van ontslagen of opgestapte medewerkers is een ‘must-have’ voor iedere organisatie. Dit proces zorgt ervoor dat deze medewerkers hun toegang tot informatie niet gebruiken om schade aan de organisatie toe te brengen. Een proces voor beëindiging moet onder andere het volgende bevatten: de

onmiddellijke verwijdering tot toegang van het netwerk, toegang tot faciliteiten en toegang tot alle applicaties die door de medewerker gebruikt werden.

Fysieke beveiliging

Het hebben van fysieke beveiligingsmaatregelen helpt sterk tegen het binnendringen van een organisatie door een social engineer. Voorbeelden van maatregelen zijn:

- Identificatie voor niet-medewerkers: Personen die op reguliere basis toegang tot de organisatie moeten hebben, moeten een soort van speciale identificatie hebben. Personen die iets af komen leveren of iets komen repareren zouden een vorm van unieke identificatie moeten hebben.

- Pas voor het vergrendelen van informatiesystemen: Een pas dat ervoor zorgt dat je toegang krijgt tot het informatie systeem kan een alternatief zijn voor inloggen met een wachtwoord. Door de pas (of een andere harde token) in bijvoorbeeld het toetsenbord te bevestigen kan er automatisch toegang tot een informatiesysteem worden verkregen. En door deze pas te verwijderen wordt automatisch het informatiesysteem vergrendeld wanneer iemand zijn of haar werkplek verlaat.

- Identificatie voor bezoekers: Bezoekers moeten te allen tijde identificatie dragen en een logboek invullen met daarin aankomsttijd, contactpersoon en vertrektijd.

- Begeleiden van bezoekers: Bezoekers moeten altijd door een medewerker in het gebouw begeleidt worden.

- Kentekenplaten opslaan: Als er een parkeergarage is met cameratoezicht, zouden alle kentekenplaten van in- en uitgaande voertuigen moeten worden opgeslagen.

- Vuilnisbakken: Vuilnisbakken zouden niet publiekelijk toegankelijk mogen zijn. Vuilnisbakken moeten staan op een beveiligde plek, zodat personen die geen toegang behoren te hebben niet op zoek kunnen gaan naar informatie.

3.6 Conclusie

Social engineering heeft als doel om ongeautoriseerde toegang tot informatie te krijgen via misleiding en is een serieuze dreiging voor veel organisaties. Omdat mensen in een organisatie de zwakste schakel zijn, is het moeilijk om een verdediging op te bouwen tegen aanvallen van social engineering. Er worden naar manieren of middelen gezocht om mensen te manipuleren die toegang tot de informatie of het gewenste systeem hebben. Het wordt steeds moeilijker om technische kwetsbaarheden uit te buiten waardoor hackers en andere kwaadwillenden zicht richten op de zwakste schakel in de informatiebeveiliging van een organisatie, namelijk de mens. Mensen bezitten psychologische eigenschappen die kwetsbaar zijn voor social engineering en waarop social engineers kunnen inspelen om tot het uiteindelijke doel te komen: het verkrijgen van de gewenste informatie.

Ieder mens bezit dus een aantal psychologische eigenschappen waarop de social engineer probeert in te spelen bij het uitvoeren van een social engineeringaanval. Hierbij maakt de social engineer gebruik van verschillende psychologische technieken. Uit de analyse is gebleken dat er een aantal psychologische eigenschappen zijn die erg kwetsbaar zijn bij een

aanval van social engineering. Het gaat dan met name om de eigenschappen autoriteit, behulpzaamheid, nieuwsgierigheid en angst. Deze eigenschappen lopen het meest gevaar om te worden beïnvloed door de psychologische technieken die een social engineer kan gebruiken. Dit komt met name omdat mensen van nature graag aardig willen worden gevonden en dus behulpzaam willen zijn naar anderen. Daarnaast zijn mensen uiterst gevoelig voor autoriteit en angst, er wordt eerder geluisterd naar iemand die hoger in aanzien staat en autoriteit uitstraalt dan naar iemand die lager in de hiërarchie van de organisatie staat. Nieuwsgierigheid is ook iets wat mensen vaak van nature bezitten en dus kwetsbaar maakt voor social engineering. Dit geldt overigens ook voor de eigenschap onverschilligheid omdat mensen vaak nonchalant en onverschillig met informatie omgaan en ze vaak niet beseffen wat de waarde van informatie is.
De psychologische technieken die een social engineer het best kan gebruiken om de verschillende psychologische eigenschappen te beïnvloeden, zijn vriendelijkheid en intimidatie. Deze twee technieken zijn waarschijnlijk het meest effectief wanneer het aankomt om eigenschappen zoals behulpzaamheid en angst te beïnvloeden. Door vriendelijk tegen iemand te zijn en daardoor aardig over te komen is de kans groter dat die persoon je zal helpen en dus het verzoek dat is neergelegd waarschijnlijk zal inwilligen. Ook voor intimidatie geldt dit, door intimiderend over te komen wordt een verzoek sneller ingewilligd omdat mensen over het algemeen bang zijn voor represailles wanneer er niet aan een verzoek wordt voldaan.

Social engineers gebruiken verschillende tactieken (aanvallen) om anderen te overtuigen en te beïnvloeden middels de psychologische technieken om zo hun doel te bereiken. Afhankelijk van welke psychologische technieken er gebruikt worden om in te spelen op de verschillende eigenschappen van mensen, kan er gekozen worden uit verschillende tactieken.
Impersonation is de tactiek die waarschijnlijk het meest succesvol kan zijn omdat deze tactiek gebruik kan maken van alle psychologische technieken en dus ook kan in spelen op alle psychologische eigenschappen. Dit maakt deze tactiek de gevaarlijkste social engineering aanval omdat voor elke situatie een specifieke rol kan worden bedacht door de social engineer. Als de social engineer uit is op wachtwoorden van medewerkers kan de rol van helpdeskmedewerker worden aangenomen om zo de medewerkers te misleiden in het weggeven van wachtwoorden. En vanwege de eigenschappen nieuwsgierigheid en onverschilligheid zijn ook tactieken zoals baiting, piggybacking en dumpsterdiving goede aanvallen om uit te voeren om aan gevoelige en vertrouwelijk informatie te komen.

De belangrijkste maatregel in het tegengaan van social engineering is om ervoor te zorgen dat er een veiligheidsbewustzijn (security awareness) bij medewerkers ontstaat. Medewerkers moeten weten wanneer ze worden aangevallen en hoe hierop dient te worden gereageerd. Hoewel er geen gegarandeerde manier is om volledig een social engineering aanval tegen te gaan, kan wel het risico worden tegengegaan en geprobeerd worden om de schade zoveel mogelijk te minimaliseren. Dit komt neer op het creëren van een veiligheidsbewustzijn bij medewerkers en het toepassen van additionele maatregelen zoals in paragraaf 3.5 staat beschreven.

4. Informatiebeveiliging awareness

Awareness (in het Nederlands bewustzijn) is een belangrijk aspect in het beveiligen van informatie, zo niet het belangrijkste aspect. Maar het creëren van een bewustzijn met betrekking tot informatiebeveiliging is vaak een lastige en moeizame aangelegenheid. In de meeste gevallen ontgaat het nut en de noodzaak de medewerkers geheel, niet alleen bij de werknemers maar ook bij het management. Ook kampt informatiebeveiliging vaak met een slecht imago (het wordt als lastig gezien, veel extra regeltjes) en wordt het gezien als de taak van anderen in de organisatie en dat het niets met de eigen functie en verantwoordelijkheid te maken heeft. Gebruikers bewust maken van hun verantwoordelijkheden in het beveiligen van de informatie en de omgeving en ze ook daadwerkelijk motiveren om dit te doen, is hetgeen wat bekend staat als informatiebeveiliging awareness.

Dit hoofdstuk ziet er als volgt uit: allereerst wordt beschreven wat er wordt verstaan onder informatiebeveiliging awareness, vervolgens wordt de aard van informatiebeveiliging awareness beschreven en wordt awareness gerelateerd aan het gedrag dat beïnvloed dient te worden. Tot slot wordt er een proces beschreven van hoe een effectief informatiebeveiliging awareness programma eruit hoort te zien.

4.1 Wat is informatiebeveiliging awareness

De term informatiebeveiliging awareness wordt gebruikt om te refereren naar een conditie waar medewerkers in een organisatie zich bewust zijn van het beveiligingsbeleid van een organisatie. Informatiesystemen kunnen alleen bruikbaar zijn als mensen ze gebruiken. Dit geldt feitelijk ook voor informatiebeveiliging awareness dat van cruciaal belang is, omdat informatie beveiligingstechnieken of procedures verkeerd kunnen worden gebruikt, verkeerd kunnen worden geïnterpreteerd of zelfs helemaal niet worden gebruikt door gebruikers en ze daardoor hun nut en waarde verliezen [SIPO00].

In de literatuur zijn verschillende definities te vinden over informatiebeveiliging awareness. Het Information Security Forum (ISF), dat één van de grootste autoriteiten op het gebied van informatiebeveiliging is, hanteert de volgende definitie:

> *"the extent to which organizational members understand the importance of information security, the level of security required by the organization and their individual security responsibilities, and act accordingly"*

De National Institute of Standards and Technology (NIST) definieert informatiebeveiliging awareness als volgt:

> *"Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly"*

Siponen [SIPO00] gebruikt de volgende definitie:

> *"a state where users in an organization are aware, ideally committed to, of their security mission"*

Dhillon definieert informatiebeveiliging awareness in [DHIL07] als volgt:

> *"participants should be aware of the need for security of information systems and networks and what they can do to enhance security"*

In deze scriptie zal de definitie van het ISF worden aangehouden omdat deze definitie niet alleen het belang van informatiebeveiliging onder medewerkers beschrijft maar ook het gedrag dat mensen erop nahouden. Dit is van groot belang omdat het gedrag van een persoon kan vaststellen hoeveel een individu bewust is van zijn of haar gedrag en de bijbehorende consequenties. Het is namelijk vaak het wangedrag van mensen dat voor problemen zorgt bij de beveiliging van informatie.

4.1.1 De plaats van awareness binnen informatiebeveiliging

In paragraaf 2.2.2 van hoofdstuk 2 is bepaald dat beveiligingsmaatregelen kunnen worden opgedeeld op drie manieren:

- Organisatorische maatregelen;
- Logische maatregelen;
- Fysieke maatregelen.

Bij awareness gaat het om organisatorische maatregelen en duidelijk niet om logische en fysieke maatregelen. Organisatorische maatregelen zijn maatregelen die betrekking hebben op de organisatie als geheel, zoals het beveiligingsbeleid, richtlijnen en procedures. In [OVER07] wordt aangegeven dat organisatorische maatregelen toepasbaar zijn op menselijke en organisatorische zaken, waardoor de volgende aspecten van informatiebeveiliging noodzakelijk zijn:

- Het opstellen, uitdragen en onderhouden van informatie beveiligingsbeleid en –plan;
- Het ontwikkelen en implementeren van procedures;
- Het organiseren van informatiebeveiligingsmaatregelen;
- Het beïnvloeden van gedrag (motivatie).

Het beïnvloeden van gedrag is een noodzakelijk aspect binnen de informatiebeveiliging en het is duidelijk dat awareness onder dit aspect valt. Om een beter bewustzijn te krijgen van het informatie beveiligingsbeleid, de procedures en maatregelingen zal het gedrag moeten worden beïnvloed en/of veranderd. Awareness is dus een noodzakelijke organisatorische maatregel.

4.1.2 Manieren om gedrag te beïnvloeden

In paragraaf 4.1.1 is gebleken dat het beïnvloeden van gedrag een belangrijk aspect is binnen de informatiebeveiliging en dat awareness gerelateerd is aan dit aspect. Bij beïnvloeding van het gedrag van personen spelen vier belangrijke zaken een rol [KOOT05]:

1. **Bewustzijn**: De bewustheid van personen dat er verschillende risico's bestaan voor de veiligheid van informatie van organisaties;
2. **Betrokkenheid**: De mate waarin de persoon zich betrokken voelt met het informatie beveiligingsbeleid van de organisatie;
3. **Belang**: Personen zijn eerder geneigd hun gedrag te veranderen wanneer dit in hun eigen belang is;
4. **Beloning**: Met een beloning (of een straf) wordt het belang van een persoon om het gedrag te veranderen tastbaar gemaakt.

Deze bovenstaande aspecten kunnen door organisaties worden gebruikt om het gedrag van de medewerkers te beïnvloeden en te veranderen. Met name het bewustzijn, de betrokkenheid en het belang kunnen door organisaties worden gebruikt om gedrag te veranderen. Deze drie aspecten worden vooral verkregen door communicatie. Beloning is een methode om naast de communicatie te gebruiken om gewenst gedrag te stimuleren, waardoor tegelijk ook het belang voor de persoon wordt onderstreept.

4.2 De aard van informatiebeveiliging awareness

In [WIPA09] onderzoekt Kamphol Wipawayangkool van de Universiteit van Texas de aard van awareness in relatie met informatiebeveiliging. Om dit te kunnen doen worden er eerst een aantal veronderstellingen beschreven die van belang zijn zijn. Ten eerste is informatiebeveiliging awareness een multidimensioneel onwaarneembaar concept. Ten tweede kan awareness worden vergroot door middel van een combinatie van de geschikte tijd, opleiding en ervaring. En ten derde, hoe meer een individu leert, hoe meer dit geassocieerd wordt met een verhoogde awareness. Vandaar dat er in het onderzoek van [WIPA09] wordt uitgegaan van de theorie van leerdoelstellingen, waarin de resultaten cognitief, affectief en gebaseerd op gedrag kunnen zijn.

- Cognitieve resultaten refereren naar variabelen die gerelateerd zijn aan de kwantiteit en het type kennis en de relatie tussen kennis elementen. Dit betekent dat cognitieve leerdoelstellingen niet alleen worden afgeleidt uit het statische kennisdomein, maar ook uit het dynamische proces van het verkrijgen, organiseren en toepassing van kennis. In andere woorden, 'weten wat het is' en 'weten hoe het te verkrijgen en te gebruiken' wordt toegeschreven aan het cognitieve leren.

- Affectieve resultaten refereren naar variabelen die kwesties omringen zoals opvattingen, motivatie en doelen die relevant zijn voor de doelstellingen van het trainingsprogramma. De logica is dat leren ook ontstaat wanneer de waarden, houdingen en motivatie van een individu veranderen.

- Resultaten gebaseerd op gedrag refereren naar vaardigheden die gekarakteriseerd worden door een aaneenschakeling van gedrag op een opeenvolgend en hiërarchisch georganiseerde manier. Een individu ontwikkelt een vaardigheid wanneer hij of zij selectief en automatisch een actie kan uitvoeren met merkbaar minder fouten dat

gebaseerd is op een integratie van veelvuldig verkregen kennis en stappen die in eerder stadium zijn aangeleerd.

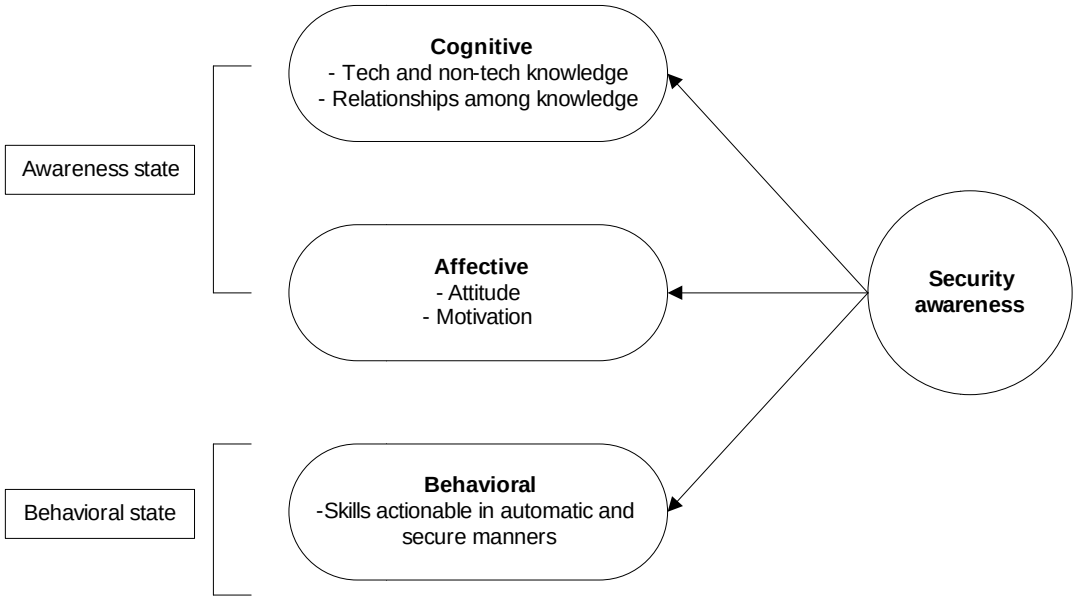
Gebaseerd op deze veronderstellingen en de theorie van leerdoelstellingen kan de aard van informatiebeveiliging awareness worden onderzocht. Gegeven dat awareness een multidimensioneel onwaarneembaar concept is, kan een individu leren om zijn of haar niveau van awareness te verbeteren op de drie hierboven genoemde dimensies (cognitief, affectief en gedrag).

- Cognitieve dimensies refereren naar de kwantiteit en de soorten van veiligheidskennis (zowel technische als niet technische kennis) en de relatie tussen de verschillende type kennis die bestaat (bijvoorbeeld toegang tot een netwerk via VPN, een individu zal dan de informatie uit het beveiligingsbeleid moet kennen en tevens ook moeten weten hoe een VPN te gebruiken).

- Affectieve dimensies refereren naar houdingen en motivatie van een individu naar veiligheidspraktijken en principes, zowel in het algemeen als met het beveiligingsbeleid van de organisatie. Bijvoorbeeld wanneer het gaat over het beleid bij het veranderen van wachtwoorden, kan een individu wel of niet het nut ervan inzien wanneer de onderliggende redenen worden uitgelegd en dus leidt tot een verbeterd niveau van awareness.

- Gedragsdimensies refereren naar de ontwikkeling van vaardigheden dat ervoor zorgt dat een individu bewust en automatisch zijn of haar taken kan uitvoeren op een veilige manier. Wanneer een individu op een bewuste en automatische manier een veilig gedrag aantoont, is het niveau van awareness verbeterd.

Dit is ook in één lijn met de definitie van informatiebeveiliging awareness van het ISF omdat bij allebei de significatie wordt erkend van niet alleen de staat van awareness (cognitief en affectief), maar ook de staat van het gedrag. Figuur 23 op de volgende pagina illustreert de multidimensionele aard van informatiebeveiliging awareness.



Figuur 23: de multidimensionele aard van informatiebeveiliging awareness

4.3 Awareness en het beïnvloeden van gedrag

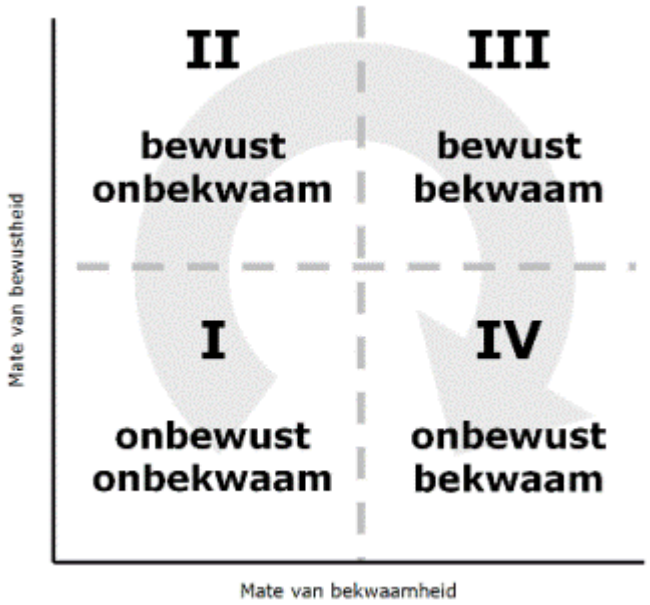
Awarness heeft te maken met het bewust zijn van risico's die er bestaan op het gebied van informatiebeveiliging. Bepaalde risico's kunnen worden beperkt met technische maatregelen. Echter, veel risico's liggen in het handelen als onderdeel van menselijk gedrag. Wanneer een beter bewustzijn van informatiebeveiliging gekregen moet worden, zal het menselijk gedrag beïnvloed moeten worden. Het gedrag van mensen moet zodanig worden beïnvloed en/of veranderd, dat het leidt tot een verhoogd veiligheidsbewustzijn [CIO09]. Zoals in paragraag 4.2 is uiteengezet, wordt awareness gerelateerd met de theorie van leerdoelstellingen. Hoe meer een persoon leert, hoe meer dit geassocieerd wordt met een verhoging van de awareness. Er kan dus gezegd worden dat wanneer een persoon leert, zijn of haar gedrag dusdanig beïnvloedt wordt dat er een verhoging van awareness optreedt. Er zijn in de loop der tijd verschillende theorieën ontwikkeld met betrekking tot leren. Abraham Maslow is een Amerikaanse psycholoog die een eigen theorie hierin heeft ontworpen. In deze paragraaf zal de theorie van Maslow worden besproken.

De leertheorie van Maslow

Abraham Maslow heeft een theorie ontworpen waarbij vier stadia zich onderscheiden en die bij elk leerproces worden doorlopen om gedragsverandering te bereiken. Dit model is dus tevens toepasbaar voor het creëren van bewustzijn en het afleren van onwenselijk gedrag op het gebied van informatiebeveiliging [CIO09].

De vier leerstadia in deze theorie bewegen zich langs twee dimensies: bewust/onbewust en bekwaam/onbekwaam. De eerste twee stadia, bewust en onbewust hebben betrekking op het gedrag (zie hoofdstuk 2, paragraaf 2.5). De andere twee stadia, bekwaam en onbekwaam, hebben betrekking op de (in)competentie van personen. Een persoon die iets leert begint altijd

in de eerste fase (onbewust, onbekwaam) en eindigt in de vierde fase (onbewust bekwaam), terwijl onderweg de tweede (bewust,onbekwaam) en de derde fase wordt dooropen (bewust, bekwaam). In de onderstaande figuur word de leertheorie van Maslow schematisch weergegeven.



Figuur 24: de leertheorie van Maslow

Fase 1: Onbewust onbekwaam

In de eerste fase is men zich niet bewust van de eigen incompetentie en dat er bepaalde vaardigheden missen. Een persoon die onbewust onbekwaam is, realiseert zich niet dat hij of zij niet weet hoe een taak moet worden uitgevoerd. Er is een compleet gebrek aan kennis en vaardigheden bij het onderwerp in kwestie.

Eigenschappen van deze fase zijn:

- De persoon is zich niet bewust van het bestaan of de relevantie van vaardigheden;
- De persoon is zich er niet van bewust dat er een bepaald gebrek is op een bepaald gebied;
- De persoon kan de relevantie of het nut ontkennen van de nieuwe vaardigheid;
- De persoon moet zich bewust van de onbekwaamheid worden voordat de ontwikkeling van de nieuwe vaardigheid kan beginnen;
- Het doel van de trainer of docent is om de persoon in de volgende fase (bewust, onbekwaam) te krijgen door te demonstreren dat de vaardigheid en het voordeel dat het met zich mee zal brengen voor meer effectiviteit bij die persoon zal zorgen.

Om gedragsverandering te bereiken is het noodzakelijk dat er bewustwording optreedt waarbij duidelijk wordt dat het oude gedragspatroon niet meer voldoet en dat men overtuigd wordt van het nut van het gewenste gedrag. Een manier om dit te doen is via confronteren en motiveren:

- Om medewerkers bewust te krijgen, is het belangrijk om ze te confronteren met de consequenties van hun gedrag;
- Om medewerkers gemotiveerd te krijgen, is het belangrijk om achtergrondinformatie (het 'wat' en 'waarom') bij het gewenste gedrag te geven.

Fase 2: Bewust onbekwaam

In deze tweede fase treedt bewustwording op, men wordt zich bewust van de eigen incompetentie. Men mist nog steeds de gewenste vaardigheden, maar weet dit nu van zichzelf. Pas wanneer men openstaat voor nieuw gedrag kan begonnen worden met het aanleren van dit gedrag.

Eigenschappen van deze fase zijn:

- De persoon wordt zich bewust van de aanwezigheid en de relevantie van de vaardigheid;
- De persoon is zich daardoor ook bewust dat er een gebrek is op een bepaald gebied, doordat er geprobeerd wordt om gebruik te maken van deze vaardigheid;
- De persoon realiseert zich door de vaardigheid op dit gebied te verbeteren, dat de effectiviteit verbeterd zal worden;
- De persoon verplicht zichzelf om de nieuwe vaardigheid te leren, en daardoor over te gaan naar de derde fase (bewust, bekwaam).

Fase 3: Bewust bekwaam

In deze fase is men bekend met het nieuwe gedrag, kent men de waarde ervan en is in staat om het gedrag te vertonen, als men zich daarop concentreert. Het gedrag dient nu geautomatiseerd te worden. OM nieuw gedrag eigen te maken is het belangrijk dat men herhaaldelijk geprikkeld wordt om dit gedrag te (blijven) vertonen en dat reflectie plaatsvindt op voortgang en resultaten.

Eigenschappen van deze fase zijn:

- De persoon bereikt deze fase in een vaardigheid wanneer deze op betrouwbare wijze en te allen tijde kan worden uitgevoerd;
- De persoon moet zich concentreren en kunnen nadenken om de vaardigheid uit te kunnen voeren;
- De persoon kan de vaardigheid zonder hulp uitvoeren;
- De persoon zal de vaardigheid niet betrouwbaar uitvoeren wanneer er niet over wordt nagedacht. De vaardigheid is nog geen natuurlijk en automatisch gedrag;
- De persoon moet de nieuwe vaardigheid blijven oefenen om naar de volgende fase te kunnen gaan.

Fase 4: Onbewust bekwaam

Men is onbewust bekwaam als het gewenste gedrag onderdeel is geworden van de persoon. Het nieuwe gedrag is ingesleten en geautomatiseerd. De opgedane kennis en vaardigheden kunnen vervolgens als basis dienen voor verdere ontwikkeling van de informatiebeveiliging.

Eigenschappen van deze laatste fase zijn:

- De vaardigheid wordt zo vaak beoefend dat het in feite een onbewuste handeling wordt, het wordt een automatisme;
- Het wordt mogelijk om sommige vaardigheden uit te oefenen, wanneer op hetzelfde moment ook iets anders wordt gedaan;

Bewustwording is dus duidelijk de eerste stap naar verbetering [CHAP10] [CIO09].

4.4 Proces van een effectief informatiebeveiliging awareness programma

In een gepubliceerd workshop rapport [INFO02] heeft het ISF een proces ontwikkeld om tot een effectief informatiebeveiliging awareness programma te komen. Het ISF heeft de volgende definitie gehanteerd:

> "*Effective security awareness is achieved through an ongoing process of learning that is meaningful to recipients, and delivers measurable benefits to the organization from lasting behvioural change"*

Effectieve informatiebeveiliging awareness programma bevat 4 belangrijke elementen:

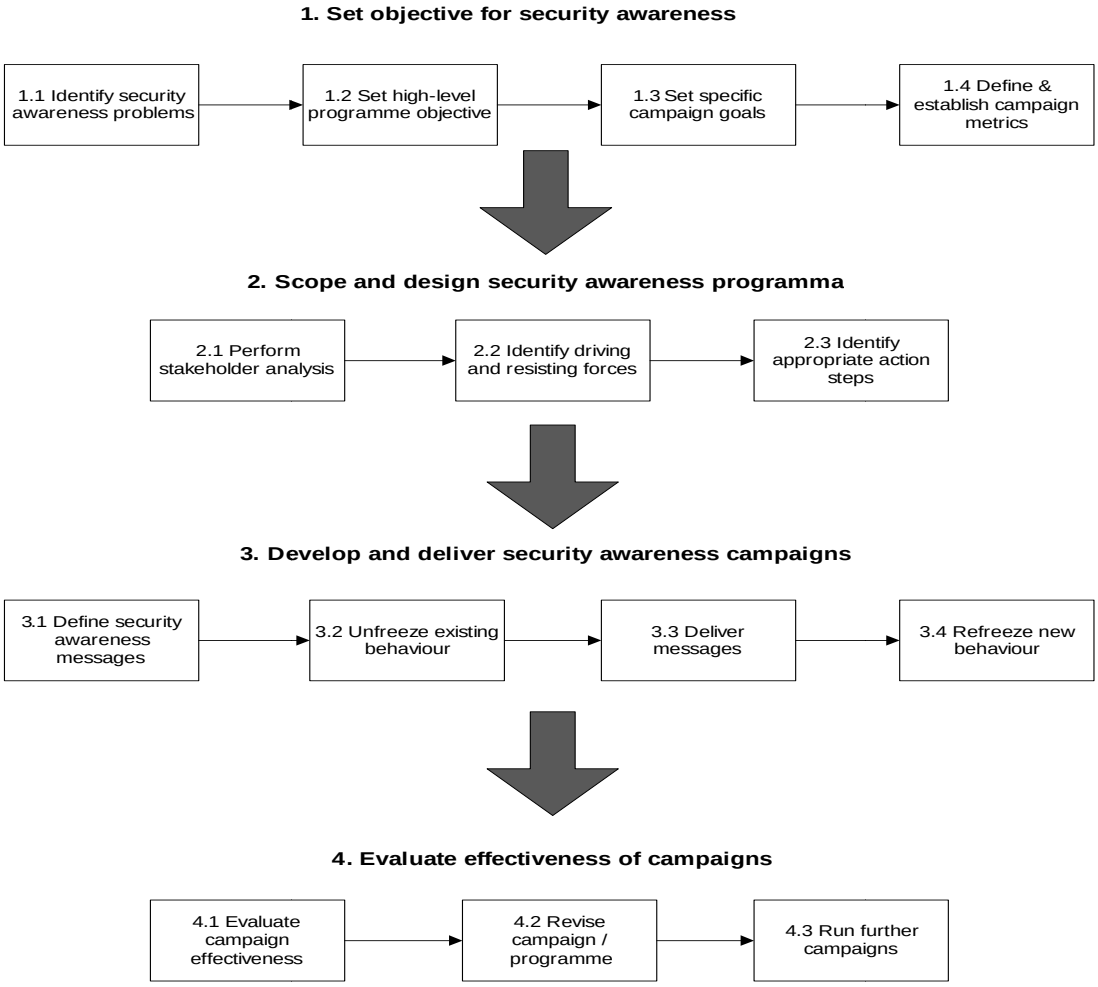
1. Een formele structuur: een awareness programma is vaak alleen succesvol wanneer het gestructureerd is als een formeel programma, in tegenstelling tot een serie van ad hoc activiteiten.

2. Zinvolle berichten: de belangrijkste mededelingen en aanpak van het programma moet relevant zijn voor het publiek en tevens consistent zijn met hun normen, waarden en doelstellingen: als beveiliging wordt gezien als een belemmering van de eigen persoonlijke activiteiten, dan zal de boodschap weinig betekenis hebben.

3. Meetbare voordelen: een effectief informatiebeveiliging awareness programma moet voor een positieve verandering in het gedrag zorgen, dat bij beveiliging komt kijken. Deze verandering moet dan onder andere leiden tot een vermindering van de kosten van security management en een vermindering van de beveiligingsrisico's.

4. Voortdurend verandering in gedrag: het doel van een effectief informatiebeveiliging awareness programma moet zijn om een positieve verandering in het gedrag van de ontvangers te creëren, ten opzichte van beveiliging. Als de verandering niet wordt aangehouden en er wordt teruggrepen naar voorgaand gedrag, dan is het programma niet effectief gebleken.

Het door het ISF ontwikkelde informatiebeveiliging awareness programma dat uitgaat van de vier criteria die hierboven zijn beschreven, is te zien in figuur 25.



Figuur 25: Proces voor een effectief informatiebeveiliging awareness programma

1. Set objective for security awareness

De eerste fase van het proces is om een duidelijke doelstelling vast te stellen. Dit is niet zo eenvoudig als dat het lijkt, een heldere en constructieve doelstelling is vaak moeilijk om te identificeren. Een doelstelling moet direct worden afgeleid van de problemen die moeten worden opgelost. Zodra de doelstelling is vastgesteld, kunnen specifieke doelen ervoor zorgen dat de doelstelling wordt bereikt

1.1: Identify security awareness problems

De eerste stap is om de problemen te identificeren die kunnen worden aangetoond door een informatiebeveiliging awareness programma. Door de problemen te identificeren, kan de doelstelling een behoefte in de organisatie aantonen.

Voorbeelden van problemen kunnen zijn:

- Het veranderen van cultuur in een organisatie;
- Het negeren van het beleid door medewerkers;
- Slechte beveiliging van informatiesystemen;
- Verzet tegen beveiliging van het management.

1.2: Set high-level programme objective

Het succes van een informatiebeveiliging awareness programma hangt sterk af van het vaststellen van een correcte doelstelling. Het definiëren van een correcte doelstelling is echter vaak geen makkelijke aangelegenheid. De niet tastbare aard van veel awareness uitkomsten betekent dat het moeilijk is om te kwantificeren wat het programma zal bereiken. Wanneer een doelstelling moet worden vastgesteld, dan is het noodzakelijk dat duidelijk de problemen naar voren komen die zijn geïdentificeerd (het probleem definiëren als onderdeel van de doelstelling) en tevens zou de doelstelling ook in lijn moeten zijn met de missie van de organisatie.

Voorbeelden van doelstellingen kunnen zijn:

- Zorg ervoor dat alle medewerkers bekend zijn met het beleid omtrent informatiebeveiliging;
- Verminder de diefstal van laptops en PDA computers;
- Implementeer een ‘clear desk’ beleid;
- Verminder ongepast gebruik van informatiesystemen en internet resources.

1.3: Set specific campaign goals

Zodra de doelstelling is vastgesteld, moet over de betreffende informatiebeveiliging awareness campagnes worden nagedacht. In sommige van de informatiebeveiliging awareness programma’s, is de doelstelling voldoende gedetailleerd om te kunnen beginnen met de awareness campagnes. Maar als een programma uiterst complex is, kan het nodig zijn om meer doelstellingen te definiëren om zo datgene wat nodig is te bereiken. Campagne doelen moeten worden gezien als subdoelstellingen en moeten op dezelfde manier worden gedefinieerd als de high-level doelstelling.

1.4: Define & establish campaign metrics

De doelstelling en de verschillende campagne doelen zouden details van een meetbare verandering moeten bevatten die door het informatiebeveiliging awareness programma en de campagnes bereikt moeten worden.

De volgende stap in het proces is om de standaarden (metrics) te definiëren die gebruikt zullen worden om het succes van de doelstelling en de campagne doelen te meten. Dit is nodig om veranderingen in gedrag te kunnen vergelijken tijdens, voor en na de awareness campagne.

Voorbeelden van metrics zijn:

- Het aantal bezoeken en de tijd van aanwezigheid op het intranet;
- De reactie op nieuws surveys over beveiliging;
- De sterkte van de wachtwoorden en de mate van verandering van wachtwoorden;
- Scores van een risico analyse;
- De balans tussen persoonlijk en zakelijk internet gebruik.

2. Scope and design security awareness programme

Wanneer de doelstellingen, de onderliggende doelen en de metrics zijn bepaald, is de volgende stap om het proces te ontwikkelen. Het doel van deze fase is om de deelnemers in te lichten over het doel van het programma en de acties te plannen die gebruikt zullen worden om de bestaande krachten te veranderen.

2.1: Perform stakeholder analysis

Een informatiebeveiliging awareness programma moet normaal gesproken altijd de steun en medewerking hebben van alle afdelingen en niet alleen van de afdeling die over de informatiebeveiliging gaat. Het is essentieel dat alle deelnemers, de stakeholders, worden geïdentificeerd en worden aangemoedigd om mee te helpen aan het programma. Een stakeholder analyse is een techniek om het belang van individuen en groepen te identificeren en in te schatten of die het project kunnen assisteren of belemmeren. Een stakeholder analyse kan :

- Individuen en groepen identificeren die een informatiebeveiliging awareness programma kunnen beïnvloeden (de stakeholders);
- De invloed (positief of negatief) schatten die deze stakeholders hebben op het programma;
- Assisteren in het ontwikkelen van ene strategie om ondersteuning te krijgen en obstakels van stakeholders te minimaliseren.

2.2: Identify driving and resisting forces

Om verandering in gedrag van individuen te krijgen, kan er gebruik gemaakt worden van driving en resisting forces. Wanneer de stakeholders zijn geïdentificeerd, moeten de driving en resisting forces worden geanalyseerd. Eén van de meest effectieve methoden om dit te doen is middels een brainstorm sessie met het gehele team. Beschouw de doelstelling en onderliggende doelen en probeer vervolgens zoveel mogelijk forces te identificeren als mogelijk. Wanneer de forces zijn geïdentificeerd, kan worden bekeken welke forces het grootste effect hebben op de situatie.

Voorbeelden van driving forces zijn:

- De behoefte om kosten te verminderen;
- Naleving bereiken met het beleid en regelgeving;
- De reputatie van de organisatie beschermen;
- Verminder het aantal incidenten met betrekking op beveiliging.

Voorbeeld van resisting forces zijn:

- Angst en verzet tegen veranderingen in een organisatie;
- Gebrek aan ondersteuning van het management voor informatiebeveiliging awareness;
- De cultuur van de organisatie hecht geen waarde aan beveiliging.

2.3: Identify appropriate action steps

Wanneer de driving en resisting forces zijn geïdentificeerd, moeten vervolgens de juiste actiestappen worden geïdentificeerd die het gewenste resultaat zullen behalen. Voor elke driving en resisting force moet het volgende worden herzien:

- Elke doelstelling en de geassocieerde forces: de actie stappen die nodig zijn om het effect op driving forces te verhogen en de actie stappen die nodig zijn om het effect op resisting forces te verminderen;
- De lijst met alle acties;
- De laatste lijst met acties om er zeker van te zijn dat ze allemaal haalbaar zijn en dat het kan worden omgezet in een actieplan.

3. Develop and deliver security awareness campaigns

Wanneer het informatiebeveiliging awareness programma ontwikkeld is, kunnen de individuele awareness campagnes worden geïdentificeerd, ontwikkeld en afgeleverd.

3.1: Define security awareness messages

Het belangrijkste bij een beveiliging awareness campagne is de boodschap dat afgeleverd moet worden om een verandering in het gedrag te kunnen realiseren. Vaak komt het voor dat dit gebeurt op een onduidelijke en herhaaldelijke manier en kan daardoor schade toebrengen aan het programma. Een boodschap moet het volgende bevatten:

- Voor wie de boodschap geldt;
- Wat het probleem is;
- Wat de consequenties zijn;
- Wat te doen;
- Wie de nieuwe boodschap gesteld heeft;
- Naar wie je moet vragen wanneer mee informatie gewenst is.

3.2: Unfreeze existing behviour

Voordat een verandering effect kan hebben, moet bestaand gedrag worden ‘ontdooid’. Het bestaande negatieve gedrag omtrent informatiebeveiliging moet eerst worden afgebroken voordat een boodschap met informatiebeveiliging positief gedrag kan worden afgeleverd.

De sleutel in het ontdooiingsproces is om indruk te maken op personeel met het feit dat er verandering nodig is, en om er zeker van te zijn dat het personeel weet:

- Dat er een probleem is;
- Dat het probleem aan hen gerelateerd is;
- Er iets gedaan moet worden om het probleem op te lossen.

3.3: Deliver messages

De informatiebeveiliging awareness boodschappen moeten op een effectieve manier worden overgebracht. Dit kan op verschillende manieren:

- Maak gebruik van verschillende kanalen voor het leveren van de boodschap;
- Verzorg beloningen voor positief gedrag;
- Dwing naleving af van het beveiligingsbeleid;
- Maak de beveiliging eenvoudig.

3.4: Refreeze new behaviour

De laatste fase in het veranderingsproces is om het gewenste positieve gedrag vast te houden dat gecreëerd is door de beveiliging awareness campagne. Dit kan door het introduceren van een proces of mechanisme dat het personeel aanmoedigt om het gedrag te behouden dat door de campagne gecreëerd is. Er zijn twee verschillende type mechanismen:

- Positieve mechanismen: moedigen het personeel aan om het nieuwe gedrag te behouden via aanmoediging en beloning;
- Negatieve mechanismen: stelt het personeel verplicht om het nieuwe gedrag te behouden via interne druk en discipline;

4. Evaluate effectiveness of campaigns

De succesvolle afhandeling van een awareness campagne moet resulteren in het gewenste positieve gedrag dat door de ontvangers van de campagne moet worden omarmd. Het succes van de campagne moet dan worden gecontroleerd om te zien of er verbeteringen mogelijk zijn wanneer in de toekomst een nieuwe campagne moet worden gehouden.

4.1: Evaluate campaign effectiveness

Het resultaat van de campagne moeten worden vergeleken en gemeten met de metrics die in de eerste fase van dit proces zijn gedefinieerd. Het is belangrijk dat de gemeten resultaten accuraat zijn omdat er verschillende factoren zijn die de validiteit kunnen beïnvloeden. De gemeten effecten moeten dan vervolgens worden vergeleken met de doelstellingen die in het begin van het programma zijn gedefinieerd. De effectiviteit van het programma kan bekend worden wanneer de resultaten met de doelstellingen zijn vergeleken.

4.2: Revise campaign/programme

De volgende fase om de effectiviteiten van een informatiebeveiliging awareness campagne te verzekeren, is om het af te zetten tegen hetgeen wat geleerd is.

Input voor het revisie proces kan zijn:

- Resultaten van 'pilot' campagnes die gegeven zijn aan een gelimiteerd publiek;
- Formele vragenlijsten over de campagne;
- Interviews met belangrijkste deelnemers om er achter te komen wat succesvol is geweest en wat beter kon.

4.3: Run further campaigns

Een informatiebeveiliging awareness programma bevat één of meerdere awareness campagnes. Deze campagnes kunnen op reguliere basis worden herhaald om personeel aan de boodschap te herinneren.

Het is belangrijk om het doel van het programma te behouden door:

- Campagnes herzien: Het optimaliseren van campagnes door de ervaringen van eerdere campagnes er in te verwerken;
- Campagnes herhalen: een campagne herhalen om het personeel te herinneren aan de boodschap van de campagne;
- Nieuwe campagnes te introduceren: ervoor zorgen dat het informatiebeveiliging awareness programma een breed scala aan awareness onderwerpen behandelt.

4.5 Conclusie

Het creëren van awareness onder medewerkers is het belangrijkste aspect in informatiebeveiliging maar is tegelijkertijd een lastige en moeizame aangelegenheid. Organisaties zijn daarin afhankelijk van de medewerkers, zij moeten ervoor open staan om hun gedrag te willen veranderen om bij te dragen aan de veiligheid van informatie. Het beïnvloeden van het gedrag van medewerkers is het belangrijkste onderdeel in het creëren van awareness onder medewerkers en is voor organisaties een noodzakelijke organisatorische maatregel. Het gedrag van medewerkers moet zodanig worden beïnvloed en/of veranderd, dat het leidt tot een verhoogd veiligheidsbewustzijn bij iedereen in de organisatie. Bij veel organisaties wordt echter het nut en de noodzaak van awareness niet ingezien vanwege de kosten en de tijd die ermee gemoeid gaat, maar ook doordat informatiebeveiliging nog vaak wordt gezien als iets dat specifiek toebehoort aan de ICT afdeling. Zij zijn immers verantwoordelijk voor de veiligheid van de informatie, informatiesystemen en de informatievoorzieningen. Maar het creëren van awareness onder medewerkers is iets wat net zo belangrijk is omdat medewerkers diegene zijn die veel met informatie omgaan en zij er dus voor verantwoordelijk zijn dat er op een correcte manier met de informatie, informatiesystemen en de informatievoorzieningen wordt omgegaan. Medewerkers van een organisatie moeten inzien dat zij één van de belangrijkste schakels zijn in de beveiliging van informatie en er daardoor ook zo naar gaan handelen. Hun gedrag moet hierin worden veranderd en de organisatie moet erop toezien dat het ook daadwerkelijk

gebeurt. De belangrijkste methode hierin is om een effectief awareness programma op te zetten met een bijbehorende campagne om zo het gedrag van de medewerkers te beïnvloeden en te veranderen met als einddoel om uiteindelijk onbewust bekwaam met informatie om te gaan.

5. Informatiebeveiliging, social engineering en awareness bij ziekenhuizen

Dit hoofdstuk beslaat het empirische gedeelte van dit onderzoek. Om de onderzoeksvraag te kunnen beantwoorden, zijn in totaal vijf experts (met betrekking tot informatiebeveiliging) van vijf verschillende ziekenhuizen geïnterviewd. In dit hoofdstuk zullen deze interviews worden besproken en geanalyseerd. Tot slot volgt er een conclusie met bijbehorende aanbevelingen.

5.1 Opzet en uitvoering interviews

In deze subparagraaf wordt uiteengezet hoe de interviews tot stand zijn gekomen. Met deze interviews, die bij vijf verschillende ziekenhuizen zijn gehouden, wordt geprobeerd om de deelvragen 5 en 6 van de onderzoeksvraag te beantwoorden. In deze subparagraaf zal worden aangegeven hoe de interviews zijn opgezet, wat het doel van het interview is, welke methode er gebruikt is, welke voorwaarden er door de ziekenhuizen zijn gesteld en hoe de representativiteit van de interviews wordt gewaarborgd.

Opzet interviews
Het interview is opgedeeld in een viertal onderwerpen, die overeenkomen met dit onderzoek. Het eerste deel van het onderzoek is van algemene aard. Het tweede deel gaat in op informatiebeveiliging: bij wie ligt de verantwoordelijkheid, wat is de rol van de medewerkers, hoe verloopt de communicatie van informatiebeveiliging naar de medewerkers en welke maatregelen worden er genomen om de informatiebeveiliging te versterken. Het derde deel richt zich op social engineering: is het ziekenhuis bekend met social engineering, heeft het ziekenhuis weleens te maken gehad met een aanval van social engineering, wat doet het ziekenhuis tegen social engineering en hoe worden de gevaren van social engineering naar de medewerkers gecommuniceerd. Het vierde en laatste deel heeft de nadruk op awareness: wat verstaat het ziekenhuis onder awareness, bij wie ligt de verantwoordelijkheid van awareness, heeft het ziekenhuis een awarenessprogramma en hoe wordt dit gecommuniceerd. In appendix A (pagina 134) is in de bijlage het interviewprotocol te vinden met daarin de volledige vragenlijst.

Doel van het interview
Het doel van het afnemen van de interviews is om de deelvragen 5 en 6 van de onderzoeksvraag te kunnen beantwoorden. Uit de interviews moeten de volgende resultaten naar voren komen:

- Wat verstaat het ziekenhuis onder informatiebeveiliging;
- Bestaat er een informatie beveiligingsbeleid en hoe wordt dit gecommuniceerd naar de medewerkers;
- Is het ziekenhuis bekend met social engineering en de gevaren die het mee brengt;
- Is het ziekenhuis bestand tegen de vele soorten aanvallen van social engineering
- Is er sprake van een veiligheidsbewustzijn ten opzichte van informatiebeveiliging en wat doet het ziekenhuis aan het veiligheidsbewustzijn van medewerkers;

Gebruikte methode
De methode die gebruikt is voor het verzamelen van de informatie is het semi-gestructureerde interview met open vragen. Aan alle geïnterviewde personen zijn dezelfde vooropgestelde vragen gesteld, in dezelfde volgorde. Dit heeft als voordeel dat:

- De analyse en vergelijking van antwoorden minder tijd in beslag zal nemen vanwege de formulering van de vragen;
- Er een hoge mate van betrouwbaarheid zal zijn vanwege het vergelijken van de resultaten van de verschillende interviews;
- Er een grote mate van flexibiliteit is, vanwege zowel het gestructureerde als ongestructureerde karakter van het interview.

Voorwaarden
Sommige ziekenhuizen hebben een aantal voorwaarden gesteld ter medewerking aan dit interview. Om deze reden zijn aan al deze voorwaarden voldaan. Zo zijn in dit onderzoek de ziekenhuizen volledig geanonimiseerd. Er zullen geen namen van ziekenhuizen in voorkomen, tevens zullen ook de namen van de personen die zijn geïnterviewd niet in deze thesis worden opgenomen. Het volledig uitgewerkte interview verslag zal eerst ter goedkeuring worden voorgelegd aan de geïnterviewde. Pas wanneer de geïnterviewde zijn of haar goedkeuring aan het verslag heeft verleend, zal het verslag worden gebruikt voor het onderzoek. Het interview verslag zal ook niet als een bijlage in deze thesis worden opgenomen. Tot slot wilden de geïnterviewden graag allemaal een exemplaar van deze thesis. Aan dit verzoek zal ook worden voldaan en alle geïnterviewden zullen een exemplaar in hun bezit krijgen.

Representativiteit
Om de representativiteit van dit onderzoek zo goed mogelijk te waarborgen, zijn in totaal twaalf ziekenhuizen benaderd, waarbij overigens geen onderscheidt is gemaakt tussen een Universitair Medisch Centrum (UMC) en een ‘gewoon’ ziekenhuis. Van de twaalf ziekenhuizen, hebben vijf ziekenhuizen positief gereageerd en waren bereidt om mee te werken aan dit onderzoek. De andere zeven ziekenhuizen wensten niet mee te werken of hadden geen tijd voor participatie aan dit onderzoek. De personen van de vijf ziekenhuizen die geïnterviewd zijn, zijn allemaal betrokken bij de informatiebeveiliging van het ziekenhuis. Omdat aan dit onderzoek vijf ziekenhuizen hebben meegewerkt, en er in Nederland meer dan 100 ziekenhuizen zijn, spreekt het voor zich dat het zeer moeilijk is om de resultaten uit dit onderzoek te laten gelden voor alle ziekenhuizen in Nederland. De uitkomsten en de resultaten van dit onderzoek zijn daarom alleen van toepassing op de vijf geïnterviewde ziekenhuizen. Het wil overigens niet zeggen dat de resultaten van dit onderzoek niet van toepassing kunnen zijn op andere ziekenhuizen. Het is denkbaar dat andere ziekenhuizen dit onderzoek kunnen gebruiken voor hun informatie beveiligingsbeleid en de omgang met social engineering. Om deze reden kan dit onderzoek ook van toegevoegde waarde voor andere ziekenhuizen zijn.

5.2 Verwerking interviewresultaten

In deze paragraaf wordt uiteengezet hoe de resultaten uit de vijf afgenomen interviews zijn verwerkt en wat de resultaten van de vijf interviews zijn. De vijf interviews zijn allen opgenomen met audioapparatuur, zodat naderhand het interview volledig kon worden uitgetypt. Dit volledig uitgewerkte interviewverslag is eerst ter goedkeuring bij de geïnterviewde neergelegd. De informatie uit het interviewverslag werd dan ook pas gebruikt voor dit onderzoek wanneer deze goedkeuring door de geïnterviewde is gegeven. Wijzigingen zijn dan ook naderhand toegepast wanneer dit door de geïnterviewde nodig werd geacht. Met behulp van het programma WEFT QDA, zijn vervolgens de vijf interview verslagen geanalyseerd. WEFT QDA is een software programma dat hulp biedt bij de analyse van ongestructureerde tekstuele data zoals interview verslagen en bij documenten. Hierdoor kunnen patronen worden ontdekt om de onderzoeksvraag goed te kunnen beantwoorden.

In de volgende drie subparagrafen zullen de resultaten uit de interview verslagen worden beschreven. Bij het analyseren en vastleggen van deze resultaten is met name gekeken naar de relevantie met de onderzoeksvraag en deelvragen. Informatie uit de interview verslagen die naderhand overbodig bleken te zijn, zijn niet in de resultaten opgenomen. De resultaten worden beschreven in relatie tot het interviewprotocol, dat wil zeggen dat de volgorde van het interview word aangehouden. Hierdoor krijg je een overzichtelijke structuur en kunnen er betere en snellere conclusies worden getrokken.

5.2.1 Ziekenhuizen en informatiebeveiliging

Alle vijf geïnterviewde ziekenhuizen zien uiteraard het belang in van een goede informatiebeveiliging en gaan er op hun eigen manier mee om. De verschillende definities die de ziekenhuizen voor informatiebeveiliging gebruiken, komen bijna allemaal met elkaar overeen, op enkele details na. Enkele definities die door ziekenhuizen gebruikt worden zijn:

> *'Informatiebeveiliging wil zeggen dat de informatie die gebruikt wordt in je processen, dat die geclassificeerd zijn, dat je weet welke informatie er is en dat daar de juiste maatregelen voor getroffen zijn. Daarnaast moet die informatie ten allen tijde beschikbaar zijn, integer zijn en moet er vertrouwelijk mee worden omgegaan.'*

> *'Het zorg dragen dat de informatie binnen het ziekenhuis, in welke vorm dan ook, papier, digitaal, of in het hoofd, beschikbaar is, betrouwbaar blijft en vertrouwelijk mee wordt omgegaan.'*

> *'Het treffen en onderhouden van je maatregelen om de betrouwbaarheid van je informatievoorziening te borgen. Dit alles gaat gepaard met het bekende rijtje, beschikbaarheid, integriteit en vertrouwelijkheid en ook een stuk controleerbaarheid.'*

> *'Informatie beveiliging draait rondom de drie speerpunten beschikbaarheid, integriteit en vertrouwelijkheid en wordt ook als zodanig in dit ziekenhuis gecommuniceerd.'*

Zoals te zien is in de verschillende definities van informatiebeveiliging, spelen de begrippen beschikbaarheid, integriteit en vertrouwelijkheid een belangrijke rol in de informatiebeveiliging van de ziekenhuizen. Met beschikbaarheid en vertrouwelijkheid wordt door de ziekenhuizen

over het algemeen hetzelfde mee bedoeld. Beschikbaarheid wordt omschreven als *'informatie dat beschikbaar moet zijn op het moment dat het ook daadwerkelijk gewenst is'* en vertrouwelijkheid wordt omschreven als *' informatie dat voor het werk en de behandeling gebruikt wordt, moet vertrouwelijk en zorgvuldig mee worden omgegaan door de juiste personen.'* Over integriteit is er geen eenduidig beeld. Integriteit wordt door vier ziekenhuizen omschreven als *'informatie moet ten allen tijde juist en correct zijn en er tevens zeker van zijn dat de informatie goed is ingevoerd en niet gemanipuleerd is.'* Eén ziekenhuis ziet dit niet als integriteit maar als betrouwbaarheid. Integriteit wordt door dit ziekenhuis omschreven als *'erop kunnen vertrouwen dat de handelingen van de medewerker in het kader van zijn of haar functie gebeurt'.* Dit wil zeggen dat medewerkers van het ziekenhuis die met patiënteninformatie in aanraking komen, dit alleen maar gebruiken waanneer zij een behandelrelatie met de desbetreffende patiënt hebben. Dit betekent dat er bijvoorbeeld niet naar informatie van vrienden, collega's of wie dan ook wordt gekeken. Met andere woorden, er moet integer met informatie worden omgegaan.

De verantwoordelijkheid over informatiebeveiliging is bij de geïnterviewde ziekenhuizen verschillend. Bij drie ziekenhuizen ligt deze eindverantwoordelijkheid helemaal bovenin, bij de raad van bestuur. Bij één van deze twee ziekenhuizen is wel de verantwoordelijkheid neergelegd bij de verschillende afdelingshoofden, dat wil zeggen dat elke afdeling verantwoordelijk is voor de informatiebeveiliging van de eigen afdeling. Bij het andere ziekenhuis heeft de geïnterviewde aangegeven verantwoordelijk te zijn dat informatiebeveiliging binnen het ziekenhuis leeft en daadwerkelijk ook groeit. Maar de geïnterviewde is niet eindverantwoordelijk, dat is de raad van bestuur en de uitvoering ligt vervolgens bij de medewerkers. Bij twee ziekenhuis zijn de geïnterviewden ook daadwerkelijk verantwoordelijk voor de informatiebeveiliging om collega's en andere medewerkers daarin te begeleiden. Eén van de geïnterviewden heeft het informatie beveiligingsbeleid ook daadwerkelijk geschreven en ook valt zijn functie rechtstreeks onder de raad van bestuur waardoor snelle communicatielijnen mogelijk zijn.
Drie van de vijf geïnterviewden geven daarnaast aan dat hoewel de raad van bestuur verantwoordelijk is voor de informatiebeveiliging van het ziekenhuis, de uitstraling van het belang van een goede informatiebeveiliging naar alle medewerkers beter kan. Dit wordt volgens deze drie geïnterviewden te weinig gedaan.

Op de vraag welke informatie binnen het ziekenhuis het meest gevoelig is, is er een eenduidig antwoord, namelijk patiënteninformatie. Er bestaat een vertrouwensrelatie tussen arts en patiënt, en de informatie tussen deze twee partijen is geheim. Artsen hebben een beroepsgeheim en de patiënt is in feite eigenaar van zijn of haar eigen informatie. Het ziekenhuis heeft deze informatie in bruikleen. De schade die optreedt is van grote invloed op het ziekenhuis en de patiënt wanneer deze informatie, om wat voor reden dan ook, op straat komt te liggen. Voor de patiënt geldt dan dat de privacy niet wordt gewaarborgd en het ziekenhuis heeft dan met name te maken met imagoschade. Dit kan grote gevolgen hebben en kan ook leiden tot grote schadeclaims. Dat zijn zaken waarvan ziekenhuizen willen dat het niet in de publiciteit komt, want dan is de kans groot dat mensen kiezen voor een ander ziekenhuis. Eén van de geïnterviewden heeft dat ook aangegeven door middel van de volgende quote: *"En ook mega imagoschade, je zou zomaar voor Pauw en Witteman kunnen worden opgeroepen en de directeur of raad van bestuur mag het dan gaan uitleggen"*.
Daarnaast behoort patiënteninformatie altijd beschikbaar en integer te zijn. Als informatie verkeerd wordt ingevoerd en daardoor bijvoorbeeld het linkerbeen wordt geamputeerd in

plaats van het rechterbeen, dan is het leed van de patiënt, de imagoschade voor het ziekenhuis en de bijbehorende schadeclaim ook niet te overzien.

De rol van de medewerkers in informatiebeveiliging is ook groot binnen de ziekenhuizen. Iedereen is gebruiker van de informatie binnen het ziekenhuis en behoort zorgvuldig met die informatie om te gaan. Alle medewerkers hebben ook een eigen account, waardoor de rol van de medewerkers in de beveiliging van informatie groot is. Zij moeten zorgvuldig met hun eigen account omgaan en daardoor de informatie beschermen. Dit is nog weleens een heikel punt in een ziekenhuis omdat er zowel algemene als persoonlijke accounts voorkomen. Dit is iets wat door vier van de geïnterviewden wordt aangestipt. Op de spoedeisende hulp van een ziekenhuis bijvoorbeeld is het erg hectisch waardoor het niet handig is om telkens in te loggen met een persoonlijk wachtwoord. Wat dus veel voorkomt zijn algemene accounts met wachtwoorden zodat iedereen er snel bij kan. Het nadeel is dan dat het niet duidelijk is wie verantwoordelijk is voor welke invoer.

Alle vijf de ziekenhuizen hebben ook eigen gedragsregels voor de medewerkers in het omgaan met informatie. Hierin staat hoe er moet worden omgegaan met e-mail en internet gebruik. Deze zijn in het beleid opgenomen en staan ook op de intranetsite van de ziekenhuizen vermeld. Drie van de geïnterviewden geeft ook duidelijk aan dat de kans groot is dat veel medewerkers het informatie beveiligingsbeleid en dus de gedragsregels niet lezen of niet weet waar ze deze moeten vinden. Ook geven zij aan dat het intranet gebruik in het ziekenhuis vrij matig is. Een quote uit één van de interviews hierover is: "*We hebben ook ICT gedragsregels, dus hoe ga je om met je pc etc. en die staan ook gepubliceerd op intranet maar dat wil niet zeggen, er zullen nog steeds een hele hoop mensen die zeggen van "goh dat wist ik niet"* en een andere quote uit een ander interview *"Ja, dat is nog heel, hoe moet ik dat zeggen, primitief. We hebben een e-mail en internet reglement, we hebben een clear-desk en clear-screen policy en een aantal vuistregels dat in het kader van de opleiding wordt meegegeven. Deze regels zijn ook beschikbaar en staan op intranet, maar het intranet gebruik van het ziekenhuis is erg matig"*.

De communicatie van het informatie beveiligingsbeleid naar de medewerkers gaat op verschillende manieren. Bij drie ziekenhuizen wordt het informatie beveiligingsbeleid onder de aandacht gebracht bij nieuwe medewerkers in de opleiding. Bij één van deze drie ziekenhuizen moeten de medewerkers ook daadwerkelijk tekenen dat ze het beleid kennen. Bij een ander ziekenhuis wordt er in de opleiding een halve dag aan informatiebeveiliging besteedt, de nieuwkomers krijgen dus een duidelijke voorlichting, terwijl de rest een beetje wordt verwaarloosd. Daarnaast komen bij twee van deze drie ziekenhuizen het informatie beveiligingsbeleid ook aan bod in bewustwordingpresentaties en campagnes. Bij één ziekenhuis wordt de communicatie van het informatie beveiligingsbeleid alleen meegenomen in een bewustwordingsprogramma en bij één ziekenhuis wordt dit beleid niet gecommuniceerd, behalve dan dat het op intranet gepubliceerd staat. Een quote uit een interview hierover: "*Ja, dat neem ik dus mee in het awarenessprogramma. Maar daar ga ik geen al te veel woorden aan vuil maken omdat ik weet dat ze dat niet lezen*".

Er zijn verschillende dreigingen die een gevaar kunnen vormen voor de verschillende informatie assets van een ziekenhuis. De grootste dreigingen zijn vooral virussen en malware. Deze bedreigingen kunnen voor systeem uitval zorgen waardoor de beschikbaarheid van informatie gevaar loopt, en in iets mindere mate ook de integriteit en de vertrouwelijkheid. Nog een andere dreiging dat een gevaar kan vormen, is diefstal. Eén geïnterviewde geeft aan dat

het weleens voorkomt dat er een laptop of pc wordt gestolen.

De meeste gevoelige plekken in een ziekenhuis, waar met informatie wordt omgegaan zijn de patiëntendossiers. Dit wordt door drie van de geïnterviewden nadrukkelijk aangegeven. Patiëntendossiers zijn gedeeltelijk digital en gedeeltelijk niet-digitaal. Met digitale patiëntendossiers moet veilig worden omgegaan, veel informatie wordt in een systeem gezet. Dit kan voor zwakheden zorgen want deze systemen staan open en er moet dus veilig mee worden omgegaan. Met niet-digitale patiëntendossiers is er het gevaar dat deze komen te liggen op plaatsen waar ze niet horen te liggen. Bijvoorbeeld door te veel dossiers op een bepaalde locatie te bewaren waardoor ze niet meer allemaal kunnen worden opgeruimd in de archiefkast en er dus een groot aantal dossiers liggen rond te slingeren. Dit geldt ook voor poliklinieken, waar veel met dossiers wordt gewerkt. Wanneer er geen personeel aanwezig is bij een polikliniek en er liggen patiëntendossiers, dan kan dit een gevaar betekenen voor de informatie in deze dossiers. Twee geïnterviewden geven ook duidelijk aan dat er nog een ander risico is, en dat is nieuwsgierigheid bij de eigen medewerkers. Medewerkers hebben op grond van hun autorisatie toegang tot het systeem en het risico bestaat dat medewerkers zich niet aan afspraken en richtlijnen houden. Bijvoorbeeld als een collega wordt opgenomen en medewerkers hun nieuwsgierigheid niet kunnen bedwingen en even willen kijken waarom hun collega wordt opgenomen. Deze twee geïnterviewden geven duidelijk aan dat inbreuk van eigen medewerkers, dus niet mensen van buiten of hackers, maar eigen personeel dat zich niet integer gedraagt, een gevaar kan vormen.

Ziekenhuizen nemen uiteraard maatregelen om deze bedreigingen ter verminderen, hoewel volgens de geïnterviewden het lastig is om een ziekenhuis te beveiligen, met name fysieke beveiliging, omdat een ziekenhuis een open instelling is en iedereen gewoon naar binnen kan lopen. Een quote uit een interview hierover: *"Ja, dat is een hele lastige, jan en alleman komt hier binnen en dat is een nadeel. Je kunt niet zeggen "die groep komt niet binnen", dat kan niet want die groep moet ook verpleegd worden. Het enigste wat je eraan kunt doen is protocollen, afspraken maken"*
Wat gedaan wordt is om niet-publieke ruimtes en ruimtes waar met informatie gewerkt wordt te beveiligen, dat betekent deze ruimtes afsluiten wanneer er niemand aanwezig is. Alle geïnterviewden geven ook aan dat dit lastig is omdat medewerkers van een ziekenhuis veel in beweging zijn en dus vaak ergens anders moeten zijn. Hierdoor worden vaak niet alle ruimtes op slot gedaan wanneer er niemand aanwezig is. Ook balies van poliklinieken zijn lastig om te beveiligen omdat deze in feite altijd open moeten zijn voor patiënten en een gesloten poliklinieken is iets wat niet patiëntvriendelijk overkomt.
Ook is het verplicht voor alle medewerkers van de vijf ziekenhuizen om identificatie te dragen, dat wil zeggen een pasje van het ziekenhuis dat aangeeft dat je ook daadwerkelijk in dienst bent van het ziekenhuis. Drie van de geïnterviewden geven aan dat hoewel het verplicht is om een pasje zichtbaar te dragen, het geen goede veiligheidsmaatregel is omdat mensen die geen pasje dragen naar alle waarschijnlijkheid niet zullen worden aangesproken.
De logische maatregelen die door de ziekenhuizen worden genomen hebben vooral betrekking op het wachtwoordenbeleid. Iedere medewerker heeft een gebruikersnaam met wachtwoord en elk ziekenhuis heeft eigen regels hoe er met dit wachtwoord moet worden omgegaan. Drie van de geïnterviewden geven ook aan dat waarschijnlijk dit wachtwoordenbeleid niet bij iedereen bekend zal zijn, net zoals ook de gedragsregels niet bij iedereen bekend zullen zijn, omdat men niet weer waar ze moeten zoeken. Het grootste gevaar in het omgaan met wachtwoorden zit volgens drie geïnterviewden in het opschrijven van de wachtwoorden en deze bijvoorbeeld vervolgens op het scherm te plakken. Dit wil soms nog weleens voorkomen en is uiteraard niet de bedoeling.

Ook werken de ziekenhuizen in sommige gevallen nog met functionele accounts, dus meerdere personen werken op één account met één wachtwoord. Sommige situaties vragen daarnaar, bijvoorbeeld in een operatiekamer of op de spoed eisen hulp waar het vaak druk en hectisch is. In deze gevallen is het niet handig wanneer telkens een ander persoon moet inloggen om iets in te vullen of bij te werken. Dit wordt wel als een probleem gezien want als er foutieve data wordt ingevoerd is het moeilijk om te herleiden wie daar verantwoordelijk voor was.

Er zit een verschil in hoe de maatregelingen voor informatiebeveiliging worden gecontroleerd en nageleefd bij de vijf ziekenhuizen. Twee geïnterviewden geven aan dat daar amper aandacht aan wordt besteedt. Twee andere geïnterviewden geven aan dat het ziekenhuis een clear-desk en clear-screen beleid heeft en dat dit ook wordt gecontroleerd. Eén geïnterviewde geeft aan dat het verschillend is en dat de verantwoordelijkheden zijn verdeeld. Afdelingen zijn zelf verantwoordelijk en dat wordt ook bij de mensen van die afdeling als zodanig neergelegd. Maar deze geïnterviewde heeft geen inzicht of alle afdelingen ook daadwerkelijk aan controle en naleving doen. Een quote uit een interview hierover: "*Ja dat doen wij amper. Als je naar de audit kijkt, waar wij slecht op scoren is die controle op naleving en de systematiek daarvan".*

5.2.2 Ziekenhuizen en social engineering

De vijf mensen van de vijf ziekenhuizen die geïnterviewd zijn geven allen aan bekend te zijn met social engineering, maar geven tegelijkertijd ook duidelijk aan dat dit niet geldt voor veel van het andere personeel. Bijvoorbeeld artsen, verpleegsters en secretaresses zullen niet of nauwelijks bekend zijn met social engineering en de gevaren die daarbij komen kijken. Een quote hierover: *"Ja goed ja, vanuit hier de informatiebeveiliging, een aantal mensen hier wel maar ik denk een hele hoop mensen nog onvoldoende".*

Onder de geïnterviewden bestaat een eenduidig beeld van wat social engineering precies is en wat het kan aanrichten. In de omschrijvingen die zij geven komt het erop neer dat social engineering wordt gezien als een methode om door middel van een smoesje aan allerlei verschillende soorten informatie te komen. Dit kan dan bewerkstelligd worden door op een psychologische manier iemand iets te laten doen wat hij of zij normaal gesproken nooit zou doen, waarbij gebruikt gemaakt kan worden van allerlei middelen. Niet alleen via technische middelen maar vooral door gesprekken aan te knopen met medewerkers en gebruik te maken van de menselijke gebreken. Cruciaal is daarbij de medewerking die wordt gegeven op een vrijwillige basis, dus niet door middel van dwang bijvoorbeeld.

Op de vraag of het ziekenhuis weleens te maken heeft gekregen met een aanval via social engineering, is ook hier eenduidig op geantwoord. Geen van de geïnterviewden weet of er in het verleden een aanval via social engineering heeft plaatsgevonden. Wel wordt aangegeven dat dit niet betekent dat er nooit iets is voorgevallen. Het kan zijn dat er een social engineeringsaanval heeft plaatsgevonden maar dat deze aanval vervolgens niet is opgemerkt. Twee quotes over dit onderwerp: *"Nee volgens mij niet, dat weet ik niet. Als het wel gebeurd is, dan hebben ze het goed gedaan"* en *"Niet dat ik weet. Alles wat er bekend is, gaat niet over social engineering."* Wel geven twee geïnterviewden aan dat hun ziekenhuis de laatste tijd last heeft van zogenaamde phishing mails, waarin word 'gevist' naar wachtwoorden van medewerkers. In één ziekenhuis heeft dit er toe tot geleidt dat een medewerker ook daadwerkelijk zijn of haar wachtwoord heeft prijsgegeven.

Social engineering wordt door drie van de geïnterviewden als een gevaar voor het ziekenhuis gezien en wat tevens een reële kans van slagen heeft, twee van de geïnterviewden zien dit wat minder. Zij zien wel het gevaar in van social engineering, maar vinden het lastig om te geloven dat iemand door middel van een social engineering aanval aan patiënteninformatie probeert te komen. Zij vragen zich af wat iemand met die informatie zou willen doen en uitrichten. Enkele quotes uit de interviews hierover: "*Het feit dat iemand zich hierbinnen voordoet als "goh ik ben die en die, kun jij me eventjes helpen of heb je even dat en dat voor mij" en op die manier probeert om op een nette manier informatie te stelen of te manipuleren, heeft denk ik een reële kans van slagen*" en *"Als men kwaadwillend wil zijn en men doet het via social engineering, dan lukt het. Als men kwaadwillend wil via techniek, dan is het al moeilijker."*

Een persoon die via social engineering een aanval uitvoert, probeert in te spelen op de psychologische eigenschappen van de mens. Op de vraag welke psychologische eigenschappen het meest kwetsbaar zijn bij ziekenhuismedewerkers, wordt door vier van de geïnterviewden aangegeven dat de eigenschap behulpzaamheid waarschijnlijk het meest kwetsbaar is. In ziekenhuizen werken namelijk mensen die van nature erg behulpzaam zijn en het helpen van mensen zit ook in hun aard. Een andere eigenschap die door twee geïnterviewden als kwetsbaar wordt gekenmerkt is de eigenschap autoriteit. Mensen die in ziekenhuizen werken kunnen gevoeliger voor autoriteit zijn dan anderen. Een arts straalt namelijk behoorlijk wat autoriteit uit en veel mensen kunnen daar gevoelig voor zijn. Enkele quotes uit de interviews: "*Behulpzaam zijn he, dat ligt ook in de aard van de verpleging hier. Dat is de aard waarom ze het doen. Dus ja dat ligt hier heel gevoelig. En ja dat kun je ze wel uitleggen maar ik denk dat je daar niet tegen kunt wapenen*", *"Ik denk het wel, ik denk dat een ziekenhuis juist extra kwetsbaar is. Ziekenhuismedewerkers zijn meestal altijd erg behulpzaam en willen altijd helpen"* en *"Ja ik denk dat de gemiddelde medewerker in de zorg gevoeliger is voor autoriteit dan anderen. We hebben hier natuurlijk een systeem he, kijk ik bedoel een arts is wat anders dan een arts-assistent en dat schilt wel. Ik denk ook wel als jij inderdaad een witte jas aanhebt dat je sommige medewerkers makkelijker overtuigt."*

Het ziekenhuis beschermen tegen social engineering is volgens de geïnterviewden zeer lastig. Iedereen kan binnenlopen in een ziekenhuis en dat maakt het lastig te beveiligen. Er zijn volgens de vijf geïnterviewden twee zaken die hierin kunnen helpen. Het eerste is een helder en duidelijk beleid dat bij de medewerkers bekend moet zijn. Dat betekent dat medewerkers zich moeten houden aan afspraken en protocollen (gedragsregels). Voorbeelden die worden gegeven zijn: nooit wachtwoorden weggeven, want daar zal door mensen van het ziekenhuis nooit om worden gevraagd en altijd met externe mensen meelopen wanneer zij ergens in het ziekenhuis moeten zijn. Het tweede dat kan helpen is bewustwording en social engineering meenemen in bewustwordingscampagnes. Duidelijk maken aan medewerkers dat social engineering bestaat en dat dit een gevaar kan zijn voor het ziekenhuis. Het moet medewerkers duidelijk worden dat er voorzichtig met informatie moet worden omgegaan en dat informatie nooit zomaar mag worden weggeven. Een quote uit een interview hierover: "*Bewustwording, dat is eigenlijk het enige. Tegen diefstal kun je wat doen, kabeltjes eraan, encrypted harde schijf, verzin maar allemaal technieken en maatregelen. Maar tegen ongeoorloofd toegang verlenen, uitgeven van een account door phishing, ja wat kun je daar tegen doen. Bewustheid bij de medewerkers, dat moet omhoog.*"

Eén geïnterviewde geeft aan dat het ziekenhuis een extra maatregel heeft genomen om ervoor te zorgen dat medewerkers hun wachtwoorden niet zullen prijsgeven. Persoonsgegevens, zoals bijvoorbeeld functioneringsgesprekken, waarvan je niet wilt dat andere mensen die te zien krijgen, zullen onder hetzelfde account komen te staan als waarmee je inlogt. Hiermee denkt dit ziekenhuis dat medewerkers minder snel geneigd zullen zijn om bijvoorbeeld wachtwoorden weg te geven. Een andere methode die een geïnterviewde aanhaalt is het vernietigen van gevoelige informatie. Deze informatie gaat in aparte containers en wordt apart vernietigd. Ook gebruikt het ziekenhuis volgens deze geïnterviewde een clear-desk en clear-screen beleid en wordt er weleens ergens binnengelopen om te kijken wat er allemaal ligt. Wanneer blijkt dat er iets niet klopt, zoals een opgeschreven wachtwoord op een computerscherm, dan wordt die persoon aangesproken of wordt er een notitie achtergelaten. Dit laatste wordt ook door een ander ziekenhuis toegepast.

Een bekende social engineering aanval is impersonation (jezelf voordoen als iemand anders). Aan de vijf geïnterviewden is de volgende vraag voorgelegd:

> *Stel dat een social engineer zich voordoet als bijvoorbeeld een helpdeskmedewerker en telefonisch contact opneemt met medewerkers met de vraag of de wachtwoorden van medewerkers wel voldoen aan de nieuwe beveiligingseisen. Deze medewerker geeft vervolgens zijn of haar wachtwoord weg.*
>
> - *Hoe kan deze aanval worden voorkomen en welke acties of maatregelen kunnen worden ondernomen om deze aanval tegen te gaan?*

Volgens alle geïnterviewden is deze aanval zeer moeilijk te voorkomen en kan eigenlijk alleen maar worden voorkomen door middel van bewustwording en de mensen er op te wijzen dat je zaken zoals wachtwoorden nooit moet prijsgeven. Twee van de geïnterviewden geven overigens duidelijk aan dat als deze aanval zou worden uitgevoerd, de kans van slagen groot is.

De gevaren van social engineering worden niet expliciet gecommuniceerd naar de medewerkers volgens de geïnterviewden. Wel wordt dit, zoals wordt aangegeven door twee van de geïnterviewden, gedaan in algemene zin. Door bijvoorbeeld in awarenes sessies duidelijk te maken dat je alert moet zijn in wat er om je heen gebeurt, door altijd je identificatiepas zichtbaar te dragen, door poster op te hangen en flyers te verspreiden. Dit zijn enkele voorbeelden die werden aangehaald. Twee geïnterviewden hebben aangegeven dat ze in de toekomst social engineering wel expliciet onder de aandacht willen brengen bij medewerkers maar dat ze nu nog te weinig voorbeelden hebben dat social engineering een gevaar kan vormen voor het ziekenhuis.

5.2.3 Ziekenhuizen en awareness

Awareness (veiligheidsbewustzijn) wordt door de geïnterviewden vooral gekenmerkt door het feit dat je ervan bewust moet zijn hoe er met informatie moet worden omgegaan, het herkennen van de waarde van informatie en er ook zo naar handelen. Enkele definities die de geïnterviewden hebben gegeven zijn:

'Dat mensen weten dat je met vertrouwelijke informatie omgaat, dat ze ook snappen dat het er is, weten wat ze er mee moeten doen en ook zo handelen. Dat zou ik awareness vinden.'

'Dat onbewust, bewust er door middel van procedures en protocollen goed met informatie wordt omgegaan.'

Awareness, het bewustzijn van de medewerkers, in de breedste zin van het woord, medewerkers van boven naar beneden, dwars door de hele organisatie, ook de tuinmannen, de mensen van algemene techniek die de papier kliko's leeggooien. Het bewustzijn van het feit dat wij hier in huis informatie hebben waar je veilig mee moet omgaan. En dan kan over bouwplannen gaan, het kan over patiënteninfo gaan, de investeringsbegroting van volgend jaar, etcetera.

Kort gezegd, kennis, gedrag en houding van medewerkers omtrent het veilig beschermen van je informatie.

Het herkennen en ook het bewustzijn hebben van de waarde van informatie en ook van de risico's. Dat je dus echt snapt waar je mee bezig ben als die informatie langskomt.

De factoren die een rol spelen in het creëren van een veiligheidsbewustzijn, zijn vooral door de mensen bewust te maken van informatieveiligheid, de rol die zij daarin spelen en door kennis bij te brengen over hun verantwoordelijkheden. Voorbeelden die de geïnterviewden aanhalen die hierin helpen zijn onder andere awareness campagnes, mensen aanspreken op hun gedrag, doelstellingen vertalen in concrete zaken zoals straffen en belonen (goed gedrag belonen en verkeerd gedrag straffen) en het hebben van een 'open mind'. Medewerkers moeten er open voor staan en moeten informatiebeveiliging willen omarmen, anders heeft het geen zin.

Bij wie de verantwoordelijkheid ligt voor de awareness in de ziekenhuizen, is nogal verschillend op gereageerd. Eén geïnterviewde geeft aan dat dit een lastige vraag was en dat het niet duidelijk is, wie voor awareness binnen het ziekenhuis verantwoordelijk is. Twee van de geïnterviewden geven aan dat de verantwoordelijkheid bij de verschillende afdelingen liggen, dat wil zeggen dat elke afdeling zelf verantwoordelijk is voor de awareness onder medewerkers. Eén geïnterviewde geeft aan dat die verantwoordelijkheid bij hemzelf ligt en één geïnterviewde laat weten dat de verantwoordelijkheid van awareness onder medewerkers bij de afdeling communicatie ligt. Dat blijkt uit de volgende quote: "*Wat je ziet is, we hebben een afdeling communicatie die daar nog het dichtst bij in de buurt komt. Dus als het over bewustwording of over ontwikkeling gaat bijvoorbeeld dan komen zij in beeld om daar voorrang aan te geven*."

Het antwoord op de vraag of het ziekenhuis het nut inziet van een goede awareness onder medewerkers, komt bij de geïnterviewden redelijk overeen. Bij vier van de geïnterviewden komt naar voren dat het ziekenhuis wel het nut ervan inziet maar dat het in de praktijk nog beter kan worden uitgedragen, en dan met name door de raad van bestuur. Één van de geïnterviewden geeft aan dat dit één van de belangrijkste aandachtspunten is vanuit het organisatorisch perspectief. Het wordt in dit ziekenhuis door de raad van bestuur ook daadwerkelijk uitgestraald dat dit een belangrijke zaak is en hebben om deze reden ook een awareness campagne geïnitieerd.

Een awareness programma voor de medewerkers van het ziekenhuis ziet er bij de vijf geïnterviewde ziekenhuizen verschillend uit. Het ene ziekenhuis doet meer aan het kweken van awareness dan het andere ziekenhuis. Zo laat één geïnterviewde weten wel een soort van awareness programma te hebben, maar dat het nog heel pril is. Er wordt niet specifiek iets aan awareness gedaan, zo worden er geen folders verspreidt of posters opgehangen, enkel wordt iets op intranet vermeld en in het personeelsblaadje gezet. Een quote uit het interview hierover: *"Dat hebben we wel, maar dat is nog heel pril. Het is ook omdat die norm dat voorschrijft. We hebben in ons clubblaadje het één en ander gezet en we gaan dus in die veiligheidsrondes awareness inbouwen."* Een andere geïnterviewde laat weten dat er wel ooit een awareness programma is geweest, maar dat daar op dit moment nieuw leven in wordt geblazen. Bij dit ziekenhuis komt er een awareness programma dat ondersteund wordt door informatie beveiligingsessies, posters en notitieblokjes voor medewerkers. Een quote uit het interview hierover: *"Het is er ooit geweest, vier, vijf jaar geleden, en daar wordt nu dadelijk nieuw leven ingeblazen. Dus het komt er wel aan, zeer zeker."*
Eén geïnterviewde vertelt dat hijzelf een verhaal houdt waarbij hij het heeft over informatiebeveiliging (beschikbaarheid, integriteit, vertrouwelijkheid), wat hij doet en waar hij bereikbaar is en hij laat wat voorbeelden met filmpjes zien. Deze geïnterviewde laat ook weten dat hij dit verhaal naar alle medewerkers van het ziekenhuis wil communiceren. Daarnaast doet dit ziekenhuis aan awareness via posters, stickers en intranet.
Een andere geïnterviewde laat weten dat het awareness programma van het ziekenhuis een soort van algemene uitstralingsbewustwording omvat, waarbij de situatie van thuis gekoppeld wordt aan de situatie van het ziekenhuis. Dat wil zeggen dat de manier waarop je thuis met gevoelige informatie omgaat, je op precies dezelfde manier om moet gaan met gevoelige informatie van het werk. Als je medewerkers daar mee weet te raken, krijg je awareness volgens deze geïnterviewde. Daarnaast is er een aparte pagina op het intranet te vinden waar alles terug te vinden is, van het informatie beveiligingsbeleid tot presentaties.
De geïnterviewde van het ziekenhuis waar de raad van bestuur de belangrijkheid en het nut van awareness ook echt uitstraalt, laat weten dat alle medewerkers een brief en een folder hebben gekregen vanuit de raad van bestuur en daarnaast hebben alle medewerkers meegedaan aan een enquête. Alle medewerkers van de verschillende afdelingen krijgen van de desbetreffende afdelingshoofden daarnaast elke maand nog een aparte brief. Het doel was om een basisbewustzijn te creëren bij de medewerkers om van daaruit gerichter te werk gaan. Dit is vervolgens gedaan door middel van onder andere gebruik te maken van intranet, introductiecursussen, folders, flyers en beveiligingsmedewerkers die met een notitieblokje rondlopen waarmee ze kunnen aangeven wat ze aantreffen.

5.3 Analyse interviewresultaten

In deze paragraaf worden de interviewresultaten uit de vorige paragraaf geanalyseerd aan de hand van de theorie uit de hoofdstukken 2, 3 en 4. Het doel is om een beeld te krijgen van het veiligheidsbewustzijn van informatiebeveiliging bij ziekenhuizen in relatie met social engineering

5.3.1 Ziekenhuizen en informatiebeveiliging

In hoofdstuk 2 is de volgende definitie van informatiebeveiliging gedefinieerd:

Informatiebeveiliging is het proces van het vaststellen van de vereiste beveiligingsrichtlijnen , maatregelen en procedures (zowel technisch als niet-technisch) met betrekking tot informatie en informatievoorziening ter waarborging van de vertrouwelijkheid , integriteit en beschikbaarheid van de informatievoorziening

De omschrijvingen van informatiebeveiliging zoals die door de vijf verschillende ziekenhuizen zijn gegeven, komen in grote lijnen overeen met deze definitie. Het belangrijkste is dat in alle van de vijf omschreven definities van informatiebeveiliging, de drie betrouwbaarheidsaspecten (beschikbaarheid, integriteit, vertrouwelijkheid) naar voren komen. Dit betekent dat de vijf geïnterviewden van de ziekenhuizen, het belang van informatiebeveiliging inzien en dit door middel van de drie betrouwbaarheidaspecten proberen te verwezenlijken.

In hoofdstuk 2 zijn de drie betrouwbaarheidsaspecten als volgt gedefinieerd:

Beschikbaarheid (Availability)	Waarborgen dat geautoriseerde gebruikers op de juiste momenten tijdig toegang hebben tot informatie en aanverwante bedrijfsmiddelen.
Integriteit (Integrity)	Het waarborgen van de correctheid en de volledigheid van informatie en verwerking
Vertrouwelijkheid (Confidentiality)	Waarborgen dat informatie alleen toegankelijk is voor degenen die hiertoe geautoriseerd zijn

De vijf geïnterviewden zien de betrouwbaarheidsaspecten als volgt:

Beschikbaarheid (Availability)	*Informatie dat beschikbaar moet zijn op het moment dat het ook daadwerkelijk gewenst is.*
Integriteit (Integrity)	*Informatie moet ten allen tijde juist en correct zijn en er tevens zeker van zijn dat de informatie goed is ingevoerd en niet gemanipuleerd is.* *&* *Erop kunnen vertrouwen dat de handelingen van de medewerker in het kader van zijn of haar functie gebeurt.*
Vertrouwelijkheid (Confidentiality)	*Informatie dat voor het werk en de behandeling gebruikt wordt, moet vertrouwelijk en zorgvuldig mee worden omgegaan door de juiste personen.*

Het aspect beschikbaarheid komt op één belangrijk punt na overeen met de beschrijving van de vijf geïnterviewden. Het is belangrijk dat duidelijk naar voren komt dat beschikbaarheid van informatie alleen geldt voor geautoriseerde gebruikers.

Bij het aspect integriteit is er wel een wezenlijk verschil. Integriteit wordt niet door alle geïnterviewden als hetzelfde gezien en kan op twee manieren worden opgevat: de integriteit van informatie en de integriteit van medewerkers. De integriteit van informatie komt overeen met het gedefinieerde aspect uit hoofdstuk 2, maar de integriteit van medewerkers komt niet terug in één van de aspecten. Het komt nog het meest in de buurt van het aspect vertrouwelijkheid, maar een belangrijk verschil is dat veel mensen in een ziekenhuis toegang tot informatie hebben, terwijl ze eigenlijk geen toegang hoeven te hebben tot die informatie. Hierdoor kunnen er dus integriteitsproblemen bij medewerkers voorkomen wanneer bijvoorbeeld iemand wordt opgenomen die ze kennen en daardoor hun nieuwsgierigheid niet kunnen bedwingen en dus besluiten om even te kijken in het dossier van die kennis. De integriteit van medewerkers kan dan ook het best apart worden gedefinieerd en kan worden gezien als geheimhouding van informatie (zoals ook in hoofdstuk 2 is beschreven):

Geheimhouding (Secrecy)	Informatie uit handen van onbevoegde gebruikers houden

Door dit op deze manier te definiëren wordt dit probleem afgevangen, informatie behoort alleen toegankelijk te zijn voor bevoegde (of geautoriseerde) gebruikers. Integriteit wordt dus gedefinieerd als het waarborgen van de correctheid en de volledigheid van informatie en verwerking. Naast de volledigheid en correctheid van informatie zijn er nog drie kenmerken (zie tabel 9 uit hoofdstuk 2 op pagina 20) die van toepassing zijn op integriteit en die eigenlijk in de definitie horen terug te komen. Geldigheid, authenticiteit en exclusiviteit zijn kenmerken van integriteit van informatie die te belangrijk zijn om te negeren. Informatie moet namelijk up-to-date zijn, de authenticiteit moet kunnen worden vastgesteld en achteraf moet het mogelijk zijn om te verifiëren wie verantwoordelijk is voor welke invoer.

Bij het aspect vertrouwelijkheid is er ook een wezenlijk verschil te zien. De definitie uit hoofdstuk 2 beschrijft dat informatie alleen toegankelijk mag zijn voor geautoriseerde medewerkers, terwijl de geïnterviewden vertrouwelijkheid zien als informatie waar vertrouwelijk en zorgvuldig mee moet worden omgegaan. Dit is toch wel een belangrijk verschillende opvatting maar door het toevoegen van het aspect geheimhouding, is dit opgelost. Informatie dat alleen toegankelijk mag zijn voor geautoriseerde medewerkers, is hetzelfde als informatie uit handen van onbevoegde gebruikers houden. Dus het aspect vertrouwelijkheid uit hoofdstuk 2, komt op hetzelfde neer als het aspect geheimhouding.

Door de interviews met de vijf ziekenhuizen is het duidelijk geworden dat de drie oorspronkelijk betrouwbaarheidsaspecten (beschikbaarheid, integriteit, vertrouwelijkheid) niet voldoende zijn om informatiebeveiliging binnen ziekenhuizen volledig te waarborgen. De toevoeging van een vierde aspect (geheimhouding) is hierin noodzakelijk. Om deze reden wordt ook in de definitie van informatiebeveiliging het aspect geheimhouding opgenomen.

De vier betrouwbaarheidsaspecten van informatiebeveiliging binnen ziekenhuizen zijn dus de volgende:

Beschikbaarheid (Availability)	Waarborgen dat geautoriseerde gebruikers op de juiste momenten tijdig toegang hebben tot informatie en aanverwante bedrijfsmiddelen.
Integriteit (Integrity)	Het waarborgen van de correctheid, de volledigheid, de geldigheid, de authenticiteit en de onweerlegbaarheid van informatie en verwerking.
Vertrouwelijkheid (Confidentiality)	Informatie dat voor het werk en de behandeling gebruikt wordt, moet vertrouwelijk en zorgvuldig mee worden omgegaan door bevoegde personen.
Geheimhouding (Secrecy)	Informatie uit handen van onbevoegde gebruikers houden

Tabel 14: Betrouwbaarheidsaspecten van informatiebeveiliging binnen ziekenhuizen

In hoofdstuk 2 zijn een aantal belangrijke aspecten van informatiebeveiliging uiteengezet waaraan een organisatie moet voldoen wil het de veiligheid van informatie garanderen. Eén van de belangrijkste aspecten is dat de verantwoordelijkheid van informatiebeveiliging bij het bestuur van de organisatie hoort te liggen en dat zij ook daadwerkelijk uitstralen dat informatiebeveiliging van groot belang is voor de organisatie. Als dit niet het geval is, en het bestuur van een organisatie straalt niet het belang van een goede informatiebeveiliging uit, dan is de kans natuurlijk groot dat de medewerkers van die organisatie de veiligheid van informatie niet serieus zullen nemen. Hierdoor kan de informatiebeveiliging van de organisatie in gevaar komen. Uit de interviews is gebleken dat de (eind)verantwoordelijkheid in de meeste gevallen bij de raad van bestuur van het ziekenhuis ligt, maar dat de communicatie naar de medewerkers toe over het belang van een goede informatiebeveiliging beter kan. De raad van bestuur van de ziekenhuizen zou dit nog beter kunnen uitdragen dan dat ze tot nu doen. Bij één ziekenhuis is dit anders en straalt de raad van bestuur duidelijk uit dat informatiebeveiliging belangrijk is en dat vooral de medewerkers hierin belangrijk zijn. Dit doen zij door onder andere een brief naar alle medewerkers te versturen en een enquête te houden onder de medewerkers.

Een ander belangrijks aspect is de naleving en controle op informatiebeveiliging. Het heeft niet echt veel nut om een informatie beveiligingsbeleid te hebben, als het niet mogelijk is om controle en naleving te verzorgen op dit beleid. Twee van de geïnterviewden hebben duidelijk aangegeven dat er in hun ziekenhuis amper aandacht wordt besteedt aan controle en naleving. Twee andere geïnterviewden geven aan dat hun ziekenhuis wel aan controle en naleving doet door andere een clear-desk en clear screen beleid en daadwerkelijke controle hierop. Eén geïnterviewde geeft aan dat de verschillende afdelingen van het ziekenhuis zelf verantwoordelijk zijn voor de controle en naleving op het informatie beveiligingsbeleid maar dat het niet duidelijk is of alle afdelingen aan controle en naleving doen.

De betrouwbaarheid van informatie en de informatievoorziening staan onder constante druk van potentiële bedreigingen. Een bedreiging is een proces of een gebeurtenis dat de kwetsbaarheid van een informatievoorziening of een informatie asset kan uitbuiten. De informatievoorzieningen die het meest gevoelig zijn voor bedreigingen, zijn de informatiesystemen van het ziekenhuis. Wanneer deze om wat voor reden dan ook geïnfecteerd raken, bijvoorbeeld door een virus, kan de beschikbaarheid van informatie in gevaar komen. In het ergste geval kunnen er dan geen operaties bij patiënten plaatsvinden

waardoor er levensgevaarlijke situaties bij patiënten ontstaan. Dit is onlangs voorgekomen bij een ziekenhuis in Hoorn, zoals te zien is in het bericht op bladzijde 24.
De informatie asset die het meest gevoelig is voor bedreigingen in een ziekenhuis, is de patiëntinformatie. Patiëntinformatie is zeer privacygevoelig en mocht informatie van een patiënt, om wat voor reden dan ook, op straat komen te liggen, dan zijn de gevolgen niet te overzien. Naast gigantische imagoschade voor het ziekenhuis wordt ook de privacy van de patiënt aangetast waardoor de patiënt een schadeclaim tegen het ziekenhuis kan indienen. De informatiebeveiliging wordt hier aangetast omdat aan de aspecten vertrouwelijkheid en geheimhouding niet wordt voldaan.
Een andere reden waarom patiënteninformatie gevoelig is voor bedreigingen is vanwege het open karakter van het patiëntendossier. Verschillende mensen binnen het ziekenhuis hebben toegang tot het patiëntendossier en wanneer iemand iets verkeerd invoert in het dossier, kan dit grote gevolgen voor de patiënt hebben. De integriteit van de patiënteninformatie komt vervolgens in het gevaar en daarbij dus ook tegelijk de kenmerken van integriteit: de correctheid, volledigheid, geldigheid, authenticiteit en de onweerlegbaarheid van de informatie. Dit probleem wordt mede gevormd vanwege het feit dat in sommige gevallen functionele accounts noodzakelijk zijn. In een operatiekamer of op de spoedeisende hulp werken verschillende medewerkers die allemaal toegang moeten hebben tot de informatiesystemen. Vaak is het daar zeer hectisch en in dergelijke omstandigheden moeten medewerkers snel en efficiënt gegevens kunnen invoeren. Het is dus niet handig dat elke medewerker dan telkens opnieuw moet in loggen onder zijn of haar eigen account. Vandaar dat in zulke situaties dan gebruik wordt gemaakt van functionele accounts. Iedereen werkt dan onder hetzelfde wachtwoord waardoor het later moeilijk is om te achterhalen wie verantwoordelijk is voor welke invoer.

Naast de dreiging dat patiënteninformatie op straat komt te liggen of dat er foutieve informatie in systemen wordt ingevoerd, zijn er nog een aantal dreigingen uit de interviews naar voren gekomen. Virussen en malware zijn grote dreigingen omdat zoals eerder aangegeven de beschikbaarheid van informatie dan gevaar loopt. Een andere dreiging dat een gevaar kan vormen is diefstal van ICT apparatuur zoals bijvoorbeeld laptops. Ziekenhuizen zijn open instellingen en hebben als doel om zo patiënt vriendelijk mogelijk over te komen. Dit betekent dat iedereen toegang heeft tot het ziekenhuis en dus naar binnen kan lopen. Wanneer bepaalde ruimtes niet worden afgesloten, is het dus mogelijk dat iemand een laptop kan meenemen.
Het open karakter van een ziekenhuis is ook van invloed op de patiëntendossiers met daarin vertrouwelijke en gevoelige informatie over patiënten. Digitale patiëntendossiers kunnen een gevaar lopen wat betreft de betrouwbaarheidsaspecten vertrouwelijkheid en geheimhouding wanneer informatiesystemen niet worden afgesloten wanneer een medewerker het informatiesysteem tijdelijk onbeheerd achterlaat. Dit geldt ook voor niet-digitale patiëntendossiers waar de aspecten geheimhouding en vertrouwelijkheid kunnen worden aangetast. Als niet-digitale patiëntendossiers komen te liggen op plaatsen waar deze niet thuis horen, bijvoorbeeld op poliklinieken waar geen personeel aanwezig is, bestaat de kans dat iemand besluit om even in die patiëntendossiers te kijken. Dit is iets wat een ziekenhuis niet wenst maar door het open karakter van het ziekenhuis, de patiëntvriendelijkheid die het wilt uitstralen en de nonchalance bij medewerkers, is dit wel mogelijk. Een andere dreiging dat uit de interviews naar voren is gekomen, is de nieuwsgierigheid bij het eigen personeel en tast de betrouwbaarheidsaspecten vertrouwelijkheid en geheimhouding aan. Door een aantal geïnterviewden is aangegeven dat het voor medewerkers moeilijk is om hun nieuwsgierigheid

te bedwingen wanneer bijvoorbeeld iemand wordt opgenomen die ze kennen. Vaak wordt dan toch even gekeken waarom die persoon is opgenomen. Dit is iets wat niet de bedoeling is en word gezien als inbreuk van eigen medewerkers.
De communicatie van het informatie beveiligingsbeleid en de bijbehorende gedragsregels naar de medewerkers kan ook een dreiging vormen. Dit gebeurt bij de vijf geïnterviewde ziekenhuizen allemaal op verschillende manieren en in sommige gevallen is aangegeven dat de kans groot is dat veel medewerkers niet bekend zijn met informatie beveiligingsbeleid. Dit komt door de gebrekkige communicatie van het beleid, doordat het beleid moeilijk is terug te vinden op het intranet en het matige gebruik van het intranet in het ziekenhuis. Dit kan mede de oorzaak zijn dat in sommige ziekenhuizen het nog wel eens voorkomt dat medewerkers niet veilig met hun wachtwoord omgaan en het wachtwoord bijvoorbeeld opschrijven en op het beeldscherm van de computer plakken.

De maatregelen die de ziekenhuizen tegen deze dreigingen nemen, kunnen worden gerelateerd aan de drie soorten maatregelen zoals die kort staan beschreven in hoofdstuk 2: Fysieke maatregelen, organisatorische maatregelen en logische maatregelen. Uit de interviews is duidelijk geworden dat een ziekenhuis lastig te beveiligen is vanwege eerder genoemde redenen zoals het open karakter van het ziekenhuis en de patiëntvriendelijke uitstraling van het ziekenhuis. De vijf ziekenhuizen hebben onder andere de volgende maatregelen genomen om de dreigingen zo veel mogelijk te elimineren. Deze maatregelen zijn een opsomming van de maatregelen zoals die door de vijf geïnterviewden zijn gegeven, dat wil zeggen dat niet elk ziekenhuis iedere maatregel ook daadwerkelijk hetzelfde uitvoert.

Fysieke maatregelen	**Organisatorische maatregelen**	**Logische maatregelen**
Niet-publieke ruimtes afsluiten	Informatie beveiligingsbeleid	Wachtwoordenbeleid
Kamers, kasten, en dergelijke afsluiten	Gedragsregels voor medewerkers	Terugdringen van rechten, toegang op persoonlijke titel en op basis van de functie
Cameratoezicht (in de toekomst)	Identificatieplicht door middel van het dragen van een pasje	Toegangsbeveiliging
Noodvoorzieningen zoals een tweede computerruimte en noodstroomvoorziening	E-mail & internet beleid	Functionele accounts zo veel mogelijk beperken
Belangrijke ruimtes beveiligen met pasje	Raad van bestuur beter voorlichten over het nut van informatiebeveiliging	
Fysieke beveiliging door middel van beveiligers in uniform	Awareness campagne	

ICT apparatuur beveiligen door middel van een ketting en slot	Clear-desk & clear-screen beleid	
	Opleiding voor nieuwe medewerkers	

Tabel 15: Maatregelen tegen dreigingen binnen ziekenhuizen

5.3.2. Ziekenhuizen en social engineering

Social engineering heeft als doel om ongeautoriseerd toegang te krijgen tot informatie via misleiding. Er worden naar manieren of middelen gezocht om op technologie of software gebaseerde systemen te kraken door de mensen te manipuleren die toegang tot de informatie of het gewenste systeem hebben.

In hoofdstuk 3 is de volgende definitie van social engineering gedefinieerd:

> ***"Social Engineering uses influence and persuasion to deceive people by convincing them that the social engineer is someone he is not , or by manipulation. As a result, the social engineer is able to take advantage of people to obtain information with or without the use of technology"***

Uit de interviews met de geïnterviewden van de vijf ziekenhuizen is gebleken dat zij een eenduidig beeld over social engineering hebben en dat dit overeenkomt met bovenstaande definitie.

> *'Social engineering is een methode om door middel van een smoesje aan allerlei verschillende soorten informatie te komen. Dit kan dan bewerkstelligd worden door op een psychologische manier iemand iets te laten doen wat hij of zij normaal gesproken nooit zou doen, waarbij gebruikt gemaakt kan worden van allerlei middelen. Niet alleen via technische middelen maar vooral door gesprekken aan te knopen met medewerkers en gebruik te maken van de menselijke gebreken. Cruciaal is daarbij de medewerking die wordt gegeven op een vrijwillige basis, dus niet door middel van dwang bijvoorbeeld'.*

Uit deze definitie blijkt dat het psychologische aspect bij social engineering van groot belang is. Mensen beïnvloeden en overtuigen waardoor ze dingen gaan doen die ze normaal gesproken nooit zouden doen en waarbij de medewerking op vrijwillige basis gebeurt.

Uit de interviews is gebleken dat de geïnterviewden bekend zijn met social engineering en wordt door drie van hen als een gevaar voor het ziekenhuis gezien. Twee van de geïnterviewden zien dit wat minder en dit komt vooral omdat zij moeite hebben om te geloven dat iemand via social engineering aan patiënten informatie probeert te komen. Door alle vijf geïnterviewden wordt wel duidelijk aangegeven dat personeel dat niet direct te maken heeft

met de informatiebeveiliging en ICT, dus verpleegsters, secretaresses en dergelijke, niet bekend zullen zijn met social engineering en de gevaren die het met zich brengt.

Een social engineer probeert zijn invloed en overtuiging te gebruiken om mensen te misleiden om aan informatie te komen. Dit doet de social engineer door in te spelen op de psychologische eigenschappen die de mensen bezitten en door gebruik te maken van psychologische technieken die de social engineer bezit. Het psychologische aspect is dus van zeer groot belang bij social engineering. In hoofdstuk 3, paragraaf 3.2 zijn verschillende eigenschappen uiteengezet die het menselijk gedrag sturen en die dus door de social engineer kunnen worden beïnvloedt om zo het doel van social engineering te bereiken. Uit de analyse in paragraaf 3.2.3 is gebleken dat de eigenschappen die het meest kwetsbaar zijn voor de verschillende technieken, de eigenschappen autoriteit, behulpzaamheid en angst zijn. Autoriteit en angst zijn daarbij aan elkaar gerelateerd want door bij een persoon in te spelen op de eigenschap autoriteit wordt automatisch ook gebruik gemaakt van de eigenschap angst. Namelijk de angst om het verzoek van die persoon, met blijkbaar veel autoriteit, niet goed uit te voeren.
Volgens vier van de geïnterviewden is behulpzaamheid ook de eigenschap die het meest kwetsbaar is bij medewerkers van een ziekenhuis. Dit komt doordat medewerkers van een ziekenhuis zeer bereidwillig zijn, het zit in hun aard om mensen te helpen zonder daarbij door te vragen. De eigenschap behulpzaamheid is dus erg kwetsbaar bij het personeel van ziekenhuizen. Ook de eigenschap autoriteit is zeer kwetsbaar bij medewerkers van ziekenhuizen. De gemiddelde medewerkers in de zorg, en dus ook in ziekenhuizen, is gevoeliger voor autoriteit dan medewerkers bij andere instellingen. Ziekenhuizen werken met een systeem en artsen zijn mensen met behoorlijk wat aanzien in een ziekenhuis en stralen ook autoriteit uit. Mensen die 'witte jassen dragen', zoals de artsen worden genoemd in de interviews, kunnen makkelijker mensen overtuigen dan bijvoorbeeld co-assistenten of arts-assistenten. Daarbij wordt in een ziekenhuis autoriteit ook vaak gekoppeld aan een hoge werkdruk. Mensen die het erg druk hebben en niet met informatiebeveiliging bezig zijn, worden plots met een bepaald urgent verzoek geconfronteerd waardoor ze in hun routine snel een beveiligingsafweging moeten maken. Hierdoor zal het vaak voorkomen dat dan een dergelijk verzoek wordt ingewilligd. Dus de eigenschap autoriteit bij de medewerkers, gekoppeld aan de technieken urgentie en overbelasting die een social engineer kan gebruiken, kan een groot gevaar vormen voor een ziekenhuis in het weggegeven van gevoelige en vertrouwelijke informatie.
Daarnaast zijn de eigenschappen nieuwsgierigheid en onverschilligheid eigenschappen die mensen van nature bezitten en dus ook medewerkers van ziekenhuizen. Mensen zijn vaak uitermate nieuwsgierig en willen eigenlijk alles weten wat er om hen heen gebeurt. Tijdens de interviews is ook gebleken dat nieuwsgierigheid onder het eigen personeel een probleem kan vormen wanneer bijvoorbeeld medewerkers het niet kunnen laten om een patiëntendossier in te zien terwijl ze er eigenlijk niet in horen te kijken.

In hoofdstuk 3, paragraaf 3.3 staan de verschillende social engineering tactieken (aanvallen) beschreven. In de onderstaande tabel staat per aanval beschreven of deze een aanval een gevaar kan vormen voor een ziekenhuis en hoe groot dit gevaar kan zijn.

Impersonation	Impersonation is een aanval met een grote kans van slagen. Behulpzaamheid en autoriteit zijn eigenschappen die erg kwetsbaar zijn en al helemaal bij medewerkers van ziekenhuizen. Dus wanneer door middel van impersonation een rol wordt aangenomen dat inspeelt op de eigenschap behulpzaamheid, is de kans van slagen van deze aanval groot.
Dumpster diving	Of deze aanval een gevaar kan vormen hangt af van een aantal factoren. Hoe wordt er met informatie omgegaan? Waar bevinden zich de afvalcontainers? Wordt gevoelige en vertrouwelijke informatie vernietigd wanneer dit wordt weggegooid?
Shoulder surfing	Shoulder surfing kan een gevaar vormen wanneer de social engineer het vertrouwen weet te winnen van het slachtoffer omdat hij of zij in de buurt moet blijven van het slachtoffer om de gewenste informatie te verkrijgen. De kans van slagen lijkt minder groot dan bij impersonation vanwege direct en fysiek contact.
Piggybacking	De piggybacking aanval is eigenlijk overbodig omdat het ziekenhuis een open instelling is en iedereen naar binnen kan. Deze aanval kan natuurlijk wel worden toegepast bij afgesloten ruimtes in het ziekenhuis. Deze aanval speelt in op onder andere behulpzaamheid en onverschilligheid onder medewerkers en kan dus een grote kans van slagen hebben.
Reverse social engineering	Deze aanval heeft een grondige voorbereiding nodig en het slagen ervan is afhankelijk van het doelwit. Deze aanval lijkt niet echt een gevaar te vormen omdat andere aanvallen, zoals impersonation, een beter en eenvoudiger alternatief voor een social engineer is.
Phishing	Phishing is een groot gevaar voor het ziekenhuis en heeft een grote kans van slagen. Door e-mails te sturen naar alle medewerkers van het ziekenhuis bestaat de kans dat er altijd één iemand intrapt en reageert op een phishing e-mail.
Trojan horses en andere malware	Ook dit is een groot gevaar voor een ziekenhuis omdat als informatiesystemen van het ziekenhuis besmet raken met een virus, de beschikbaarheid van informatie in gevaar komt.

Popup window	Deze aanval lijkt niet echt een gevaar te vormen omdat een social engineer de nodige technische kennis moet bezitten en andere aanvallen een beter alternatief zijn om aan informatie te komen.
Batiting	Baiting kan een gevaar vormen wanneer medewerkers hun nieuwsgierigheid niet in bedwang kunnen houden. Deze aanval heeft een redelijke kans van slagen omdat deze aanval dus inspeelt op de eigenschap nieuwsgierigheid en mensen nu eenmaal nieuwsgierig zijn en het niet kunnen laten om even te kijken wat er op de gevonden USB-stick staat.

Tabel 16: Social engineering tactieken in relatie met ziekenhuizen

De aanvallen impersonation, phishing, trojan horses en baiting lijken op het eerste gezicht het grootste gevaar te vormen en de aanvallen te zijn die de grootste kans van slagen te hebben. Impersonation is een groot gevaar omdat de eigenschappen behulpzaamheid en autoriteit uiterst kwetsbaar bij ziekenhuismedewerkers zijn. Als een social engineer zich besluit voor te doen als een arts en een 'witte jas' weet te bemachtigen, kan hij zich voordoen als een autoritair persoon en dus op de eigenschap autoriteit bij de medewerkers van het ziekenhuis inspelen. Wanneer bijvoorbeeld verpleegsters denken met een arts te maken te hebben, zijn zij snel geneigd om aan het verzoek van die 'arts' te voldoen.

Phishing is een groot gevaar omdat met één e-mail alle medewerkers kunnen worden benaderd en er hoeft maar één medewerkers te zijn die er intrapt er erop reageert. Dit kan bijvoorbeeld gebeuren wanneer het lijkt alsof de e-mail afkomstig is van de helpdesk en er in de e-mail wordt gevraag naar het wachtwoord van een account. Uit twee interviews is ook gebleken dat deze twee ziekenhuis de laatste tijd last hebben gehad van deze phishing e-mails, waarin naar de wachtwoorden van medewerkers is gevraagd. In één ziekenhuis heeft dit er toe tot geleidt dat een medewerker ook daadwerkelijk zijn of haar wachtwoord heeft prijsgegeven.

Dat virussen zoals trojan horses een gevaar voor een ziekenhuis kunnen zijn blijkt wel uit de drie berichten op pagina's 24 en 25. Een trojan horse kan ervoor zorgen dat informatiesystemen worden geïnfecteerd en dat daardoor een ziekenhuis plat komt te liggen. Doordat de beschikbaarheid van de informatie dan wordt aangetast, is het mogelijk dat operaties moeten worden uitgesteld. Dit zou dan tot levengevaarlijke situaties voor patiënten kunnen leiden.

Baiting kan een gevaar vormen wanneer medewerkers hun nieuwsgierigheid niet weten te bedwingen en willen weten wat er op de gevonden USB-stick staat. Een social engineer kan deze stick (geïnfecteerd met een key-logger) op een strategische plaats hebben achtergelaten en op deze manier wachtwoorden achterhalen wanneer de stick wordt aangesloten op een computersysteem.

Het is niet duidelijk of de vijf geïnterviewde ziekenhuizen weleens te maken hebben gehad met een aanval van social engineering (behalve dan van phishing e-mails). Geen van de geïnterviewden weet of er in het verleden een aanval via social engineering heeft plaatsgevonden. Dit wil overigens niet zeggen dat er nooit een aanval via social engineering heeft plaatsgevonden of dat het niet geprobeerd is, het is dan alleen nooit opgemerkt of geregistreerd. Het herkennen van een social engineeringsaanval is tegelijkertijd één van de grootste gevaren van social engineering. Je weet namelijk niet dat je wordt aangevallen, je bent immers in de veronderstelling dat je te maken hebt met een vertrouwd persoon waardoor je geneigd bent om te voldoen aan het verzoek dat je wordt voorgelegd. Omdat je niet weet dat je bent aangevallen, zal dit dus ook nooit gemeld worden. En zelfs wanneer een social engineeringsaanval door middel van bijvoorbeeld impersonation niet lukt, dat wil zeggen dat het doelwit de informatie niet aan de social engineer wil meegeven, dan zal dit ook niet worden gemeld om de dood eenvoudige reden dat je namelijk helemaal niet weet dat je ben aangevallen. Het doelwit zal dan wel een opmerking tegen iemand hierover maken, zoals 'die persoon heeft om die informatie gevraagd maar ik heb dat niet meegegeven', maar dan nog zal er naar alle waarschijnlijkheid geen alarmbelletje zijn gaan rinkelen over het feit dat er iets fout zit. Dus een aanval van social engineeirng (en vooral van impersonation) is heel moeilijk om te herkennen omdat er weinig tot geen bewijs wordt achtergelaten dat er een aanval heeft plaatsgevonden.

Een organisatie tegen social engineering beschermen is niet eenvoudig. Dit geldt ook voor een ziekenhuis en vanwege de specifieke psychologische eigenschappen die medewerkers van een ziekenhuis bezitten en het open karakter van een ziekenhuis, is het misschien nog wel lastiger om een ziekenhuis tegen social engineering te beschermen dan een andere organisatie of instelling. Dit wordt ook door de vijf geïnterviewden aangegeven. De maatregelen die de ziekenhuizen nemen voor de veiligheid van informatie zijn dan ook gericht op het beschermen van die informatie en niet specifiek op de gevaren van social engineering. De maatregelen die de ziekenhuizen nemen zijn de maatregelen die staan beschreven in tabel 15 op bladzijde 104. Om het ziekenhuis te beschermen tegen social engineering zijn er een tweetal aandachtspunten nodig die onder de aandacht moeten worden gebracht volgens de vijf geïnterviewden. Er moet een helder en duidelijk informatie beveiligingsbeleid zijn dat tevens bij alle medewerkers bekend moet zijn. Bij alle vijf geïnterviewde ziekenhuizen is er ook een helder en duidelijk beleid maar is dit vaak niet bekend bij alle medewerkers. Het andere aandachtspunt is bewustwording (awareness) en social engineering meenemen in het informatie beveiligingsbeleid en de awareness campagnes. De vijf ziekenhuizen doen allemaal aan het creëren van awareness om informatiebeveiliging onder de aandacht te brengen van de medewerkers maar dit gebeurt op allerlei verschillende manieren en niet alle medewerkers worden ook daadwerkelijk bereikt. De impersonation aanval bijvoorbeeld is een aanval die moeilijk te verdedigen is, iets dat wordt bevestigd door de geïnterviewden. Deze aanval is zeer moeilijk om te voorkomen en kan eigenlijk maar worden voorkomen wanneer er awareness bij de medewerkers is en de mensen erop te wijzen dat zaken zoals wachtwoorden nooit moeten worden prijsgegeven. Twee van de geïnterviewden geven ook duidelijk aan dat als deze aanval zou worden uitgevoerd, de kans van slagen groot is.

De methode die beschreven staat in hoofdstuk 3, paragraaf 3.5.1, om social engineering tegen te gaan, komt ook overeen met de twee aandachtspunten die door de geïnterviewden zijn gegeven. Deze methode beschermt organisaties door middel van verschillende niveaus tegen social engineering. In paragraaf 3.5.1 staat de methode uitgebreid beschreven, hieronder volgt een beknopte samenvatting.

Niveau 1	Een sterk, duidelijk en helder informatie beveiligingsbeleid met aandacht voor social engineering. Het beleid moet medewerkers helpen om een verzoek van een social engineer te herkennen en zich vervolgens tegen dit verzoek te kunnen verzetten. Het beveiligingsbeleid moet een aantal gebieden aanduiden (zoals een goed wachtwoorden beleid) om een fundament te kunnen zijn in het tegengaan van social engineering. Het beleid tegen social engineering helpt medewerkers zich te verdedigen tegen de verschillende psychologische technieken die kunnen worden gebruikt.
Niveau 2	Awareness training voor alle medewerkers. Alle medewerkers moeten worden getraind in het kweken van een beveiligingsbewustzijn.
Niveau 3	Weerstandstraining voor alle medewerkers. Een training in weerstand zorgt ervoor dat medewerkers geen informatie weggeven die de social engineer nodig heeft.
Niveau 4	Regelmatige herinneringen over de noodzakelijkheid van beveiligingsbewustzijn. Het trainen van mensen in weerstand bieden tegen social engineering is vaak maar effectief in een korte periode. Reguliere en creatieve herinneringen zijn nodig om mensen bewust te houden van de gevaren van social engineering.
Niveau 5	Methoden in het systeem inbouwen om een aanval bloot te stellen en te stoppen.
Niveau 6	Reageren op incidenten. Er moet een goed gedefinieerd proces zijn dat een medewerker kan beginnen zodra hij of zij denkt wanneer er iets mis is.

Tabel 17: Een verdediging tegen social engineering

Naast deze methode om social engineering tegen te gaan zijn er nog aanvullende maatregelen nodig om een goede verdediging tegen social engineering op te bouwen. In paragraaf 3.5.2 zijn deze maatregelen uiteengezet, in de tabel hieronder volgt een beknopte samenvatting.

Wachtwoorden beleid	Er moet een beleid bestaan voor het verkrijgen, creëren en veranderen van wachtwoorden.
Beoordeling van de kwetsbaarheid van de organisatie	Organisaties moeten periodieke beoordelingen doen over de (mogelijke) kwetsbaarheden
Classificatie van gegevens	Social engineers gebruiken de kennis van anderen gebruiken om aan informatie te komen, hierdoor is het van belang om een data classificatie model te hebben waar alle medewerkers zich van bewust zijn. Data classificatie geeft een vorm van veiligheid aan bedrijfsinformatie.
Aanvaardbaar gebruiksbeleid	Een gebruiksbeleid zorgt ervoor dat vertrouwelijke data niet gedeeld wordt en dat informatiesystemen niet misbruikt worden. Een dergelijk beleid bevat informatie over hoe een informatiesysteem gebruikt moet worden en dat informatiesystemen alleen gebruikt worden waarvoor ze bedoeld zijn.
Achtergrond controles	Social engineers gebruiken iedere methode tot hun beschikking om hun doel te bereiken. Ook door zelf te gaan werken voor de organisatie dat door de social engineer als doelwit is uitgekozen.
Beëindigingsproces	Een effectief beëindiginsproces voor het afschrikken van ontslagen of opgestapte medewerkers is een ‘must-have’ voor iedere organisatie. Dit proces zorgt ervoor dat deze medewerkers hun toegang tot informatie niet gebruiken om schade aan de organisatie toe te brengen.
Fysieke beveiliging	Het hebben van fysieke beveiligingsmaatregelen helpt sterk tegen het binnendringen van een organisatie door een social engineer.

Tabel 18: Additionele maatregelen tegen social engineering

Bovenstaande maatregelen zijn voorbeelden van maatregelen die ziekenhuizen zouden kunnen nemen in het tegen gaan van social engineering. Deze maatregelen, samen met de maatregelen die de ziekenhuizen al nemen in beveiligen van de informatie, kunnen het begin vormen van een goede verdediging tegen social engineering.

5.3.3. Ziekenhuizen en awareness

In hoofdstuk 4 is de volgende definitie van awareness gedefinieerd:

> *"the extent to which organizational members understand the importance of information security, the level of security required by the organization and their individual security responsibilities, and act accordingly"*

Deze definitie beschrijft niet alleen het belang van informatiebeveiliging onder medewerkers maar beschrijft ook het gedrag dat mensen erop na moeten houden om deze informatiebeveiliging te waarborgen. Dit is van groot belang omdat het gedrag van een persoon kan vaststellen hoeveel een individu bewust is van zijn of haar gedrag en de bijbehorende consequenties. Het is namelijk vaak het wangedrag van mensen dat voor problemen zorgt bij de beveiliging van informatie.
Uit de vijf interviews met de mensen van de verschillende ziekenhuizen is gebleken dat zij op dezelfde manier over het begrip awareness denken. Awareness wordt door de geïnterviewden vooral gekenmerkt door het feit dat je ervan bewust moet zijn hoe er met informatie moet worden omgegaan, het herkennen van de waarde van informatie en er ook zo naar handelen.

De verantwoordelijkheid van awareness onder medewerkers behoort te liggen bij de mensen die ook verantwoordelijk zijn voor het informatie beveiligingsbeleid van het ziekenhuis. Zij zijn immers degene die verantwoordelijk zijn voor de veiligheid van informatie en die dus ervoor moeten zorgen dat alle medewerkers de informatie van het ziekenhuis zullen beschermen. De raad van bestuur moet dit ondersteunen door openlijk te communiceren dat awareness van informatiebeveiliging van groot belang is voor het ziekenhuis en dat alle medewerkers hierin een rol spelen. Uit de interviews is naar voren gekomen dat dit niet bij ieder ziekenhuis het geval is. Bij sommige ziekenhuizen is het niet duidelijk bij wie de verantwoordelijkheid precies ligt en er wordt maar door één raad van bestuur van een ziekenhuis gecommuniceerd en uitgestraald dat awareness onder medewerkers van groot belang is voor de informatie veiligheid van het ziekenhuis.

Er zij verschillende factoren die een rol spelen in het creëren van awareness bij de medewerkers volgens de geïnterviewden. Het bewust maken van de informatieveiligheid en de rol van de medewerkers daarin en door kennis bij te brengen over hun verantwoordelijkheid, zijn daarbij de belangrijkste. In hoofdstuk 4 wordt uiteengezet dat het veranderen van het menselijk gedrag een belangrijke rol speelt in het creëren van awareness. Om een beter bewustzijn te krijgen van het informatie beveiligingsbeleid en de procedures en maatregelingen, zal het gedrag moeten worden beïnvloed en/of veranderd. Dit wordt dus ook door de geïnterviewden als zondanig aangegeven en de voorbeelden die zij aanhalen die hierin helpen zijn onder andere awareness campagnes en/of programma's, mensen aanspreken op hun gedrag, doelstellingen vertalen in concrete zaken zoals straffen en belonen (goed gedrag belonen en verkeerd gedrag straffen) en het hebben van een 'open mind'. Medewerkers moeten er open voor staan en moeten informatiebeveiliging willen omarmen, anders heeft het geen zin. In hoofdstuk 4, paragraaf 4.1.2, staat beschreven dat bij beïnvloeding van het gedrag van personen, vier belangrijke zaken een rol spelen:

Bewustzijn	De bewustheid van personen dat er verschillende risico's bestaan voor de veiligheid van informatie van organisaties.
Betrokkenheid	De mate waarin de persoon zich betrokken voelt met het informatie beveiligingsbeleid van de organisatie.
Belang	Personen zijn eerder geneigd hun gedrag te veranderen wanneer dit in hun eigen belang is.
Beloning	Met een beloning (of een straf) wordt het belang van een persoon om het gedrag te veranderen tastbaar gemaakt.

Tabel 19: Aspecten die bij beïnvloeding van gedrag een belangrijke rol spelen

Deze bovenstaande aspecten kunnen, samen met de voorbeelden die door de geïnterviewden zijn gegeven, door organisaties en dus ook ziekenhuizen worden gebruikt om het gedrag van de medewerkers te beïnvloeden en te veranderen. Door onder andere awareness campagnes uit te voeren wordt het bewustzijn van de medewerkers vergroot, wordt ook de betrokkenheid vergroot en gaan zij het belang van een goed informatie beveiligingsbeleid inzien. Belonen (of straffen) is een effectieve methode dat hierin kan helpen.

De vijf geïnterviewde ziekenhuizen hebben allemaal een informatiebeveiliging awareness programma waarin wordt geprobeerd om awarenes te kweken onder het personeel. Dit programma ziet er bij alle vijf de ziekenhuizen verschillend uit en het ene ziekenhuis doet het anders en besteedt er meer aandacht aan dan het andere ziekenhuis. Zo is er één ziekenhuis dat het zeer serieus aanpakt en waar de raad van bestuur duidelijk uitstraalt dat informatiebeveiliging awareness belangrijk is en dat het van grote invloed is op de functionering van het ziekenhuis. Dit hebben zij naar alle medewerkers gecommuniceerd door middel van een brief en enquête die door de medewerkers moest worden ingevuld. Hierna is dit ziekenhuis gericht te werk gegaan om informatiebeveiliging awareness onder de aandacht te brengen en te kweken door een awareness campagne.
Drie andere ziekenhuizen doen ook het nodige aan informatiebeveiliging awareness maar toch op een minder effectieve manier dan het bovenstaande ziekenhuis. Eén ziekenhuis doet zelfs niet specifieks iets aan awareness en heeft ook geen awareness programma, enkel wat losse acties.

In hoofdstuk 4, paragraaf 4.3, staat een voorbeeld beschreven van hoe een effectief informatiebeveiliging awareness programma er uit behoort te zien. Een dergelijk programma moet worden opgebouwd rond de volgende vier belangrijke elementen:

Een formele structuur	Een awareness programma is vaak alleen succesvol wanneer het gestructureerd is als een formeel programma, in tegenstelling tot een serie van ad hoc activiteiten.

Zinvolle berichten	De belangrijkste mededelingen en aanpak van het programma moet relevant zijn voor het publiek en tevens consistent zijn met hun normen, waarden en doelstellingen: als beveiliging wordt gezien als een belemmering van de eigen persoonlijke activiteiten, dan zal de boodschap weinig betekenis hebben.
Meetbare voordelen	Een effectief informatiebeveiliging awareness programma moet voor een positieve verandering in het gedrag zorgen, dat bij beveiliging komt kijken. Deze verandering moet dan onder andere leiden tot een vermindering van de kosten van security management en een vermindering van de beveiligingsrisico's
Voortdurend verandering in het gedrag	Het doel van een effectief informatiebeveiliging awareness programma moet zijn om een positieve verandering in het gedrag van de ontvangers te creëren, ten opzichte van beveiliging. Als de verandering niet wordt aangehouden en er wordt teruggrepen naar voorgaand gedrag, dan is het programma niet effectief gebleken.

Tabel 20: Belangrijke elementen van een effectief informatiebeveiliging awareness programma

Deze vier elementen moeten ervoor zorgen dat informatiebeveiliging awareness op een structurele manier wordt opgezet zodat door middel van duidelijke, heldere en zinvolle awareness acties het gedrag wordt beïnvloedt. Dit levert voordelen op voor zowel medewerkers als de organisatie en moet uiteindelijk leiden tot een aanhoudende verandering in het gedrag. In paragraaf 4.3 wordt tevens een proces van een informatiebeveiliging awareness programma beschreven dat deze vier elementen heeft geïntegreerd. Dit proces bevat vier fases waarin op een formele en gestructureerde manier een informatiebeveiliging awareness programma wordt opgezet. In de eerste fase wordt een duidelijke doelstelling vastgesteld en moet direct worden afgeleid van de problemen die moeten worden opgelost. Wanneer de doelstellingen zijn bepaald, wordt in de volgende fase het proces ontwikkeld. Het doel van deze fase is om de deelnemers in te lichten over het doel van het programma en de acties te plannen die gebruikt zullen worden. Wanneer het informatiebeveiliging awareness programma ontwikkeld is, wordt in de derde fase de individuele awareness campagnes geïdentificeerd, ontwikkeld en afgeleverd. De succesvolle afhandeling van een awareness campagne moet in de vierde fase resulteren in het gewenste positieve gedrag dat door de ontvangers van de campagne moet worden omarmd. Het succes van de campagne moet dan worden gecontroleerd om te zien of er verbeteringen mogelijk zijn wanneer in de toekomst een nieuwe campagne moet worden gehouden.

5.4 Conclusie en aanbevelingen

Naar aanleiding van de afgenomen interviews met vijf experts op het gebied van informatiebeveiliging van vijf verschillende ziekenhuizen, kunnen de volgende conclusies en aanbevelingen worden gedaan om een hoger veiligheidsbewustzijn te creëren onder medewerkers wanneer het aankomt op informatiebeveiliging en social engineering.

Eenduidige definitie van informatiebeveiliging en de vier betrouwbaarheidsaspecten

Uit de interviews is gebleken dat alle vijf geïnterviewden op dezelfde manier over informatiebeveiliging denken. Er is een eenduidig beeld over wat informatiebeveiliging inhoudt en dat de betrouwbaarheidsaspecten hierin van groot belang zijn. De definitie van informatiebeveiliging kan het best als volgt worden omschreven:

> *Informatiebeveiliging is het proces van het vaststellen van de vereiste beveiligingsrichtlijnen , maatregelen en procedures (zowel technisch als niet-technisch) met betrekking tot informatie en informatievoorziening ter waarborging van de vertrouwelijkheid , integriteit, beschikbaarheid en geheimhouding van de informatievoorziening*

Het is aan te bevelen om de drie oorspronkelijke betrouwbaarheidsaspecten, beschikbaarheid, integriteit en vertrouwelijkheid, uit te breiden met een vierde aspect, namelijk geheimhouding. Door het toevoegen van dit vierde aspect worden eventuele onduidelijkheden over deze aspecten weggenomen. Het aspect geheimhouding zorgt ervoor dat er geen verschillende opvattingen meer hoeven te zijn over met name het aspect integriteit. Integriteit wordt door de geïnterviewden vooral gezien als integriteit van informatie, terwijl één geïnterviewde dit ziet als integriteit van mensen (dus hoe mensen met informatie omgaan). Het aspect geheimhouding lost dit op omdat geheimhouding moet waarborgen dat informatie uit handen van onbevoegde gebruikers moet blijven. Dat betekent dus bijvoorbeeld dat er regels moeten zijn voor medewerkers wat betreft het inzien van patiëntendossiers. De vier betrouwbaarheidsaspecten worden als volgt gedefinieerd:

Beschikbaarheid (Availability)	Waarborgen dat geautoriseerde gebruikers op de juiste momenten tijdig toegang hebben tot informatie en aanverwante bedrijfsmiddelen.
Integriteit (Integrity)	Het waarborgen van de correctheid, de volledigheid, de geldigheid, de authenticiteit en de onweerlegbaarheid van informatie en verwerking.
Vertrouwelijkheid (Confidentiality)	Informatie dat voor het werk en de behandeling gebruikt wordt, moet vertrouwelijk en zorgvuldig mee worden omgegaan door bevoegde personen.
Geheimhouding (Secrecy)	Informatie uit handen van onbevoegde gebruikers houden.

Door deze vier onderstaande betrouwbaarheidsaspecten te omarmen en te gebruiken, wordt de informatiebeveiliging van ziekenhuizen dus verbetert en hoeven en geen misverstanden meer te bestaan over wat precies bedoelt wordt met welke betrouwbaarheidsaspecten.

Raad van bestuur moet duidelijk uitstralen dat informatiebeveiliging belangrijk is

Om de beveiliging van informatie succesvol te laten zijn, moet de raad van bestuur van het ziekenhuis het belang van informatiebeveiliging communiceren naar alle medewerkers. Dit moet gebeuren op een manier waarop het bij de medewerkers duidelijk wordt dat informatiebeveiliging menens is en dat juist de medewerkers de belangrijkste schakel zijn in het beveiligen van de informatie. De raad van bestuur moet dit duidelijk uitstralen, door bijvoorbeeld een awareness campagne op te laten zetten, dit vervolgens op een heldere en krachtige manier te communiceren naar de medewerkers en duidelijk laten weten dat medewerking vereist is. Wanneer dit niet gebeurt en de raad van bestuur straalt niet uit dat informatiebeveiliging belangrijk is, dan kunnen medewerkers gaan denken dat het ziekenhuis niet veel doet aan de beveiliging van informatie en dat ze het ook niet belangrijk vinden. Hierdoor is het mogelijk dat ook de medewerkers de informatiebeveiliging niet serieus nemen, waardoor er misschien gevaarlijke situaties kunnen ontstaan. Het is dus van groot belang dat het hoogste orgaan van het ziekenhuis, de raad van bestuur, duidelijk laat merken dat informatiebeveiliging een belangrijke schakel is voor het functioneren van het ziekenhuis. Door dit op een heldere en krachtige (en misschien zelfs ludieke) manier te doen, wordt ook bij de rest van het personeel het belang van informatiebeveiliging aangewakkerd.

Naleving en controle op informatiebeveiliging

Een ander belangrijk aspect om de beveiliging van informatie succesvol te laten zijn, is de naleving en controle die er moet zijn op informatiebeveiliging. In drie van de vijf geïnterviewde ziekenhuizen is gebleken dat hier amper aandacht aan wordt besteedt. Wanneer er geen controle op de naleving van het informatie beveiligingsbeleid wordt uitgevoerd, weet het ziekenhuis dus niet hoe het personeel met de beveiliging van informatie omgaat en hoe zij hierover denken. Zonder naleving en controle heeft het dan ook geen nut om een informatie beveiligingsbeleid te hebben omdat er niet wordt gecontroleerd of de medewerkers zich aan het beleid houden en er niet kan worden gemeten of het beleid ook daadwerkelijk invloed heeft op het gedrag van de medewerkers wat betreft informatiebeveiliging. Voor ziekenhuizen is het onmogelijk om alle aspecten van informatie beveiliging te controleren maar zaken zoals het afsluiten van kritische en niet-publieke ruimtes en het hebben van een clean-desk en clean-screen beleid kan worden gecontroleerd. Op elke afdeling kan bijvoorbeeld hier iemand voor verantwoordelijk zijn die dit regelmatig controleert en bij een overtreding vervolgens een notitie achterlaat.

Goede communicatie van het informatie beveiligingsbeleid

Een slechte communicatie van het informatie beveiligingsbeleid kan een dreiging vormen voor een ziekenhuis. Slechte communicatie kan ervoor zorgen dat medewerkers niet voor 100% bekend zijn met het beleid en in veel gevallen vaak niet weten waar ze het beleid kunnen vinden. Dit is ook gebleken uit de interviews, waar is aangegeven dat bij zeker drie ziekenhuizen de medewerkers niet allemaal bekend zullen zijn met het informatie beveiligingsbeleid. Dit wordt mede veroorzaakt door de gebrekkige communicatie van het

beleid, doordat het beleid moeilijk is terug te vinden op het intranet en door het matige gebruik van het intranet in het ziekenhuis. Het intranet is een belangrijk medium waarop het informatie beveiligingsbeleid kan worden verspreidt. Gelet op de belangrijkheid dat de raad van bestuur heeft in de uitstraling van het belang en het nut van informatiebeveiliging, kan het hun taak zijn om dit beleid bij de medewerkers onder de aandacht te brengen door het te publiceren op intranet en er tevens voor te zorgen dat de medewerkers het beleid op intranet kunnen vinden. Hierdoor wordt het intranet extra onder de aandacht van de medewerkers gebracht waardoor de kans groot is dat er weer meer gebruik van gemaakt zal worden.

Het erkennen van de gevaren van social engineering voor ziekenhuizen

Ziekenhuizen moeten inzien en erkennen dat social engineering een gevaar kan vormen voor de informatievoorzieningen van ziekenhuizen. Dat sommige experts van de geïnterviewde ziekenhuizen zich niet kunnen voorstellen dat patiënteninformatie voor bepaalde mensen interessant kan zijn en ook niet kunnen voorstellen voor welke doeleinden patiënteninformatie gebruikt kan worden, doet niets af aan het feit dat social engineering een gevaarlijk wapen is om aan informatie, zoals over patiënten, te komen. De mens is de zwakste schakel in de beveiliging van informatie en is eenvoudig te beïnvloeden door middel van social engineering. Ziekenhuizen moeten dus erkennen dat social engineering bestaat en dat het een gevaar kan vormen voor de informatie veiligheid van het ziekenhuis. Dit hoort boven te beginnen, bij de raad van bestuur, en moet via een awareness programma en campagne naar alle medewerkers worden gecommuniceerd. Door social engineering op te nemen in het awareness programma en te communiceren via een campagne, worden de gevaren van social engineering erkend en tegelijkertijd ook gecommuniceerd naar het personeel.

Social engineering opnemen in het informatie beveiligingsbeleid en in awareness programma's en campagnes

De medewerkers moeten bekend raken met social engineering. Zij moeten weten wat social engineering precies inhoudt, wat de gevaren zijn, hoe ze social engineering kunnen herkennen en wat ze er tegen kunnen doen. De eerste stap hierin is om social engineering op te nemen in het informatie beveiligingsbeleid en vervolgens via de verschillende awareness programma's en campagnes te communiceren. Door sociaal engineering op deze manier naar de medewerkers te communiceren, raken zij bekend met social engineering en wordt de kans kleiner dat een aanval via social engineering zal slagen.

Maatregelen tegen social engineering die ziekenhuizen kunnen nemen

Hoewel het moeilijk is om een ziekenhuis tegen social engineering te beschermen, kunnen er wel maatregelen worden getroffen om de kans kleiner te maken dat een aanval via social engineering zal slagen. Uit de gehouden interviews zijn er maatregelen (en ook de maatregelen op pagina 69) naar voren gekomen die de ziekenhuizen treffen om de beveiliging van informatie zo optimaal mogelijk te laten verlopen. Het betreft de volgende maatregelen:

Fysieke maatregelen	Ruimtes die niet toegankelijk mogen zijn voor publiek, moeten ten allen tijde zijn afgesloten.
	Kamers en kasten die niet afgesloten zijn, nooit onbeheerd achterlaten.
	Het plaatsen van camera's op kritieke plekken.
	Belangrijke en niet publieke ruimtes beveiligen door middel van een pasje, zodat de deur alleen opengaat bij gebruik van dat pasje.
	Fysieke beveiligers in uniform die in het ziekenhuis rondlopen.
	ICT apparatuur vastleggen aan een slot en ketting zodat diefstal niet mogelijk is.
Organisatorische maatregelen	Een goed informatie beveiligingsbeleid dat bekend is bij de medewerkers en dat ook makkelijk voor de medewerkers is terug te vinden.
	Gedragsregels voor medewerkers in hoe er dient te worden omgegaan met de informatievoorzieningen.
	Identificatieplicht door middel van het dragen van een pasje.
	Mensen aanspreken die geen pasje dragen van het ziekenhuis wanneer zij zich in niet-publieke ruimtes bevinden.
	Achtergrond controles.
	Een duidelijk e-mail- en internetbeleid.
	Een clear-desk & clear-screen beleid.
	Beoordeling van de kwetsbaarheid van de organisatie.
	Een opleiding voor nieuwe medewerkers waarin het belang van informatiebeveiliging wordt uitgelegd en hoe zij daarin kunnen bijdragen.
	Een beëindigingsproces.
	Een awareness programma met bijbehorende campagne

Logische maatregelen	Een duidelijk wachtwoordenbeleid.
	Toegang tot informatie op persoonlijke titel en op basis van de functie.
	Classificatie van gegevens.
	Functionele accounts zoveel mogelijk beperken.

Tabel 21: Maatregelen tegen social engineering binnen ziekenhuizen

Door het goed uitvoeren van deze informatie beveiligingsmaatregelen worden automatisch ook de gevaren van social engineering teruggedrongen. Fysieke maatregelen die duidelijk aanwezig zijn in het ziekenhuis, zoals fysieke beveiliging en cameratoezicht, kunnen afschrikkend werken waardoor een social engineer kan besluiten om de aanval niet uit te voeren. Ook organisatorische en logische maatregelen helpen in het terugdringen van de gevaren van social engineering. Wanneer medewerkers weten hoe er met informatie moet worden omgegaan en zich houden aan de opgestelde gedragsregels en het wachtwoordenbeleid, is de kans kleiner dat iemand zijn of haar wachtwoord zal weggeven. Deze maatregelen, maar bijna alle maatregelen, zijn afhankelijk van het bewustzijn van de medewerkers in de beveiliging van informatie. Dit beveiligingsbewustzijn moet worden vergroot en de belangrijkste maatregel dat hieraan bijdraagt is een goed, effectief en duidelijk awareness programma met bijbehorende campagne.

Daarnaast kunnen ziekenhuizen regels in het informatie beveiligingsbeleid opnemen waaraan het personeel zich dient te houden. Belangrijke regels die te maken hebben met de informatieveiligheid zijn de volgende:

- Medewerkers mogen nooit hun gebruikersnaam en/of wachtwoord weggeven;
- Wachtwoorden mogen niet worden opgeschreven en op het computerscherm worden geplakt;
- Vertrouwelijke informatie mag niet onbeheerd worden achtergelaten;
- Bij het verlaten van een ruimte dient altijd de computer te worden vergrendeld;
- Informatie mag uitsluitend worden gedeeld met mensen die hiertoe bevoegd zijn;
- Spreek mensen aan wanneer zij niet zichtbaar een identificatiepas van het ziekenhuis dragen. Dit dient vooral te gebeuren in niet-publieke ruimtes;
- Loop altijd met externe mensen mee. Laat ze nooit zelf naar hun bestemming gaan en blijf altijd aanwezig;
- Geef nooit zomaar patiënteninformatie via telefoon, fax of e-mail door. Controleer altijd de ontvanger;
- Spreek medewerkers aan op onveilig gedrag;
- Geprinte documenten moeten meteen worden opgehaald;
- Lees op het intranet het informatie beveiligingsbeleid alsmede het beleid voor het gebruik van e-mail en intranet.

Verantwoordelijkheid van awareness

In het informatie beveiligingsbeleid moet duidelijk gedefinieerd staan wie er verantwoordelijk is voor het creëren van awareness onder medewerkers. Wanneer dit niet het geval is, is de kans groot dat er geen goed awareness programma en campagne van de grond komt waardoor medewerkers een minder veiligheidsbewustzijn zullen hebben. Voor de beveiliging van informatie is het dus belangrijk dat er één persoon (of meerdere) zich primair bezig houdt met het opzetten van een awareness programma en campagne. Vaak is dit in een organisatie de security officer. Belangrijk is dat in ieder geval de verantwoordelijkheid komt te liggen bij de mensen die ook verantwoordelijk zijn voor het informatie beveiligingsbeleid, want zij zijn immers de personen die ook verantwoordelijk zijn voor de veiligheid van informatie en er dus voor moeten zorgen dat alle medewerkers de informatie zullen beschermen. Daarbij is het belangrijk dat de raad van bestuur erkent dat het creëren van awareness speciale aandacht vereist en het ook ondersteunt uitstraalt naar al het personeel.

Het creëeren van een geschikt informatiebeveiliging awareness programma en campagne

Elk ziekenhuis behoort een informatiebeveiliging awareness programma en campagne te hebben waarin alle medewerkers een beter veiligheidsbewustzijn wordt aangeleerd. Om te beginnen dient de raad van bestuur dit te ondersteunen en uit te stralen naar alle medewerkers. Dit kunnen zij doen door iedereen een persoonlijke brief te sturen waarin aandacht wordt gevraagd voor informatiebeveiliging en awareness en voor medewerking aan het awareness programma en de campagne. Door te laten zien dat het hoogste orgaan van het ziekenhuis, de raad van bestuur, het belangrijk vindt dat medewerkers verantwoordelijk zijn voor de informatie veiligheid, zullen medewerkers eerder geneigd zijn om mee te werken aan het awareness programma.

Op bladzijde 81 staat beschreven hoe een awareness programma er uit kan zien. Een goed en degelijk awareness programma behoort in ieder geval te voldoen aan de volgende vier elementen:

- Een awareness programma behoort een formele structuur te hebben. Een awareness programma is vaak alleen succesvol wanneer het gestructureerd is als een formeel programma;
- Een awareness programma moet bestaan uit zinvolle berichten. De belangrijkste mededelingen en aanpak van het programma moet relevant zijn voor het publiek en tevens consistent zijn met hun normen, waarden en doelstellingen: als beveiliging wordt gezien als een belemmering van de eigen persoonlijke activiteiten, dan zal de boodschap weinig betekenis hebben;
- Een awareness programma moet meetbare voordelen hebben. Een effectief informatiebeveiliging awareness programma moet voor een positieve verandering in het gedrag zorgen, dat bij beveiliging komt kijken. Deze verandering moet dan onder andere leiden tot een vermindering van de kosten van security management en een vermindering van de beveiligingsrisico's;
- Een awareness programma moet voor voortdurende veranderingen in het gedrag zorgen. het doel van een effectief informatiebeveiliging awareness programma moet zijn om een positieve verandering in het gedrag van de ontvangers te creëren, ten opzichte van beveiliging. Als de verandering niet wordt aangehouden en er wordt teruggrepen naar voorgaand gedrag, dan is het programma niet effectief gebleken.

Een awareness programma moet ervoor zorgen dat medewerkers het belang van informatiebeveiliging gaan inzien en wat voor rol zij daarin spelen. Uiteindelijk moet dit een verandering in het gedrag veroorzaken waardoor ze veiliger met informatie zullen omgaan. Er zijn een viertal apsecten die hierin een belangrijke rol kunnen spelen:

- Bewustzijn: De bewustheid van personen dat er verschillende risico's bestaan voor de veiligheid van informatie van organisaties;
- Betrokkenheid: De mate waarin de persoon zich betrokken voelt met het informatie beveiligingsbeleid van de organisatie;
- Belang: Personen zijn eerder geneigd hun gedrag te veranderen wanneer dit in hun eigen belang is;
- Beloning: Met een beloning (of een straf) wordt het belang van een persoon om het gedrag te veranderen tastbaar gemaakt.

Deze bovenstaande aspecten kunnen worden gebruikt om het gedrag van de medewerkers te beïnvloeden en te veranderen. Door het uitvoeren van het awareness programma, door middel van campagnes, wordt het bewustzijn van de medewerkers vergroot, wordt ook de betrokkenheid vergroot en gaan zij het belang van een goed informatie beveiligingsbeleid inzien. De campagnes die gebruikt kunnen worden om het awareness programma over te brengen zijn onder andere via de volgende manieren:

Persoonlijke brief van raad van bestuur	Een persoonlijke brief van de raad van bestuur aan alle medewerkers laat zien dat het ziekenhuis waarde hecht aan informatiebeveiliging. De raad van bestuurt heeft een behoorlijk autoriteit waardoor medewerkers geneigd zijn om te voldoen aan het verzoek van de raad van bestuur.
Enquête	Een enquête onder medewerkers houden over informatiebeveiliging kan een beeld creëren dat laat inzien informatiebeveiliging belangrijk is en dat alle medewerkers hierin een rol spelen.
Cursus voor nieuwe medewerkers	In de introductiecursus voor nieuwe medewerkers kan een awareness presentatie worden gehouden.
Training bestaande medewerkers	Bestaande medewerkers kunnen een cursus volgen waarin een presentatie over awareness wordt gehouden.
Communicatie via het personeelblad en intranet	In het personeelsblad en op intranet kunnen artikelen worden geplaatst over informatiebeveiliging en awareness.
Posters, flyers, stickers, etc.	Posters, flyers en stickers zijn effectieve manieren om snel en eenvoudig berichten over te brengen omtrent awareness.

Notitieblokjes	Door notities achter te laten bij medewerkers die onveilig met informatie omgaan, wordt de awareness vergroot en is de kans minder groot dat dit nogmaals voorkomt.
Inhuren van een derde partij	Een aanval laten uitvoeren door een externe derde partij kan er bij medewerkers voor zorgen dat de ogen open gaan en zich realiseren dat zij erg kwetsbaar zijn en er dus een verhoogd awareness niveau optreedt.
Mensen aanspreken	Door medewerkers aan te spreken die onveilig met informatie omgaan, wordt de kans kleiner dat er nogmaals onveilig met informatie wordt omgegaan en er dus een verhoogd awareness niveau optreedt.

Tabel 22: Campagnes voor een informatiebeveiliging awareness programma

Dit zijn enkele voorbeelden van manieren waarop verschillende boodschappen uit het awareness programma middels een campagne kunnen worden overgebracht. Deze manieren moeten ervoor zorgen dat het gedrag van de medewerkers wordt beïnvloedt waardoor ze beter met de veiligheid van informatie zullen omgaan.

6. Conclusie

In dit afsluitende hoofdstuk worden de deelvragen en de uiteindelijke onderzoeksvraag beantwoord. Voordat het antwoord op de onderzoeksvraag wordt gegeven, worden eerst de verschillende deelvragen beantwoord. De deelvragen zijn in de meeste gevallen al beantwoord in de verschillende hoofdstukken, waardoor deze deelvragen kort en bondig zullen worden beantwoord. Waar nodig zal worden verwezen naar de bijbehorende hoofdstukken en paragrafen voor extra informatie.

6.1 Antwoord deelvraag 1

Deelvraag 1: Wat wordt er verstaan onder het begrip informatiebeveiliging en wat is de rol van de mens hierin?

De uiteindelijke definitie die in dit onderzoek wordt gebruikt is de volgende definitie:

> *Informatiebeveiliging is het proces van het vaststellen van de vereiste beveiligingsrichtlijnen , maatregelen en procedures (zowel technisch als niet-technisch) met betrekking tot informatie en informatievoorziening ter waarborging van de vertrouwelijkheid , integriteit, beschikbaarheid en geheimhouding van de informatievoorziening*

Deze definitie is mijns inziens een juiste en volledige definitie omdat duidelijk wordt dat zowel de beveiligingsrichtlijnen, maatregelen en de procedures een belangrijke rol spelen in de beveiliging van informatie. Ook belangrijk in deze definitie is dat wordt aangegeven dat niet alleen technische zaken moeten worden vastgesteld, maar ook niet-technische zaken zoals bijvoorbeeld een awareness programma. Dit zijn belangrijke aspecten die in andere definities niet worden opgenomen. Daarnaast is duidelijk dat de betrouwbaarheidsaspecten (vertrouwelijkheid, integriteit, beschikbaarheid, maar ook het extra toegevoegde aspect geheimhouding), voor de waarborging zorgen van informatie en de informatievoorzieningen. De vier betrouwbaarheidsaspecten worden als volgt gedefinieerd:

Beschikbaarheid (Availability)	Waarborgen dat geautoriseerde gebruikers op de juiste momenten tijdig toegang hebben tot informatie en aanverwante bedrijfsmiddelen.
Integriteit (Integrity)	Het waarborgen van de correctheid, de volledigheid, de geldigheid, de authenticiteit en de onweerlegbaarheid van informatie en verwerking.
Vertrouwelijkheid (Confidentiality)	Informatie dat voor het werk en de behandeling gebruikt wordt, moet vertrouwelijk en zorgvuldig mee worden omgegaan door bevoegde personen.
Geheimhouding (Secrecy)	Informatie uit handen van onbevoegde gebruikers houden.

Extra informatie over informatiebeveiliging, deze definitie en de vier betrouwbaarheidsaspecten is terug te vinden in hoofdstukken 2 en 5.

De rol van de mens in informatiebeveiliging is ontzettend groot. In de beveiliging van informatie wordt de mens over het algemeen altijd als de zwakste schakel gezien. De technische beveiliging van informatie is bij veel organisaties en instellingen vaak goed geregeld, maar de mens achter de computer blijft kwetsbaar. Mensen zijn namelijk te beïnvloeden door gebruik te maken van sociale en communicatieve vaardigheden. Onbewust kunnen mensen ertoe worden aangezet om bedrijfsgegevens weg te geven of om bepaalde handelingen ter verrichten. Wanneer het om het beveiligen van informatie gaat kunnen mensen naïef, nonchalant en onverschillig overkomen omdat ze vaak de waarde van informatie niet weten en hoe hier mee moet worden omgegaan. Het menselijk aspect is iets dat vaak wordt onderschat maar waar eigenlijk heel veel aandacht aan moet worden besteedt.

6.2 Antwoord deelvraag 2

Deelvraag 2: Wat wordt er bedoeld met social engineering, welke aanvallen zijn er en hoe kunnen deze worden herkend en tegengegaan?

De volgende definitie wordt in dit onderzoek gebruikt over social engineering:

> ***"Social Engineering uses influence and persuasion to deceive people by convincing them that the social engineer is someone he is not , or by manipulation. As a result, the social engineer is able to take advantage of people to obtain information with or without the use of technology"***

Deze definitie geeft het psychologische aspect goed weer dat bij social engineering komt kijken. Social engineering is namelijk een vorm van hacken waar weinig tot geen technologie bij komt kijken maar zich vooral richt op het psychologische aspect van hacken, mensen beïnvloeden en overtuigen om ze dingen te laten doen die ze anders niet zouden doen. Het doel van social engineering is om iemand (het doelwit) te doen misleiden in het verstrekken van waardevolle informatie of toegang te krijgen tot die informatie of resource. Een hacker die gebruik maakt van social engineering, een social engineer, doet dit door in te spelen op de psychologische eigenschappen die ieder mens bezit. Dit gebeurt door middel van verschillende psychologische technieken die de social engineer kan gebruiken bij het uitvoeren van een aanval via social engineering. Zie paragraaf 3.2 uit hoofdstuk 3 voor verdere uitleg van deze psychologische factoren van social engineering.

Er zijn in totaal negen verschillende social engineering aanvallen die kunnen worden uitgevoerd (zie paragrafen 3.3 en 3.4 uit hoofdstuk 3 voor uitgebreide beschrijvingen van deze aanvallen):

Impersonation	Voordoen als een ander persoon om een vertrouwensrelatie op te bouwen om toegang en/of informatie te krijgen.
Dumpster diving	Het verkrijgen van informatie door middel van het doorzoeken van afval.
Shoulder surfing	Het verkrijgen van informatie door ongemerkte observatie van het doelwit.
Piggybacking	Het ongemerkt binnenkomen van een gebouw of ruimte.
Reverse social engineering	Het doelwit initieert contact met de social engineer.
Phishing	Het oplichten van het doelwit door een vertrouwde situatie te creëren waarbij het doelwit nietsvermoedend allerlei vertrouwelijke informatie weggeeft.
Trojan horses & andere malware	Het onbewust installeren van een trojan horse of andere malware.
Popupwindow	Het creëren van een situatie waarbij het doelwit nietsvermoedend informatie invoert in een vals computerscherm.
Batiting	Op specifieke plekken spullen achterlaten die door het doelwit als interessant kunnen worden gezien en vervolgens wordt meegenomen om het op de werkplek te bekijken.

Het herkennen van een social engineering aanval is zeer moeilijk. In de meeste gevallen heeft het doelwit niet door dat hij of zij wordt aangevallen en slachtoffer is van een social engineering aanval. Dit komt omdat er door de social engineer een natuurlijke en vertrouwelijke situatie wordt gecreëerd waarbij het doelwit op een zodanig manier wordt beïnvloedt dat hij of zij niet in de gaten heeft dat er iets mis is en dat de veiligheid van informatie daardoor gevaar loopt. Daarnaast wordt er ook bijna geen bewijs achtergelaten dat er een aanval via social engineering heeft plaatsgevonden. Het tegengaan van aanvallen via social engineering is al net zo lastig als het herkennen ervan. De belangrijkste maatregel hierin is om awareness te kweken onder medewerkers van de organisatie door hun gedrag in informatiebeveiliging te beïnvloeden. Zij moeten het belang van informatie veiligheid en de waarde van informatie inzien. Dit kan worden bewerkstelligd door middel van opleiding en training in awareness met daarnaast extra organisatorische, logische en fysieke maatregelen. In paragraaf 3.5 uit hoofdstuk 3 en in de hoofdstuk 4 en 5 worden deze zaken uitgebreid besproken.

6.3 Antwoord deelvraag 3

Deelvraag 3: Wat word er verstaan onder het begrip veiligheidsbewustzijn?

Het hebben van een veiligheidsbewustzijn (security awareness) onder medewerkers van organisaties is het belangrijkste aspect in informatiebeveiliging. Wanneer dit niet aanwezig is, is de beveiliging van informatie in gevaar omdat mensen dan niet weten hoe met er met gevoelige en vertrouwelijke informatie moet worden omgegaan en de kans bestaat dat deze informatie aan onbevoegde wordt weggegeven of op straat komt te liggen. Medewerkers bewust maken van hun verantwoordelijkheden in het beveiligen van de informatie en de omgeving en ze ook daadwerkelijk motiveren om dit te doen, is hetgeen wat bekend staat als het hebben en creëren van een veiligheidsbewustzijn.

In dit onderzoek wordt de volgende definitie van veiligheidsbewustzijn (awareness) gebruikt:

> *"the extent to which organizational members understand the importance of information security, the level of security required by the organization and their individual security responsibilities, and act accordingly"*

Deze definitie beschrijft niet alleen het belang van informatiebeveiliging onder medewerkers maar ook vooral het gedrag dat mensen erop nahouden in relatie met informatiebeveiliging. Dit is belangrijk omdat het gedrag van een persoon kan vaststellen hoe bewust iemand is van de veiligheid van informatie. Vaak is het namelijk het (wan)gedrag van mensen dat voor problemen zorgt bij de beveiliging van informatie.

In hoofdstuk 4 wordt dit onderwerp uitgebreid beschreven en onderbouwd.

6.4 Antwoord deelvraag 4

Deelvraag 4: Welke factoren spelen een rol in het hebben en creëren van een veiligheidsbewustzijn?

De grootste factor dat hierin een rol speelt is het menselijk gedrag. Dit gedrag moet zodanig worden veranderd of beïnvloedt dat mensen op een betere manier met de veiligheid van informatie omgaan. Om een beter bewustzijn te krijgen van het informatie beveiligingsbeleid, de procedures en maatregelingen zal het gedrag moeten worden beïnvloed en/of veranderd. Het gedrag van mensen moet zodanig worden beïnvloed en/of veranderd, dat het leidt tot een verhoogd veiligheidsbewustzijn. Het uiteindelijke doel moet zijn dat medewerkers onbewust maar bekwaam met informatie omgaan. Dat betekent dat het gewenste gedrag een onderdeel moet zijn van een individu, waarin dit gedrag is ingesleten en geautomatiseerd.

Bij het beïnvloeden van dit gedrag spelen vier belangrijke aspecten een rol:

Bewustzijn	De bewustheid van personen dat er verschillende risico's bestaan voor de veiligheid van informatie van organisaties.
Betrokkenheid	De mate waarin de persoon zich betrokken voelt met het informatie beveiligingsbeleid van de organisatie.
Belang	Personen zijn eerder geneigd hun gedrag te veranderen wanneer dit in hun eigen belang is.
Beloning	Met een beloning (of een straf) wordt het belang van een persoon om het gedrag te veranderen tastbaar gemaakt.

Deze vier aspecten kunnen worden gebruikt om het gedrag van de medewerkers te beïnvloeden en te veranderen. Met name het bewustzijn, de betrokkenheid en het belang kunnen door organisaties worden gebruikt om gedrag te veranderen. Deze drie aspecten worden vooral verkregen door communicatie. Beloning is een methode om naast de communicatie te gebruiken om gewenst gedrag te stimuleren, waardoor tegelijk ook het belang voor de persoon wordt onderstreept.

Door deze aspecten op te nemen in een informatiebeveiliging awareness programma en uit te voeren door middel van een awareness campagne kan er een beter veiligheidsbewustzijn onder medewerkers worden gecreëerd.

In hoofdstuk 4 wordt dit onderwerp uitgebreid beschreven en onderbouwd.

6.5 Antwoord deelvraag 5

Deelvraag 5: Is er sprake van een veiligheidsbewustzijn ten opzichte van informatiebeveiliging en social engineering bij ziekenhuizen en wat doet het ziekenhuis om het veiligheidsbewustzijn van medewerkers te vergroten?

Uit de interviews met vijf experts op het gebied van informatiebeveiliging van vijf verschillende ziekenhuizen, is gebleken dat niet elk ziekenhuis hetzelfde veiligheidsbewustzijn heeft wanneer het de beveiliging van informatie betreft. Uiteraard wordt het belang ingezien van een goede informatiebeveiliging maar elk ziekenhuis gaat daar op hun eigen manier mee om. Zo is de verantwoordelijkheid over informatiebeveiliging verschillend. Bij sommige ziekenhuizen ligt deze verantwoordelijkheid bij de raad van bestuur, bij een ander ziekenhuis ligt deze verantwoordelijkheid bij de verschillende afdelingen en bij andere ziekenhuizen is de persoon die over informatiebeveiliging gaat verantwoordelijk. Daarnaast wordt niet bij ieder ziekenhuis door de raad van bestuur uitgestraald dat het hebben van een veiligheidsbewustzijn in de beveiliging van informatie belangrijk is.
Ook is duidelijk geworden dat hoewel er bij ieder ziekenhuis een informatie beveiligingsbeleid bestaat en er gedragsregels zijn voor de omgang met informatie, e-mail en internet, de kans bestaat dat veel medewerkers dit beleid en deze gedragsregels niet kennen of niet weten waar dit kan worden gevonden. Mogelijke oorzaken hiervoor kan het slechte gebruik van het

intranet zijn of geen effectieve manier van communicatie van het informatie beveiligingsbeleid richting het personeel. Nog een ander aspect dat bij een aantal ziekenhuizen verschillend is, is bij wie de verantwoordelijkheid ligt voor het creëren van een veiligheidsbewustzijn onder het personeel. Bij het ene ziekenhuis wordt dit beter aangepakt dan bij het andere ziekenhuis.

Wat betreft het veiligheidsbewustzijn in social engineering, is een iets ander verhaal. Sommige geïnterviewde experts van de ziekenhuizen zien een gevaar in social engineering en dat een aanval van social engineering een reële kans van slagen kan hebben. Andere ziekenhuizen zien ook wel het gevaar in, maar vinden het moeilijk om te geloven dat iemand via social engineering een ziekenhuis zal aanvallen. De geïnterviewde experts zijn allemaal bekend met social engineering maar hebben aangegeven dat de kans heel groot is dat ander personeel, zoals secretaresses of verpleegsters, geen idee heeft wat social engineering is, wat het inhoudt en welke gevaren social engineering met zich mee brengt. Social engineering wordt ook niet door de ziekenhuizen meegenomen in het informatie beveiligingsbeleid of in awareness programmes en campagnes. Hierdoor zal het merendeel van de medewerkers niet bekend zijn met social engineering en wat dit kan aanrichten wanneer een aanval plaatsvindt.

Om het veiligheidsbewustzijn van informatiebeveiliging van medewerkers te vergroten, maken alle ziekenhuizen gebruik van diverse methoden om dit te bereiken. Zo hebben de meeste ziekenhuizen een informatie beveiliging awareness programma dat er bij ieder ziekenhuis verschillend uitziet. Het ene ziekenhuis besteedt er ook meer aandacht aan en pakt het serieuzer aan dan het andere ziekenhuis. De vijf ziekenhuizen doen dus allemaal aan het creëren van awareness om het veiligheidsbewustzijn van de medewerkers te vergroten maar dit gebeurt op allerlei verschillende manieren en niet alle medewerkers worden ook daadwerkelijk bereikt.

Er kan geconcludeerd worden dat er bij sommige ziekenhuizen een beter veiligheidsbewustzijn omtrent informatiebeveiliging bestaat dat bij andere ziekenhuizen. Bij deze ziekenhuizen lijkt dit nog niet voldoende te zijn. Het mag bijvoorbeeld niet voorkomen dat medewerkers niet bekend zijn met het informatie beveiligingsbeleid en bijbehorende gedragsregels. Een veiligheidsbewustzijn ten opzichte van social engineering is er bij de geïnterviewde ziekenhuizen nog minder en in sommige gevallen bijna helemaal niet. Dit wordt ook erkend door aan te geven dat veel mensen niet bekend zullen zijn met social engineering, dat social engineering ook niet wordt opgenomen in een awareness programma en dat een aanval via social engineering een reële kans van slagen heeft.

Voor meer informatie en extra toelichting, zie hoofdstuk 5.

6.6 Antwoord deelvraag 6

Deelvraag 6: Zijn ziekenhuizen zich bewust van de gevaren van social engineering en zijn ziekenhuizen bestand tegen de verschillende soorten aanvallen van social engineering?

Zoals in de vorige deelvraag is beantwoord is er geen echt veiligheidsbewustzijn wanneer het aankomt op social engineering. De kans van slagen van een social eengineering aanval is relatief groot omdat veel mensen die niet direct betrokken zijn met de beveiliging van

informatie niet bekend zijn met social engineering en omdat er ook geen aandacht wordt geschonken aan social engineering in de awareness programma's en campagnes die de ziekenhuizen uitvoeren. Hierdoor worden de gevaren van social engineering niet gecommuniceerd naar het personeel van de ziekenhuizen.

Daarbij is het beschermen van ziekenhuizen tegen social engineering een lastige aangelegenheid. Een ziekenhuis is een open instelling waar iedereen toegang tot heeft en dus ook zomaar kan binnenlopen. Daarbij zijn ziekenhuis medewerkers getraind om zo patiëntvriendelijk mogelijk over te komen en zit het in hun aard om mensen te helpen en dus behulpzaam over te komen. Social engineering is een methode dat hierin op probeert in te spelen waardoor een aanval van social engineering grote kans van slagen heeft. De eigenschap dat medewerkers van ziekenhuizen behulpzaam willen overkomen maakt hen dus kwetsbaar voor aanvallen van social engineering. Een andere psychologische eigenschap die medewerkers van ziekenhuizen vaak bezitten is de eigenschap autoriteit. Mensen die in ziekenhuizen werken kunnen gevoeliger voor autoriteit zijn dan anderen. Een arts straalt namelijk behoorlijk wat autoriteit uit en veel mensen kunnen daar gevoelig voor zijn. Ook hierop kan social engineering inspelen door te proberen om deze eigenschap uit te buiten.

Van de negen social engineering aanvallen die in hoofdstuk 3 zijn gedefinieerd, zijn er een aantal aanvallen die een grotere kans van slagen lijken te hebben dan andere aanvallen. De impersonation aanval bijvoorbeeld is een aanval met een grote slagingskans. Zoals aangegeven is een ziekenhuis een open instelling en werken er ontzetten veel medewerkers, niet iedereen kent elkaar. Door gebruik te maken van de impersonation aanval kan de social engineer zich voordoen als iemand anders, bijvoorbeeld een medewerker, om zo bepaalde informatie afhandig te maken. Hierbij wordt dan ingespeeld op een bepaalde psychologische eigenschap, afhankelijk van de gekozen rol, waardoor de medewerker waarop deze aanval wordt uitgevoerd extra kwetsbaar wordt. In de meeste gevallen heeft deze persoon dan ook niet door dat hij of zij wordt aangevallen. Deze aanval is zeer moeilijk te voorkomen en kan eigenlijk alleen maar worden voorkomen door middel van een veiligheidsbewustzijn dat aanwezig moet zijn bij medewerkers.

Het is dus zeer moeilijk om ziekenhuizen bestand te maken tegen social engineering aanvallen. De belangrijkste maatregelen hierin zijn om een duidelijk informatie beveiligingsbeleid te hebben dat tevens bij alle medewerkers bekend moet zijn en het kweken van een veiligheidsbewustzijn onder de medewerkers. Daarbij dient social engineering te worden meegnomen in het informatie beveiligingsbeleid en de awareness programma's en campagnes

6.7 Antwoord onderzoeksvraag

Onderzoeksvraag: Kan social engineering een gevaar voor een ziekenhuis vormen, hoe is het gesteld met het veiligheidsbewustzijn van informatiebeveiliging bij ziekenhuizen wanneer er sprake is van social engineering en hoe kan dit veiligheidsbewustzijn worden versterkt?

Door het apart beantwoorden van de deelvragen, is tegelijkertijd ook de onderzoeksvraag al gedeeltelijk beantwoord.

Het veiligheidsbewustzijn bij ziekenhuizen wanneer het aankomt op informatiebeveiliging, is bij ieder ziekenhuis wisselend. Uit de interviews is gebleken dat het ene ziekenhuis meer aan de beveiliging van informatie doet dan het andere ziekenhuis. Er zijn ziekenhuizen die er meer aandacht aan besteden en er serieuzer mee omgaan. Dit zijn dan automatisch ook de ziekenhuizen waar een hoger veiligheidsbewustzijn onder de medewerkers aanwezig is omdat deze ziekenhuizen ook meer doen aan het creëren van awareness bij het personeel van het ziekenhuis. Hoewel er bij sommige ziekenhuizen een hoger veiligheidsbewustzijn over informatiebeveiliging is dan bij andere ziekenhuizen, geldt dit niet echt voor social engineering. Uit de interviews is gebleken dat ziekenhuizen kwetsbaar voor aanvallen van social engineering kunnen zijn. Er is geen echt veiligheidsbewustzijn ten opzichte van social engineering omdat social engineering door sommige ziekenhuizen niet als een gevaar wordt gezien en er verder in het informatie beveiligingsbeleid en in de awareness programma's en campagnes geen aandacht aan wordt geschonken.

Uit dit onderzoek is dan ook gebleken dat social engineering een gevaar kan vormen voor ziekenhuizen. De redenen die in dit onderzoek naar voren zijn gekomen en die onderbouwen dat social engineering voor ziekenhuizen een gevaar kunnen vormen, zijn de onderstaande redenen. Er dient te worden bijgezegd dat een aantal redenen zijn afgeleidt uit de afgenomen interviews met de vijf experts van vijf ziekenhuizen. Dat hoeft dus niet te betekenen dat al deze redenen ook toepasbaar zijn op alle ziekenhuizen.

Ziekenhuizen zijn open instellingen

Ziekenhuizen zijn instellingen met een open karakter waar iedereen toegang tot heeft en naar binnen kan lopen. Dit is een groot gevaar in tegenstelling tot bij andere organisaties of instellingen waar je eerst nog langs fysieke beveiliging moet om binnen te komen. Een social engineer hoeft dus minder moeite te doen om bij informatie, informatiesystemen of informatievoorzieningen te komen. Ook zijn medewerkers hierdoor makkelijker te benaderen, wat het eenvoudiger maakt in het toepassen van een social engineering aanval.

De specifieke psychologische eigenschappen van ziekenhuis medewerkers

Mensen bezitten psychologische eigenschappen die kunnen worden uitgebuit door middel van een social engineering aanval. Dit geldt helemaal voor ziekenhuis medewerkers die hierin extra kwetsbaar zijn. Ziekenhuis medewerkers zijn namelijk van nature erg behulpzaam, zij willen de best mogelijk zorg bieden aan patiënten en zijn dus getraind in het zo patiëntvriendelijk mogelijk overkomen richting de bezoekers in het ziekenhuis. Deze eigenschap, met name behulpzaamheid, kan door een social engineer worden uitgebuit door hierop in te spelen. Doordat medewerkers dus zo behulpzaam mogelijk willen overkomen is de kans groter dat zij een bepaald verzoek van een social engineer zullen inwilligen. Ook de eigenschap dat mensen gevoelig zijn voor autoriteit, maakt hen extra kwetsbaar. Een ziekenhuis werkt met een bepaald systeem waarin artsen en dokters veel autoriteit hebben. Een social engineer die zich weet voor te doen als een arts, heeft een grote kans om informatie los te krijgen van bijvoorbeeld een verpleegster vanwege het feit dat artsen een grote uitstraling van autoriteit hebben. Een verpleegster zal waarschijnlijk niet durven om een

arts tegen te spreken en niet de informatie te geven waar die arts om vraagt. Deze twee eigenschappen maken ziekenhuis medewerkers dus extra kwetsbaar voor social engineering. Daarnaast zijn zij ook, net zoals veel andere mensen, kwetsbaar voor andere eigenschappen zoals onverschilligheid (nonchalant en op de verkeerde manier omgaan met informatie) en nieuwsgierigheid (willen weten wat er op een gevonden USB-stick staat).

De vele medewerkers die er in een ziekenhuis werken

In een ziekenhuis werken tal van verschillende medewerkers en afhankelijk van de grootte van het ziekenhuis zijn er duizenden medewerkers in dienst. Daarbij zijn er mensen die in ploegendienst werken, die part-time werken, die extern zijn aangetrokken of mensen die vrijwilligerswerk doen. Het bereiken van al deze mensen om een veiligheidsbewustzijn te creëren omtrent informatiebeveiliging en social engineering is dus erg lastig.

Doordat een ziekenhuis veel medewerkers in dienst heeft, speelt nog een andere dreiging een grote rol. Een social engineering aanval via phishing bijvoorbeeld heeft daardoor een grotere kans van slagen omdat door middel van deze aanval alle medewerkers via een e-mail kunnen worden benaderd. In deze phishing e-mail kan dan om wachtwoorden worden gevraagd en er hoeft van deze duizenden medewerkers er maar één te zijn die hierin op ingaat en zijn of haar wachtwoord weggeeft. Hoe meer medewerkers er dus in een organisatie werken, hoe groter een dergelijke aanval kans van slagen heeft.

Geen duidelijke communicatie en uitstraling van de raad van bestuur dat informatiebeveiliging belangrijk is

Uit de interviews is gebleken dat niet bij ieder ziekenhuis de raad van bestuur, het hoogste orgaan van een ziekenhuis, duidelijk communiceert naar de medewerkers dat informatiebeveiliging belangrijk is. Zij stralen niet naar de medewerkers uit dat zij de belangrijkste schakel zijn in de beveiliging van informatie. Om een verhoogd veiligheidsbewustzijn te creëren onder de medewerkers is dit wel een belangrijks aspect aangezien de medewerkers het gevoel moeten krijgen dat het ziekenhuis informatiebeveiliging als een belangrijk onderdeel ziet. Als de raad van bestuur dit niet uitstraalt, kun je ook van medewerkers niet verwachten dat zij het belang inzien van een goede informatiebeveiliging.

Patiënteninformatie is vertrouwelijke en gevoelige informatie

Informatie over patiënten is binnen een ziekenhuis vertrouwelijke en gevoelige informatie wat de beveiliging ervan extreem belangrijk maakt. Wanneer deze informatie via social engineering, of via wat voor reden dan ook, op straat komt te liggen, is de imagoschade niet te overzien en kan er daarnaast een forse schadeclaim verwacht worden. Het ziekenhuis is er daarom alles aan gedaan om dit te voorkomen.

Een social engineering aanval is moeilijk om te herkennen

Het herkenen van een social engineering aanval is niet eenvoudig en is één van de grootste gevaren van social engineering. Je bent je er namelijk niet van bewust dat je wordt aangevallen, je bent immers in de veronderstelling dat je te maken hebt met een vertrouwd persoon waardoor je geneigd bent om te voldoen aan het verzoek dat je wordt voorgelegd. Je

weet niet dat je door middel van social engineering wordt aangevallen, waardoor een dergelijke aanval ook bijna nooit gemeld zal worden. Hierdoor kunnen er geen acties op worden ondernomen om het in de toekomst tegen te gaan. Uit de gehouden interviews is ook gebleken dat de geïnterviewde experts niet weten of het ziekenhuis weleens te maken heeft gehad met een social engineering aanval. Dit wil niet zeggen dat er nooit een aanval via social engineering heeft plaatsgevonden of dat het niet geprobeerd is, het is dan alleen nooit opgemerkt of geregistreerd. Dus een aanval van social engineering is heel moeilijk om te herkennen omdat je niet weet dat je wordt aangevallen en omdat er weinig tot geen bewijs wordt achtergelaten dat er een aanval heeft plaatsgevonden. Wat hierin ook meespeelt is dat personeel zoals bijvoorbeeld verpleegsters, secretaresses en arts-assistenten waarschijnlijk nog nooit van social engineering gehoord hebben (wat ook in de interviews werd aangegeven). Dit maakt het ook moeilijk om een social engineering te herkennen.

Het niet aanspreken van mensen die geen identificatiepasje van het ziekenhuis dragen

In een ziekenhuis behoort iedereen die werkzaam is binnen het ziekenhuis een zichtbare identificatiepas te dragen. De regel is dat mensen die geen identificatie pas dragen maar zich toch bevinden in een ruimte die niet toegankelijk behoort te zijn voor publiek, worden aangesproken op het niet dragen van de identificatiepas. Dit is een regel die door de medewerkers vaak niet wordt toegepast omdat zij niet durven om (mogelijke) collega's hierop aan te spreken. Medewerkers willen niet overkomen als een soort politieagent richting hun collega's waardoor mensen die geen pas dragen niet zo snel zullen worden aangesproken. Dit is voor een social engineer natuurlijk handig om te weten omdat hij of zij geen identificatiepas heeft en ook niet zo snel in het bezit van een identificatiepas kan komen.

Social engineering wordt niet opnemen in het informatie beveiligingbeleid en in de awareness programma's en campagnes

De geïnterviewde ziekenhuizen hebben allemaal een informatie beveiligingsbeleid en voeren ook verschillende awareness programma's en campagnes uit. Wat hierin niet terugkomt is social engineering en de bijbehorende aanvallen en gevaren die het met zich mee brengt. Hierdoor zijn de medewerkers van de ziekenhuizen niet bekend met social engineering en hoe ze hiermee om moeten gaan. Uit de interviews is ook gebleken dat, behalve de mensen die werkzaam zijn op de ICT afdeling en dus te maken hebben met het informatie beveiligingsbeleid, de rest van het personeel waarschijnlijk nog nooit van social engineering gehoord heeft. Door social engineering in het informatie beveiligingsbeleid en in de awareness programma's en campagnes op te nemen, raken de medewerkers bekend met social engineering waardoor de kans kleiner wordt dat een aanval kans van slagen heeft. Ze krijgen dan immers inzicht in hoe een social engineer te werk gaat waardoor het voor ze mogelijk wordt om eventueel de aanval te herkennen en maatregelen te treffen.

Slechte kennis van het informatie beveiligingsbeleid en de gedragsregels onder medewerkers

Bij een aantal van de geïnterviewde ziekenhuizen is duidelijk geworden dat waarschijnlijk niet alle medewerkers bekend zullen zijn met het informatie beveiligingsbeleid en de gedragsregels in het omgaan met informatie, e-mail en internet. De oorzaken die hieraan ten grondslag liggen zijn vaak het slechte gebruik van het intranet waarop het beleid en de

gedragsregels zijn terug te vinden en een slechte communicatie van het informatie beveiligingsbeleid en de bijbehorende gedragsregels. In awareness programma's en campagnes wordt hier niet voldoende aandacht aan besteedt. Medewerkers die geen kennis van het informatie beveiligingsbeleid hebben en ook de gedragsregels niet kennen, kunnen een gevaar vormen voor de beveiliging van informatie en de gevaren van social engineering.

Geen goede aandacht aan controle en naleving op het informatie beveiligingsbeleid en de gedragsregels

Het hebben van een effectief informatie beveiligingsbeleid en gedragsregels heeft niet echt nut wanneer er geen controle op naleving wordt uitgevoerd. Wanneer medewerkers het beleid op een foutieve manier uitvoeren en er nooit op worden aangesproken, dan blijven ze dit beleid ook in de toekomst op de verkeerde manier uit te voeren. Er moet dus een soort van controle mechanisme zijn om medewerkers te kunnen controleren bij de uitvoering van het informatie beveiligingsbeleid zodat het gedrag van de medewerkers hierin verander wordt. Uit de interviews is ook gebleken dat bij sommige ziekenhuizen er weinig tot geen aandacht wordt geschonken aan controle op naleving van het informatie beveiligingsbeleid en de bijbehorende gedragsregels.

Vanwege de hierboven uiteengezette redenen, kan geconcludeerd worden dat social engineering een gevaar kan vormen voor de geïnterviewde ziekenhuizen, hoewel het bij het ene ziekenhuis een groter gevaar kan vormen dan bij het andere ziekenhuis. Dit wil dus niet zeggen dat dit voor alle ziekenhuizen in Nederland geldt, er kunnen immers ziekenhuizen zijn die wel het gevaar van social engineering inzien en er ook de nodige aandacht aan besteden.

Door het toepassen van de aanbevelingen die in paragraaf 5.5 van hoofdstuk 5 staan beschreven, kan er een hoger veiligheidsbewustzijn worden gekweekt onder medewerkers van ziekenhuizen wanneer het aankomt op informatiebeveiliging en social engineering. Door het toepassen van deze aanbevelingen is het aannemelijk dat het gevaar van social engineering zal afnemen. Het is echter niet mogelijk om het gevaar helemaal weg te halen vanwege het simpele feit dat zolang er mensen in organisaties of instellingen werken, er fouten gemaakt zullen worden.

Appendix A: Bijlage

Interview protocol

Naam:

Functie:

Ziekenhuis:

Plaats:

Tijd:

Interviewvragen

De interviewvragen zijn opgedeeld in vier onderwerpen: algemeen, informatiebeveiliging, social engineering en awareness.

Algemeen

1. Kunt u een taakomschrijving van uw werkzaamheden geven?
2. Wat zijn uw verantwoordelijkheden?

Informatiebeveiliging

3. Wat verstaat u onder informatiebeveiliging?

Informatiebeveiliging is opgebouwd rondom de begrippen vertrouwelijkheid, integriteit en beschikbaarheid. Zij zorgen voor de betrouwbaarheid van de informatie binnen het vakgebied van de informatiebeveiliging en worden ook wel de betrouwbaarheidsaspecten genoemd.

4. Wat verstaat u onder vertrouwelijkheid, integriteit en beschikbaarheid van informatie en hoe worden deze betrouwbaarheidsaspecten binnen het ziekenhuis gewaarborgd?
5. Bij wie ligt de verantwoordelijkheid voor informatiebeveiliging binnen het ziekenhuis?
6. Welk soort informatie is het meest gevoelig binnen het ziekenhuis?

7. Wat voor schade kan er optreden wanneer er (gevoelige) informatie wordt verloren en naar buiten gebracht?

8. Wat is de rol van de medewerkers in informatiebeveiliging?

9. Bestaan er voor medewerkerkers gedragsregels in het omgaan met informatie en zijn ze bekend met dit beleid?

10. Hoe wordt het beleid omtrent informatiebeveiliging gecommuniceerd naar de medewerkers?

11. Wat zijn de meest gevoelige plekken (kwetsbaarheden) in een ziekenhuis wat betreft het omgaan met informatie?

12. Welk soort dreigingen kunnen een gevaar zijn voor de informatie assets van het ziekenhuis?

13. Welke maatregelen zijn genomen om bedreigingen te verminderen?
    a. Organisatorische maatregelen
    b. Logische maatregelen
    c. Fysieke maatregelen

14. Hoe worden de maatregelen voor informatiebeveiliging nageleefd en gecontroleerd?

15. Heeft het ziekenhuis wettelijk verplichtingen omtrent informatiebeveiliging?

Social engineering

16. Is men binnen het ziekenhuis bekend met social engineering en wat verstaat het ziekenhuis onder social engineering?

17. Hoe gaat een social engineer volgens u te werk, met andere woorden hoe zie het proces van een social engineering aanval er precies uit?

18. Heeft in het verleden het ziekenhuis weleens te maken gekregen met een aanval van social engineering? Zo ja, hoe is hier vervolgens op gereageerd?

19. Wat doet het ziekenhuis tegen social engineering en welke maatregelen worden er getroffen?

20. Een social engineer probeert in te spelen op psychologische eigenschappen van de mens. Welke psychologische eigenschappen zijn volgens u het meest kwetsbaar?

21. Een bekende social engineering aanval is impersonation (jezelf voordoen als iemand anders). Stel dat een social engineer zich voordoet als bijvoorbeeld een helpdeskmedewerker en contact opneemt met medewerkers met de vraag of de wachtwoorden van medewerkers wel voldoen aan de nieuwe beveiligingseisen. Deze medewerker geeft vervolgens zijn of haar wachtwoord weg.
    - Hoe kan deze aanval worden voorkomen?

- Welke acties/maatregelen moeten worden ondernomen om deze aanval tegen te gaan?

22. Een andere bekende social engineering aanval is door middel van list en bedrog toegang tot ongeautoriseerde ruimtes te krijgen (piggybacking), waardoor er naar waardevolle informatie kan worden gezocht (afval doorzoeken, conmputersystemen infecteren).
    - Hoe kan deze aanval worden voorkomen?
    - Welke acties/maatregelen moeten worden ondernomen om deze aanval tegen te gaan?

23. Hoe worden deze maatregelingen gecontroleerd of ze daadwerkelijk ook worden nageleefd?

24. Worden de gevaren van social engineering naar de medewerkers gecommuniceerd en zo ja, op welke manier?

Awareness

25. Wat verstaat u onder security awareness (veiligheidsbewustzijn)?

26. Welke factoren spelen volgens u een rol in het hebben en creëren van een veiligheidsbewustzijn?

27. Wie is er binnen het ziekenhuis verantwoordelijk voor awareness en hoe wordt awareness naar de medewerkers gecommuniceerd?

28. Ziet men binnen het ziekenhuis het nut van awareness bij medewerkers?

29. Heeft het ziekenhuis voor de medewerkers een awarenessprogramma? Zo nee, waarom niet en wat zijn de belangrijkste knelpunten?

30. Wat wordt binnen het ziekenhuis gedaan om de awareness bij medewerkers te vergroten?

31. Zijn er regels en richtlijnen in het informatiebeveiligingsbeleid opgenomen met betrekking tot awareness?

Appendix B: Literatuurlijst

Artikelen

[ALLE06] Allen, Malcolm, *Social Engineering: a means to violate a computer system*, SANS Information Security Reading Room, 2003

[ARTH10] Arthurs, Wendy, *A proactive defense against social engineering,* SANS Information Security Reading Room, last update June 2010

[CBP08] College Bescherming Persoonsgegevens, *Informatiebeveiliging in ziekenhuizen voldoet niet aan de norm,* Den Haag, 2008

[CIO07] CIO platform Nederland, *Informatiebeveiliging, resultaat van de CIO interest Group,* tweede publicatie, juni 2007

[CVIB00] Code voor informatiebeveiliging, Nederlands centrum van normalisatie-instituut, 2000, De Nederlands vertaling van de Engelse Britse standaard BS7799.

[DANK05] Dankelman, J., e.a., Fundamental aspects of learning minimally invasive surgical skills, University of Technology Delft, Minimally Invasive Therapy. 2005; 14:4-5; 247–256

[DOLA04] Dolan, Aaron, *Social Engineering,* SANS Information Security Reading Room, 2004

[GOPA10] Gopalakrishnan, Eakan, *Social Engineering: Facts, Myths and Countermeasures*, University of Southhampton, maart 2010

[GRAG02] Gragg, David, *A Multi-level Defense Against Social Engineering,* SANS Information Security Reading Room, 2002

[GRAN01] Granger, Sarah, *Social Engineering Fundamentals: Hacker Tactics*, Security Focus, 2001

[GULA03] Gulati, Radha, *The threat of social engineering and your defense against it,* SANS Information Security Reading Room, 2003

[HERZ10] Herzig, Terrel, *Information security in Healthcare*, Healthcare Information and Management Systems Society, 2010

[INFO02] Information Security Forum, *Effective Security awareness: workshop report*, London, 2002

[JORD05] Jordan, Myles & Goudey, Heather, *The Signs, Signifiers and semiotics of the succesful semantic attack*, 14th Annual EICAR Conference 2005, St.Juliens/Valletta, Malta, 2005

[KANT07] Kanters, F, *De security officer als manager centraal in het beïnvloedingsproces*, Infosecurity, 2 mei 2007

[KOOT05] Koot, Andre & Haas, Jim de, *Organisaties overschatten niveau van awareness*, Informatiebeveiliging, Juli 2005

[KOOP03] Koops, Bert-Jaap, *De Code voor Informatiebeveiliging naar Nederlands recht*, Informatiebeveiliging, 5, 20-24, 2006

[MAUW06] Mauw, Sjouke & Oorstdijk, Martijn, *Attack trees: door de bomen de bedreigingen zien*, GvIB Informatiebeveiliging, 7(1):16-17, Februari 2006

[ON2I09] ON2IT Security, *Beveiliging voor de zorg,* 2009

[OPEL05] Opel, Alexander, *Thesis: Design and Implementation of a support tool for attack trees*, Otto-von-Guericke University, Magdeburg, Maart 2005

[REDM06] Redmon, Kevin, *Mitigation of Social Engineering Attacks in Corporate America*, East Carolina University, 2006

[SCHN99] Schneier, Bruce, *Attack Trees*, Dr. Dobb's journal, December 1999

[SIEG09] Siegel, Daniel, *Thesis: On the new threats of social engineering exploiting social networks*, Technische Universiteit Munchen, 2009

[SIPO00] Siponen, Mikko, *A conceptual foundation for organizational information security awareness,* Information Management & Computer Security, Augustus 2000, pagina 31 - 41

[SOLM04] Solms, Basie van, *The 10 deadly sins of information security management*, Computers & Securit4. Elsevier, nr. 23, 2004, pagina 371 - 376

[SPRU04] Spruijt, Marcel, *Informatiebeveiliging en bewustzijn,* Informatiebeveiligingjaarboek 2004/2005, Ten Hagen en Stam, nr.1, 2004

[WEL04] Wel, Jaap van der, *Veilige informatie-uitwisseling zonder de zorg te compliceren*, Medisch contact, september 2004

[WIPA09] Wipawayangkool, Kamphol, *Exploring the nature of security awareness: A philosophical perspective*, Issues in Information Systems, Volume X, No. 2, 2009

Boeken

[CIAL01] Cialdini, Robert, *Influence: Science and Practice,* Allyn & Bacon, 4th edition, 2001

[DHIL07] Dhillon, Gurpreet, *Principles of information systems security: text and cases, Jogn Willey & Sons, 2007*

[LACE09] Lacey, David, *Managing the human factor in information security,* John Wiley & Sons Ltd, West-Sussex, 2009

[LOOI04] Looijen, Maarten, *Beheer van informatiesystemen*, Ten HageStam, 6de druk 2004

[OVER07] Overbeek, Paul, e.a., *Informatiebeveiliging onder controle*, Pearson Education Benelux B.V, juni 2007

[PELT05] Peltier, Thomas, e.a, *Information Security Fundamentals*, CRC Press, 2005

[TANE03] Tanenbaum, Andrew, *Computernetwerken*, Pearson Education Benelux B.V., 4e editie, maart 2003

[WHIT09] Whitaker, Andrew, *Chained exploits: Advanced Hacking Attacks from Start to Finish*, Addison-Wesley Proffesional, 2009

Internetbronnen

[BAIL10] Bailey, David, *Identity theft check up: Electronic Medical Records are the new credit cards*, Redpin Information Security Assessment, 2010 http://www.redspin.com/blog/2010/03/03/identity-theft-check-up-electronic-medical-records-are-the-new-credit-cards/

[CHAP10] Chapman, Alan, *Conscious competence learning model, stages of learning*, 2003-2010 http://www.businessballs.com/consciouscompetencelearningmodel.htm

[FELL08] Fellows, *Onderzoek naar Identiteitsfraude*, oktober 2008 http://www.vitasys.nl/content/21837/download/clnt/22987_IdentiteitsfraudeKoggenlander.pdf

[HEAD08] Headline, *Informatiebeveiliging in de zorg van levensbelang*, HEAD, Vereniging van financials, september 2008. Nummer 109, 25e jaargang http://www.headonline.nl/dsc?c=getobject&s=obj&objectid=1665&!sessionid=1lYKh2rESxt7shQMc8wifEJY0Ms2xeUF0l13O9Gm9WMmlywPu1tafNJgLg6zRPhi&!dsname=HEADExtern

[HINE05] Hiner, Jason, *Change your company's culture to combat Social Engineering attacks,* Gartner Information Security conference, 2005 http://articles.techrepublic.com.com/5100-10878_11-1047991.html

[MEDI09] MedicalFacts, *Informatiebeveiliging binnen de zorg,* Medicalfacts.nl., april 2009 http://www.medicalfacts.nl/2009/04/20/informatiebeveiliging-binnen-de-zorg/

[NEN7510] NEN 7510, Informatiebeveiliging binnen de zorgsector http://www.nen7510.org/publicaties/3409

[PVIB08] PvIB, *Basiskennis beveiliging van informatie*, 2008 http://www.ibpedia.nl/images/8/83/Basiskennis_beveiligen_van_informatie_18e.pdf

[THES10] Thesis BV, *Leerstijlen van Kolb*, 2005 – 2010 http://www.thesis.nl/kolb/

[VLIE09] Vliet, Mark van, *Informatiebeveiliging in de zorg,* Getronics Consulting, 2009 http://www.getronicsconsulting.com/web/file?uuid=e6403d62-8cb8-4c18-a076-0cde1107dbab&owner=4269fe99-6d30-4cb6-87d5-cd4f9f6107a6&contentid=1075

[WOLT05] Wolthuis, Alinda, NEN 7510: Zorgsector krijgt oog voor informatiebeveiliging, TNO magazine, december 2005

http://www.tno.nl/images/shared/overtno/magazine/ict4_2005_13_zorg.pdf

Appendix C: Figuren- en tabbellenlijst

Figuur **Pagina**

Tabel

Appendix D: Contactinformatie

Naam:	Danny Hamelink
Telefoon:	06-50547468
E-mail:	danny.hamelink@gmail.com

Naam:	Dr. Luca Consoli
Bezoekadres:	Heyendaalseweg 135 6525 AJ Nijmegen
Postadres:	Postbus 9010 6500 GL Nijmegen
Telefoon:	024-3653065
E-mail:	l.consoli@science.ru.nl

Naam:	Prof. dr. ir. Theo van der Weide
Bezoekadres:	Heyendaalseweg 135 6525 AJ Nijmegen
Postadres:	Postbus 9010 6500 GL Nijmegen
Telefoon:	024-3653361
E-mail:	th.p.vanderweide@cs.ru.nl