Social engineering binnen de Nederlandse Rijksoverheid

Onderzoek naar informatiebeveiligingsbeleid

Student:	Dennis Spijker
Identiteitsnummer:	850957727

Datum rapport:	12 november 2017
Datum presentatie:	24 november 2017
Datum einde inschrijving:	23 april 2018

Social engineering binnen de Nederlandse Rijksoverheid

Onderzoek naar informatiebeveiligingsbeleid

Social engineering within the Dutch Government

Research into information security policy

Opleiding:	Open Universiteit, faculteit Management, Science & Technology Masteropleiding Business Process Management & IT
Programme:	Open University of the Netherlands, faculty of Management, Science & Technology Master Business Process Management & IT
Cursus:	IM9806 Afstudeertraject Business Process Management and IT
Student:	Dennis Spijker
Identiteitsnummer:	850957727
Datum:	12 november 2017
Afstudeerbegeleider	dr. ir. H.L. Jonker
Meelezer	prof. dr. R.J. Kusters
Versie nummer:	1.0
Status:	definitief

Abstract

In het beveiligen van informatie binnen organisaties, is de rol van de medewerker cruciaal in het kunnen weerstaan van social engineeringsaanvallen. De medewerker heeft immers vanuit zijn/haar functie geautoriseerd toegang tot (delen) van informatie, deze bevoegdheid kan door aanvallers worden misbruikt om zo toch over de benodigde informatie te kunnen beschikken. Binnen de scope van de Rijksoverheid is onderzocht in hoeverre er beleid is op social engineering, de medewerkers bewust zijn van dit beleid en of medewerkers slachtoffer zijn van social engineering.

Het onderzoek laat zien dat in het Rijksinformatiebeveiligingsbeleid en de onderliggende maatregelen er onvoldoende aandacht is voor social engineering als dreigingsfactor. Ook is 52% van de medewerkers en 38% van de managers onvoldoende bekend met het begrip, de motieven, de methoden en het aanvalsverloop van social engineering. De noodzaak tot handelen is groot, ongeveer de helft (49%) van de medewerkers binnen de Rijksdienst heeft aangegeven dat deze het afgelopen half jaar te maken heeft gehad met één of meerdere social engineeringsaanvallen.

Het gepresenteerde referentieraamwerk kan als basis dienen om gericht beleid op social engineering te ontwikkelen en daarmee uitvoering te geven aan het vergroten van de awareness op social engineering onder medewerkers.

Sleutelbegrippen

Social engineering, Rijksoverheid, informatiebeveiligingsbeleid, medewerker awareness, management

Voorwoord

De opleiding Business Process Management & IT aan de Open Universiteit heeft mij een kijkje in de keuken van het wetenschappelijk onderzoek gebracht, ik heb genoten van de verdieping en de leerzame stof. Hoewel de reis langer duurde dan ik vooraf had verwacht of gehoopt, is deze het meer dan waard geweest. Deze scriptie over het onderzoek naar social engineering binnen de Rijksoverheid vormt het afsluitende deel van de opleiding.

Het realiseren van dit onderzoek was niet mogelijk geweest zonder de medewerking van tal van betrokken. Allereerst wil ik graag mijn afstudeerbegeleiders dr. ir. Hugo Jonker en prof. dr. Rob Kusters bedanken voor de begeleiding en feedback gedurende het literatuuronderzoek en het empirisch onderzoek.

Alle medewerkers binnen de Rijksdienst dank voor het deelnemen aan de survey, en in het bijzonder de geïnterviewde informatiebeveiligingsfunctionarissen die openhartig hun ervaringen met mij wilden delen. Speciale dank aan Harmke en Eric voor het vertrouwen om mij als externe onderzoeker te willen ontvangen en voor de begeleiding binnen de organisatie.

Tot slot wil ik mijn familie en in het bijzonder mijn vrouw en kinderen bedanken voor de steun, het geduld en de aanmoediging de afgelopen jaren.

Dennis Spijker

November 2017

Samenvatting

Informatiebeveiliging is er op gericht om de informatie binnen organisaties, d.m.v. organisatorische processen en technische maatregelen te beschermen tegen onbevoegden. Een aanvaller die dergelijke beveiligingsmechanisme wil omzeilen kan daarbij gebruiken van social engineering technieken, zoals het misbruiken van de goede wil van medewerkers en daardoor toch (onbevoegd) informatie weten te verkrijgen. In het beveiligen van informatie binnen organisaties, is de rol van de medewerker cruciaal in het kunnen weerstaan van social engineeringsaanvallen. De medewerker heeft immers vanuit zijn/haar functie geautoriseerd toegang tot (delen) van informatie, deze bevoegdheid kan door aanvallers worden misbruikt om zo toch over de benodigde informatie te kunnen beschikken.

Het doel van dit onderzoek is om te achterhalen welke van de geïdentificeerde social engineeringsmaatregelen uit het literatuuronderzoek zijn doorgevoerd binnen het informatiebeveiligingsbeleid van de Rijksoverheid en de mate waarin managers en medewerkers op de hoogte zijn van dit informatiebeveiligingsbeleid. Daarnaast wordt onderzocht in hoeverre de Rijksoverheid slachtoffer is van social engineering. Om het aanwezige informatiebeveiligingsbeleid en de werking in de praktijk vast te kunnen stellen, is een archiefonderzoek naar het beleid uitgevoerd, zijn informatiebeveiligingsfunctionarissen van de Rijksdienst geïnterviewd en is een online survey onder alle medewerkers uitgezet.

Belangrijke algemene maatregelen in de strijd tegen social engineering zijn volgens het referentieraamwerk; opleiding en bewustwording, management buy-in en incidentopvolging. Het archiefonderzoek laat zien er in het Rijksbeleid en de informatiebeveiligingsmaatregelen onvoldoende aandacht is voor social engineering als dreigingsfactor. Het survey onderzoek wijst uit dat 52% van de medewerkers en 38% van de managers onvoldoende bekend is met het begrip, de motieven, de methoden en het aanvalsverloop van social engineering. Ruim 84% van de medewerkers geeft aan een training m.b.t. social engineering wenselijk te vinden en slechts 36% van de medewerkers ervaart dat het informatiebeveiligingsbeleid actief wordt uitgedragen.

De noodzaak tot handelen is groot, ongeveer de helft (49%) van de medewerkers binnen de Rijksdienst heeft ook aangegeven dat deze het afgelopen half jaar te maken heeft gehad met één of meerdere social engineeringsaanvallen.

Met de resultaten van dit onderzoek, pleit dit voor het inzetten op twee zaken; a. maak werk van Rijksbeleid gericht op social engineering en b. werk door trainingen, opleiding aan het vergroten van de awareness op social engineering. Het ontwikkelde referentieraamwerk kan hierbij als vertrekpunt dienen, om de volledigheid van de aanpak te toetsen en daarbij prioritering in het beleid op social engineering aan te brengen. De gevoerde aanpak op phishing mail binnen de Rijksoverheid laat zien dat dit effect heeft op het bewustzijn, deze werd namelijk door alle (100%) medewerkers herkend.

Inhoudsopgave

1. Introductie

1.1. Inleiding

Dit document beschrijft de opzet, uitvoering en resultaten van het herhalende onderzoek naar social engineering binnen de Nederlandse Rijksoverheid. Het eerder uitgevoerde onderzoek (Van der Laan, 2016) vormt de basis voor dit herhalende onderzoek en zal als onderdeel van het onderzoek ook worden onderzocht op aanpak en de mogelijkheden om deze te generaliseren en te hanteren voor andere rijksoverheid onderdelen.

Het doel van dit empirisch onderzoek is het herhalen van het eerder uitgevoerde wetenschappelijk onderzoek naar social engineering binnen de Rijksoverheid en daarmee staven c.q. uitbreiden van de opgebouwde kennis-set. Het document dient tevens als bewijs van het kunnen uitvoeren van wetenschappelijk onderzoek en vormt het afsluitende examen van de Open Universiteit opleiding Business Proces Management & IT.

Het document is als volgt opgebouwd:
In hoofdstuk 1 worden de context van het onderzoek, de relevantie, de probleemstelling en de opdrachtformulering gepresenteerd.
In hoofdstuk 2 wordt het ontwerp van het onderzoek behandeld, de opzet van het empirisch onderzoek. Aspecten die voorbijkomen zijn de doelstelling, onderzoeksvragen, afbakening en scope, onderzoeksbenadering en de onderzoekspopulatie.
In hoofdstuk 3 komt de methode van onderzoek aan de orde. Dit hoofdstuk beschrijft de onderzoeksstrategie, welke onderzoeksmethoden bestaan, welke zijn gebruikt en de reden waarom hiervoor is gekozen. Vervolgens wordt de methode van dataverzameling beschreven.
In hoofdstuk 4 wordt de uitvoering van het onderzoek behandeld, een terugblik op hoe het praktijkonderzoek is verlopen.
In hoofdstuk 5 worden de resultaten van het onderzoek gepresenteerd.
In hoofdstuk 6 wordt teruggekeken naar de doelstelling en onderzoeksvragen om deze vervolgens te beantwoorden, hier conclusies uit te trekken en worden aanbevelingen voor verder onderzoek gedaan.
In hoofdstuk 7 wordt een product- en procesreflectie gepresenteerd. Hier wordt gereflecteerd op de kwaliteit van het onderzoek en de houdbaarheid van de conclusies. Tevens wordt besproken wat goed ging en wat beter kan in de toekomst, met de bijbehorende leerpunten.

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

In de bijlagen zijn additioneel de gebruikte en verkregen onderzoeksgegevens opgenomen, het gaat om Bijlage A: Aanvalstactieken social engineering en Bijlage B: Maatregelen Informatiebeveiliging die zijn gebruikt in het referentieraamwerk, Bijlage C: Online survey vragen en Bijlage D: Interview vragen zoals gehanteerd in het onderzoek en Bijlage E: Uitgewerkte Interviews als bron voor de resultaten van dit onderzoek.

1.2. Context

De aanleiding van dit onderzoek vormt de constatering dat er onvoldoende wetenschappelijk literatuur is naar social engineering binnen overheden en in het bijzonder in relatie tot de Nederlandse Rijksoverheid (Van der Laan, 2016).

Social engineering is een aanvalstechniek binnen de context van informatiebeveiliging. Informatiebeveiliging is er op gericht om de informatie binnen organisaties, d.m.v. organisatorische, proces en technische maatregelen te beschermen tegen onbevoegden. Een aanvaller die dergelijke beveiligingsmechanisme wil omzeilen kan daarbij gebruiken van social engineering technieken, zoals het misbruiken van de goede wil van medewerkers en daardoor toch (onbevoegd) informatie weten te verkrijgen. Uit eerdere onderzoeken uitgevoerd binnen andere sectoren en landen, is gebleken dat 48 % van de grotere organisaties en 32 % van de kleinere organisaties te maken hebben gehad met social engineeringsaanvallen (Van der Laan, 2016).

Het vorig jaar uitgevoerde onderzoek naar social engineering binnen de Rijksoverheid (Van der Laan, 2016) laat zien dat er een wezenlijk verschil is in de mate waarin informatiebeveiligingsbeleid is doorgevoerd binnen de Rijksoverheid en de mate waarin de medewerkers op de hoogte zijn van dit informatiebeveiligingsbeleid. Vrijwel alle informatiebeveiligingsmaatregelen op het gebied van social engineeringsaanvallen, zoals geïdentificeerd in het literatuuronderzoek, zijn alleen indirect aanwezig in het informatiebeveiligingsbeleid van de Rijksoverheid. Daarnaast concludeert Laan in zijn onderzoek dat dit informatiebeveiligingsbeleid niet volledig is op het gebied van social engineering en deze onvoldoende doordringt tot de werkvloer. De gemiddelde social engineering awareness van een medewerker ligt in dit onderzoek op 65 %, waarbij 5 van de 19 social engineering aspecten onder de 50 procent scoren en slechts één aspect de volledige 100 procent.

In deze herhalingsstudie zal het eerder ingezette onderzoekswerk worden voortgezet, dat wil zeggen op basis van de eerder gehanteerde opzet zal opnieuw een Rijksonderdeel worden onderzocht naar het gehanteerde beleid, de bekendheid met de gevaren en blootstelling aan social engineeringsaanvallen. Daarnaast zal het onderzoek worden verbreed naar de rol van het management, om de conclusie van Van der Laan op het onvoldoende doordringen tot de werkvloer verder te kunnen staven.

1.3. Relevantie

Dit herhalende onderzoek naar social engineering kent een wetenschappelijke relevantie door het verkrijgen van een breder inzicht naar ;

- Wat het informatiebeveiligingsbeleid is van de Nederlandse Rijksoverheid m.b.t. social engineering .
- Of de medewerkers van de Nederlandse Rijksoverheid zich bewust zijn van het geldende informatiebeveiligingsbeleid.
- Of er verschillen waarneembaar zijn tussen management en medewerker m.b.t. informatiebeveiligingsbeleid en de praktijk.
- In welke mate de Nederlandse Rijksoverheid zelf slachtoffer is van social engineeringsaanvallen.

Daarnaast kent het onderzoek ook een praktische relevantie voor de Nederlandse Rijksoverheid als geheel en het onderzochte Rijksonderdeel in het bijzonder;

- Risicobeheersing m.b.t. social engineering: door inzicht te krijgen in de mate van aanwezigheid van informatiebeveiligingsbeleid inzake social engineering kunnen risico's in kaart worden gebracht, om deze vervolgens indien nodig af te dekken.
- Inzicht in de awareness van de medewerkers: de aanwezigheid van informatiebeveiligingsbeleid wil niet zeggen dat alle medewerkers hiervan automatisch op de hoogte zijn. Met het onderzoek wordt inzichtelijk gemaakt in hoeverre de medewerkers op de hoogte zijn van het opgestelde informatiebeveiligingsbeleid.
- Kennismaking met of het ophalen van de kennis met betrekking tot social engineering en de aspecten ervan: de deelnemers aan de interviews en de online survey bouwen kennis op die ze nog niet hadden.

1.4. Probleemstelling

In het beveiligen van informatie binnen organisaties, is de rol van de medewerker cruciaal in het kunnen weerstaan van social engineeringsaanvallen. De medewerker heeft vanuit zijn/haar functie geautoriseerd toegang tot (delen) van informatie, deze bevoegdheid kan door aanvallers worden misbruikt om zo toch over de benodigde informatie te kunnen beschikken.

Het doel van dit onderzoek is om te achterhalen welke van de geïdentificeerde social engineeringsmaatregelen uit het literatuuronderzoek (Bijlage B: Maatregelen Informatiebeveiliging) zijn doorgevoerd binnen het informatiebeveiligingsbeleid van de Rijksoverheid en de mate waarin managers en medewerkers op de hoogte zijn van dit informatiebeveiligingsbeleid. Daarnaast zal worden onderzocht in welke mate de Rijksoverheid slachtoffer is van social engineering.

1.5. Opdrachtformulering

De eerste onderzoeksvraag in deze scriptie luidt:

Onderzoeksvraag 1: *Wat is het verschil tussen de mate waarin informatiebeveiligingsbeleid is doorgevoerd binnen de Rijksoverheid omtrent de geïdentificeerde social engineering maatregelen uit het literatuuronderzoek en de mate waarin de medewerkers en management op de hoogte zijn van dit informatiebeveiligingsbeleid?*

Hierbij zijn de volgende twee hypotheses geformuleerd:

Hypothese 1: Het informatiebeveiligingsbeleid met betrekking tot social engineering binnen de Rijksoverheid is niet bekend bij het merendeel van de medewerkers.

Gesteld wordt dat minimaal de helft van de medewerkers (50%) bevestigend moet kunnen antwoorden op de vragen rondom het bekend zijn met het gevoerde informatiebeveiligingsbeleid op social engineering.

Hypothese 2: Het informatiebeveiligingsbeleid met betrekking tot social engineering binnen de Rijksoverheid wordt niet uitgedragen door het management.

Uitdragen wordt geïnterpreteerd als het actief informeren van medewerkers over het beleid. Gesteld wordt dat minimaal de helft van medewerkers (50%) bevestigend moet antwoorden om te kunnen spreken over het uitdragen van informatiebeveiligingsbeleid binnen de afdelingen.

De deelvragen die horen bij de eerste onderzoeksvraag:

Deelvraag 1: *Welke informatiebeveiligingsdocumenten zijn leidend binnen de Nederlandse Rijksoverheid?*
Deelvraag 2: *Zijn de medewerkers binnen de Rijksoverheid inhoudelijk bekend met deze informatiebeveiligingsdocumenten?*
Deelvraag 3: *Zijn de medewerkers binnen de Rijksoverheid bekend met de terminologie van social engineering?*
Deelvraag 4: *Welke social engineering maatregelen worden op beleidsniveau direct of indirect afgedekt door het aanwezige informatiebeveiligingsbeleid binnen de Rijksoverheid?*
Deelvraag 5: *Wat is de mate van awareness van de medewerkers binnen de Rijksoverheid van het informatiebeveiligingsbeleid met betrekking tot social engineering?*
Deelvraag 6: *Is er een verschil waarneembaar tussen het management en de medewerkers, qua bekendheid met het informatiebeveiligingsbeleid en de kennis over social engineering?*

De tweede onderzoeksvraag in deze scriptie luidt:

Onderzoeksvraag 2: *In hoeverre is de Rijksoverheid zelf het doelwit of slachtoffer van social engineering aanvallen?*

Hierbij is de volgende hypothese geformuleerd:

Hypothese 3: Meer dan 50 procent van de onderzochte Rijksoverheid-medewerkers is in de afgelopen zes maanden slachtoffer geweest van een social engineering aanval.

De deelvragen die horen bij de tweede onderzoeksvraag:

Deelvraag 7: *Van welke social engineering aanvallen is de Nederlandse Rijksoverheid in het afgelopen jaar slachtoffer geweest en welk medium gebruikten deze aanvallen?*

2. Ontwerp en aanpak

2.1. Onderzoeksbenadering

Het onderzoek is deductief van aard, dat wil zeggen met de uit de literatuurstudie verkregen theorie is een model opgebouwd, waarmee de praktijksituatie zal worden getoetst. De basis van het theoretisch model (referentieraamwerk) vormt het uitgevoerde literatuuronderzoek (Van der Laan, 2016) (Spijker, 2016), waarmee het informatiebeveiligingsbeleid in relatie tot social engineering en de kennis hierover binnen de Rijksoverheid zal worden getoetst.

Het door Van der Laan gehanteerde social engineering referentieraamwerk is voor dit vervolgonderzoek herontwerpen, dat wil zeggen herzien en uitgebreid, om de herhaalbaarheid en de herkenbaarheid van de studie binnen een bredere Rijksoverheid context mogelijk te maken. In paragraaf 2.3 zal de opzet van het referentieraamwerk voor dit onderzoek verder worden besproken.

De onderzoeksvragen hebben zowel een kwalitatief als kwantitatief karakter, dit pleit voor een gemengde methode van data verzamelen. Door een kwantitatieve benadering is het mogelijk om op basis van de verkregen resultaten, uitspraken te kunnen generaliseren en bevindingen te verklaren in relatie tot de onderzoekspopulatie. Om het aanwezige informatiebeveiligingsbeleid en de werking in de praktijk (diepte) vast te kunnen stellen, zal gebruik moeten worden gemaakt van kwalitatieve methoden.

Door deze combinatie van methoden is triangulatie mogelijk, door zowel kwantitatieve als kwalitatieve gegevens te verzamelen ontstaat een rijker beeld van het onderzoeksveld.
In hoofdstuk 3 zal de gehanteerde methodologie en mogelijke inzetbare onderzoeksinstrumenten verder worden besproken.

2.2. Doelstellingen

De doelstellingen van dit empirisch onderzoek zijn:

- Te onderzoeken in hoeverre er informatiebeveiligingsbeleid is opgesteld met betrekking tot social engineering binnen de Nederlandse Rijksoverheid.
- De dekkingsgraad van het informatiebeveiligingsbeleid inzake social engineering te beschrijven.
- De bewustwording van het informatiebeveiligingsbeleid met betrekking tot social engineering bij de medewerkers te bevorderen.
- Aan te geven hoe bekend de medewerkers van de Rijksoverheid zijn met het begrip social engineering en de terminologie van social engineering.
- Te onderzoeken of er verschillen waarneembaar zijn tussen management en medewerkers, qua bekendheid met beleid en kennis over social engineering.
- Te onderzoeken of de Nederlandse Rijksoverheid te maken heeft gehad met aanvallen via social engineering in de afgelopen zes maanden.

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

2.3. Referentieraamwerk

Voor het onderzoek is een referentieraamwerk ontwikkeld. Het referentieraamwerk onderkent de in de literatuurstudie gevonden social engineeringsaanvallen en informatiebeveiligingsmaatregelen, welke zullen worden gebruikt voor het empirisch onderzoek. Door deze tegen elkaar af te zetten is het tevens mogelijk de onderlinge relatie weer te geven en de relevantie van maatregelen te bepalen. Met de verkregen onderzoekresultaten kunnen verklaringen worden gezocht en antwoorden geformuleerd op de gestelde hypothesen en onderzoeksvragen, daarnaast kunnen deze uitkomsten worden gebruikt om het referentieraamwerk aan te scherpen met de uit de praktijk verkregen inzichten.

Aan deze herhalingsstudie ligt het eerder uitgevoerde onderzoek van Van der Laan (Van der Laan, 2016) ten grondslag dat als uitkomst een conceptueel model heeft van de verschillende social engineering aanvalstactieken en de geïdentificeerde beveiligingsmaatregelen. Dit conceptuele model zal op punten worden herzien en uitgebreid, om de herhaalbaarheid en de herkenbaarheid van de studie binnen de bredere Rijksoverheid context mogelijk te maken. Daarnaast zijn in het oorspronkelijke raamwerk ook een aantal hiaten geconstateerd, die hieronder worden besproken en indien mogelijk zijn verwerkt in het gehanteerde onderzoeksmodel.

Het gehanteerde onderzoeksmodel van Van der Laan (Van der Laan, 2016) naar social engineering binnen de Rijksoverheid onderkent wel alle in de literatuurstudie behandelde social engineering aanvalstypen, maar niet alle behandelde beveiligingsmaatregelen. Uit de toelichting blijkt niet welke afwegingen de auteur hierbij heeft gemaakt om delen wel of niet op te nemen. Opmerkelijk is dat daarbij de onderwerpen “betrokkenheid management” en “opleiding, bewustwording” in de behandelde literatuur als essentiële beveiligingsmaatregelen worden genoemd, deze terugkomen in het referentieraamwerk, maar vervolgens niet in het uit te voeren empirisch onderzoek worden betrokken en behandeld.

De lijst van social engineering aanvalstypen onderkent een twintigtal technieken, in het onderliggende literatuuronderzoek ontbreken echter een tweetal technieken. Voor de volledigheid van het onderzoek zijn de ontbrekende technieken “Mail-outs” en “Phreaking” toegevoegd aan de verklarende lijst van social engineering technieken, zie Bijlage A: Aanvalstactieken social engineering.

Van der Laan behandeld in de literatuurstudie Laan (Van der Laan, 2016) de ISO 27001 Code voor informatiebeveiliging, waarbij social engineering maatregelen zijn gegroepeerd naar de stadia/verloop van een dienstverband van een medewerker. Deze groepering biedt mijn ziens een prima kapstok om het referentieraamwerk op volledigheid van onderwerpen te toetsen en daarbij ook recht te doen aan de onderwerpen “betrokkenheid management” en “opleiding, bewustwording”. Door het model daarbij slechts uit te breiden, wordt daarmee de herhaalbaarheid van de studie geen geweld aan gedaan. Daarnaast draagt het gebruik van de ISO standaard ook bij aan de herkenbaarheid binnen het onderzoeksdomein, de Rijksoverheid. Het te onderzoeken Rijksoverheid beveiligingsbeleid en de BIR maatregelen zijn immers afgeleiden van de ISO 27001 norm.

Om genoemde bezwaren weg te nemen, is het referentieraamwerk social engineering Figuur 1 als volgt opgezet en uitgewerkt.

				Nr	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
				Soort	Organisatorisch							Fysiek					Organisatorisch						Logisch		Organisatorisch	
				Thema	Personele beveiliging							Toegangsbeveiliging					Informatiebeveiliging								Beveiligingsproces	
				ISO 27001	8.1.2	8.1.3	8.2.1	8.2.2	8.2.3	8.3.2	8.3.3	9.1.1	9.1.2	9.1.2	9.1.2	9.1.3	7.2.1	10.7.3	10.9.3	11.3.1	11.3.2	11.3.3	10.4.1	10.8.4	13.1.1	15.2.1
Nr	Fase	Aard	Aanvalstactiek	Maatregel	Screening CV, referenties*	Arbeids-voorwaarden	Management buy-in	Opleiding en bewustwording	Disciplinaire maatregelen	Retourneren bedrijfsmiddelen	Blokkering toegangsrechten	Beveiligings-camera's	Aanmeldprocedure bezoekers*	Bezoekerspasjes	Foto-identificatiepasjes	Toegangsdeuren*	Informatie classificatie	Documentafhandeling/-vernietiging	Beperken publieke informatie*	Wachtwoord management	Locken van computer	Clean desk	Antivirus / antiphishing	E-mailfiltering	Incident afhandeling	Audit beleid / audit controles
1	Voorbereiding	M	Dumpster diving				X	X				X		X		X		X						X	X
2		M	People spotting				X	X				X				X								X	X
3		M	Physical reconnaissance / Shoulder surfing				X	X				X	X	X		X						X	X		X	X
4		M	Pretexting / Profiling		X		X	X					X	X	X		X	X	X	X						X
5		T	Mail-outs*				X	X											X				X	X	X	X
6		T	Phishing				X	X									X	X	X	X			X	X	X	X
7		T	Phreaking* / Vishing				X	X		X	X						X	X	X	X					X	X
8		T	Virtual reconnaissance / Waterholing				X	X											X	X			X		X	X
9		T	Web search				X	X									X		X							X
10	Manipulatie	M	Physical Impersonation		X		X	X		X	X	X	X	X	X	X		X	X						X	X
11		M	Reverse social engineering		X		X	X				X	X	X		X	X		X	X	X	X			X	X
12		T	Virtual impersonation / Fake profiles		X		X	X		X	X							X	X						X	X
13	Exploitatie	M	Direct approach			X	X	X	X			X	X	X	X	X	X	X			X			X	X	X
14		M	Office Snooping / Desk sniffing				X	X				X	X	X	X	X		X		X	X	X			X	X
15		M	Piggybacking / Tailgating			X	X	X	X			X	X	X		X									X	X
16		T	Baiting / Item dropping			X	X	X	X							X							X		X	X
17		T	Data leakage				X	X			X					X	X	X					X	X	X	X
18	Uitvoering	M / T	Identity theft				X	X		X	X		X		X	X	X			X					X	X
19		T	Malicious software				X	X			X									X			X	X	X	X

Figuur 1 Social Engineering referentieraamwerk, aanvallen x maatregelen

In het referentieraamwerk social engineering (Figuur 1) zijn de social engineering aanvalstactieken afgezet tegenover de te nemen maatregelen. Per social engineeringsaanval is met een X aangegeven welke maatregelen relevant zijn in het afdekken van het potentiele risico dat een (overheids-)organisatie loopt. Een *zwarte* X representeert de weergave zoals overgenomen uit het oorspronkelijke model van Laan, een *groen* of *rood* gekleurde X geeft respectievelijk weer dat het model op dat punt is aangevuld met relevante maatregelen of de relevantie van de maatregel in twijfel wordt getrokken.

Door het model op te zetten naar de fasen van de social engineeringsaanval tegenover de soort en het thema van de maatregel, is door deze context in één oogopslag duidelijk welke maatregelen passend zijn op bepaalde social engineering aanvalstactieken. De aard van de social engineeringsaanval kan daarbij *(M)enselijk* of *(T)echnologisch* zijn en heeft betrekking op een fase van *voorbereidende*, *manipulatieve*, *exploiterende* of *uitvoerende* activiteiten. De te nemen maatregelen zijn te groeperen naar het thema, *personele beveiliging, toegangsbeveiliging, informatiebeveiliging* of hebben betrekking op het *beveiligingsproces*. Daarbij is tevens de soort maatregel, *fysiek, logisch* of *organisatorisch* en de link naar de Baseline Informatiebeveiliging Rijk (BIR) / ISO 27001 norm weergegeven.

Door de social engineeringsaanvallen te groeperen naar de fase van een aanval, bleek ook dat er drie aanvallen in het model waren opgenomen die volgens de theorie geen social engineeringsaanval zijn. “Manipulatie van emoties” is een psychologische vorm van het uitbuiten van emoties in bijvoorbeeld de manipulatie fase. “Advanced persistent threat” is een verzamelnaam van gecombineerde (langdurige) technologische aanvallen. “Internal Threats” is zeker een dreiging, maar geen social engineeringsaanval. De eerder opgenomen aanvallen, “Manipulatie van emoties”, “Advanced persistent threat” en “Internal Threats” zijn daarom buiten beschouwing gelaten en buiten het model gelaten. Het totaal aantal social engineeringsaanvallen betrokken in dit onderzoek komt daarmee op 19.

Door het eiken van de maatregelen met de BIR / ISO 27001 norm, blijkt uit de gegeven toelichting in het onderzoek van Laan, dat er een discrepantie is ontstaan in de uitleg en daarmee de invulling van de relevantie van maatregelen in het onderzoek. De maatregel “Beperken datalekken” is in het empirisch onderzoek ingevuld als “het voordoen en afhandelen van een (datalek-) beveiligingsincident”, terwijl in de onderliggende theorie wordt gesproken over “het verminderen van de hoeveelheid …publieke informatie”. Ook bleken drie beschreven maatregelen niet verwerkt in het model; “Arbeidsvoorwaarden duidelijk ?”, “Beperken datalekken” en “Incidentafhandelingsstrategie”.

Om de herhaalbaarheid van het onderzoek in tact te houden zijn de volgende twee maatregelen onderscheiden en als volgt opgenomen in het raamwerk;

- Nr. 15 - “Beperken publieke informatie”, het verminderen van de hoeveelheid beschikbare specifieke gegevens zorgt ervoor dat een aanval niet de moeite waard is. Websites, openbare databases, internetregisters en andere publiek toegankelijke bronnen dienen alleen algemene informatie te bevatten.
- Nr. 21 - “Incident afhandeling”, een gedocumenteerde incidentreactiestrategie zal ervoor zorgen dat een gebruiker onder druk precies weet welke procedures hij dient te volgen.

Daarnaast is “Arbeidsvoorwaarden” aan het raamwerk Figuur 1 toegevoegd onder maatregelnummer 2.

De maatregelen “Controle beschikbaarheid positieve referenties” en “Controle juistheid van Curriculum” worden als complementair beschouwd en zijn daarom samengevoegd tot “Screening CV en referenties”.

Het totaal aantal maatregelen komt daarmee op 22. De complete lijst aan maatregelen en omschrijvingen is toegevoegd als Bijlage B: Maatregelen Informatiebeveiliging.

2.4. Scope

Het empirisch onderzoek zal plaats vinden binnen de Nederlandse Rijksoverheid.

De Rijksoverheid is onderdeel van de overheid en bestaat onder andere uit elf ministeries in Den Haag, de uitvoerende diensten die onder deze ministeries vallen en de Hoge Colleges van Staat. In totaal werken er bij de Rijksoverheid zo’n 100.000 rijksambtenaren, verspreid over heel Nederland.

Onder de verantwoordelijkheid van de ministeries vallen veel ambtelijke organisaties en uitvoerende diensten, ook wel sectoren of Rijksdiensten genoemd, daarnaast maken verschillende zelfstandige bestuursorganen, inspecties en agentschappen deel uit van de Rijksoverheid.

Gegeven deze omvangrijke context, daarbij de beperkte tijd, middelen en onderzoekscapaciteit die beschikbaar zijn tijdens deze afstudeeropdracht, is besloten om in te zoomen op één Rijksdienst. Het resultaat van dit onderzoek zal worden vergeleken met het in 2016 uitgevoerde onderzoek (Van der Laan, 2016) bij twee andere Rijksonderdelen.

2.5. Afbakening en voorwaarden

In dit onderzoek wordt niet onderzocht in hoeverre de Nederlandse Rijksoverheid beschermd is tegen social engineering. Het gaat in dit onderzoek om de aanwezigheid en het bewustzijn van het informatiebeveiligingsbeleid.

Het anonimiseren van de resultaten van het onderzoek is een harde voorwaarde van de betreffende Rijksdienst om mee te werken aan dit onderzoek. Tevens is bepaald dat het onderzoek plaats moet vinden op de hoofdlocatie van de Rijksdienst, medewerkers op nevenlocaties zijn daarmee uitgesloten van dit onderzoek.

3. Methodologie

3.1. Onderzoeksmethode

Om de onderzoeksvragen te kunnen beantwoorden en de hypothese bij de probleemstelling te staven, is een passende onderzoeksmethode nodig. Er zijn verschillende methoden om onderzoek uit te voeren, in het begeleidende boek “Methoden en technieken van onderzoek” (Saunders, 2015) worden zeven methoden onderscheiden; het experiment, het survey onderzoek, de casestudy, de action research, de grounded theory, de etnografie en het archiefonderzoek. Elk van deze methoden hebben voor- en nadelen in verschillende situaties. De keuze voor een methode hangt af van een aantal factoren, zoals het soort onderzoeksvraag, de controle die de onderzoeker heeft over de feitelijke gedragsgebeurtenissen en de focus op hedendaagse of historische verschijnselen.

Een korte uiteenzetting van de methoden, kenmerken en mogelijke toepasbaarheid voor deze studie.

methode	toelichting	kenmerken	toepasbaar
experiment	Doel van een experiment is het bestuderen van causale verbanden, door na te gaan of een verandering in één onafhankelijke variabele een verandering teweegbrengt in een andere afhankelijke variabele.	- Formeren van experimentele en controle groepen - Willekeurige toedeling aan groepen - Onderzoeker bepaald welke blootstelling plaats vindt - Minimale invloeden van buitenaf - Voor en achteraf metingen	NEE
survey (deductief)	Met een survey onderzoek is het mogelijk door middel van een gestandaardiseerde vragenlijst, kwantitatieve data te verzamelen, die met behulp van beschrijvende en verklarende statistieken kunnen worden geanalyseerd.	- Een ruim domein, veel onderzoekseenheden - Arbeidsintensieve data generatie - Meer breedte dan diepte - (a)selecte steekproef - Kwantitatieve data en analyse	JA
casestudy	De casestudy is vooral interessant als je een goed begrip wilt krijgen van de context van het onderzoek en de processen die worden doorlopen. Verklarend en verkennend onderzoek, beantwoorden van waarom, wat en hoe vragen.	- Een smal domein, klein aantal onderzoekseenheden - Arbeidsintensieve benadering - Meer diepte dan breedte - Een selecte steekproef - Open waarneming op locatie - Kwalitatieve data en onderzoeksmethoden	JA
action research	Action research kent als onderzoeksvorm een expliciete nadruk op actie, zoals de gevolgen van veranderingen, samen met betrokkenen te onderzoeken. Geschikt voor het beantwoorden van hoe	- Nadruk op doorvoeren van veranderingen - Actieve betrokkenheid onderzoeker in het veranderproces - Verkrijgen van inzicht door verkennen, volgen en beoordelen van deelnemers	NEE

methode	toelichting	kenmerken	toepasbaar
	vragen.	- Actieve deelname betrokkenen bij het proces	
grounded theory (inductief)	Met een grounded theory aanpak ligt de nadruk op het ontwikkelen en opbouwen van een theorie, waarbij geprobeerd wordt gedrag te voorspellen en te verklaren.	- Een zoekende houding van de onderzoeker - Voortdurend onderling met elkaar vergelijken van empirische data en theoretische concepten - Zorgvuldige en consequente toepassing van procedures en technieken van data-analyse en betekenis geven aan de data	NEE
etnografie (inductief)	Etnografie is gericht op het beschrijven en interpreteren van de sociale wereld door middel van een onderzoek uit eerste hand.	- Beschrijven van een cultuur - Inzicht verkrijgen in een bepaalde context vanuit perspectief van de betrokkenen - Actieve deelname onderzoeker aan het sociale proces - Methode kost zeer veel tijd, bestrijkt langere periodes van onderzoek	NEE
archief onderzoek	Archiefonderzoek richt zich op het onderzoek van voornamelijk administratieve gegevens en documenten als bron.	- Gebruik maken van eerder en door anderen geproduceerd onderzoeksmateriaal - Onderzoekvragen gericht op het verleden en de veranderingen in de loop van de tijd. - Haalbaarheid onderzoek sterk afhankelijk van beschikbaarheid van documenten.	JA

Tabel 1 Onderzoeksmethoden, kenmerken en toepasbaarheid

De eerste indicatie van toepasbaarheid in Tabel 1 laat zien, dat op basis van de kenmerken van de methoden van onderzoek, zowel het survey onderzoek, de casestudy als het archiefonderzoek in het licht van de deductieve opzet van de onderzoeksvragen in deze studie toepasbaar zijn.

De onderzoeksvragen hebben zowel een kwalitatief als kwantitatief karakter. Dit pleit voor een gemengde methode van data verzamelen.

Om de hypothesen te kunnen toetsen en uitspraken te generaliseren, is een brede studie om kwantitatieve data te kunnen verzamelen gewenst. Het survey onderzoek zal worden gebruikt om de kennis over het informatiebeveiligingsbeleid en social engineering, door middel van vragenlijsten te toetsen.

Om het aanwezige informatiebeveiligingsbeleid en de werking in de praktijk (diepte) vast te kunnen stellen, zullen respectievelijk de instrumenten archiefonderzoek en case study worden ingezet.

Door deze combinatie van methoden is triangulatie mogelijk, door de kwalitatieve gegevens verkregen uit de interviews te vergelijken met de kwantitatieve gegevens verkregen uit de survey, ontstaat een rijker beeld van het onderzoeksveld.

3.2. Onderzoekspopulatie

Een belangrijk onderdeel van het empirisch onderzoek is de samenstelling van de onderzoeksgroepen. De onderzoeksgroepen bestaan uit medewerkers van de participerende Rijksdienst.

De representativiteit van de populatie is afhankelijk van de bereidheid van de Rijksdienst en haar medewerkers om deel te nemen aan het onderzoek. Idealiter nemen alle afdelingen en medewerkers deel aan het onderzoek. In verband met de beperking in tijd, geld en capaciteit van zowel de onderzoeker als de Rijksdienst is dit niet haalbaar.

Voor deze studie zijn twee onderzoeksgroepen samengesteld, waarbij verschillende varianten zijn gekozen om de onderzoeksgroep te bepalen.

Onderzoeksgroep 1: selecte steekproef

Deze onderzoeksgroep is door de onderzoeker selectief samengesteld. De geselecteerde medewerkers hebben een rol als IB-functionaris binnen een afdeling. Deze medewerkers zijn bekend met de gehanteerde aanpak en terminologie, hebben goed zicht op de uitvoering van het informatiebeveiligingsbeleid in de praktijk en specifiek het onderzoeksonderwerp social engineering.

Onderzoeksgroep 2: aselecte steekproef

Deze onderzoeksgroep is aselectief samengesteld, dat wil zeggen alle medewerkers binnen de populatie van de Rijksdienst kunnen deelnemen aan het onderzoek. Door geen beperkingen in de deelnemersgroep op te leggen, ontstaat inzicht in de reikwijdte van het informatiebeveiligingsbeleid en specifiek het onderzoeksonderwerp social engineering.

3.3. Onderzoekstrategie

In deze paragraaf zal een beknopt overzicht gegeven worden van de gehanteerde strategie bij de uitvoering van dit onderzoek.

De onderzoeksstrategie bestaat uit de volgende opeenvolgende stappen:

- **Eerste aanzet onderzoeksplan** Schetsen van de contouren van een herhalingsstudie naar social engineering, opstellen onderzoeksvragen en plan van aanpak.
- **Opstellen conceptueel raamwerk** Op basis van de verkregen informatie uit de literatuurstudie, afstemming met begeleiders en prototyping, zal een conceptueel raamwerk worden opgesteld. Het raamwerk dient als basis voor het verdere empirisch onderzoek.
- **Uitwerken onderzoeksplan** Het beschrijven van de aanpak, gehanteerde methoden, populatie en bronnen.
- **Starten uitvoering onderzoek, uitzetten survey** Afstemmen met de organisatie over praktische invulling van het onderzoek, communicatie en organiseren fysieke toegang onderzoeker. Start van informatieverzameling via een online survey met de groep aselectief geselecteerde medewerkers.

- **Archiefonderzoek beleidsdocumenten** Onderzoek van informatiebeveiligingsbeleid en aanvullende documenten. De resultaten worden gebruikt om onderzoeksvraag 1 te beantwoorden.
- **Casestudy, afnemen interviews** Informatieverzameling door interviews met de groep selectief geselecteerde medewerkers.
- **Analyse interviews** De interviews worden met elkaar vergeleken om te bepalen welke overeenkomsten en verschillen er zijn. Deze informatie wordt gebruikt bij het beantwoorden van onderzoeksvraag 1.
- **Analyse survey** Verwerken en duiden resultaten kennis en bewustzijn over informatiebeveiligingsbeleid en social engineering. Deze informatie wordt gebruikt bij het beantwoorden van onderzoeksvragen 1 en 2.
- **Schrijven eindverslag** Het uiteindelijke resultaat is een verslaglegging van de bevonden resultaten die voortkomen uit de hierboven genoemde stappen. Tevens geeft de scriptie antwoord op de onderzoeksvragen in de vorm van een conclusie en wordt in de reflectie teruggeblikt op het uitgevoerde onderzoek.
- **Presentatie scriptie** De presentatie vormt het slotstuk van het afstudeeronderzoek. In deze presentatie zal een samenvatting worden gegeven over het onderzoeksverloop met daarin de belangrijkste bevindingen en conclusies.

3.4. Data en databronnen

Voor het empirisch onderzoek worden de volgende data en databronnen geraadpleegd.

Methode	Bron
Archiefonderzoek	De afdeling Beveiliging van de Rijksdienst is gevraagd naar relevante documentatie omtrent het aanwezige informatiebeveiligingsbeleid op het onderzoeksonderwerp social engineering. Deze documenten kunnen o.a. bestaan uit beleidstukken, 'factsheets', 'best practices', procesbeschrijvingen en/of trainingsmateriaal.
Casestudy	Onderzoeksgroep 1 zal door middel van interviews (Bijlage D: Interview vragen) worden bevraagd naar de werking in de praktijk (diepte) van het informatiebeveiligingsbeleid.
Survey onderzoek	Onderzoeksgroep 2 zal door middel van een gestructureerde vragenlijst (Bijlage C: Online survey vragen) worden bevraagd op de kennis over het informatiebeveiligingsbeleid, maatregelen en ervaringen omtrent het onderzoeksonderwerp social engineering.

Tabel 2 Overzicht gehanteerde data en databronnen

3.5. Dataverzameling

Door de gevoeligheid van de materie en de bedachtzaamheid over de mogelijke gevolgen van de constateringen in een onderzoek, zijn organisaties en haar medewerkers over het algemeen zeer beschermend in het delen van informatie. Om de bereidheid van het delen van gegevens in het kader van dit onderzoek te vergroten en daarmee meer waarde uit het onderzoek te halen, is in het data verzamelen de volgende aanpak en werkwijze gehanteerd.

Archiefonderzoek

In het archiefonderzoek naar het aanwezige informatiebeveiligingsbeleid omtrent het onderzoeksonderwerp social engineering, zijn in afstemming met de afdeling Beveiliging van de Rijksdienst, de volgende documenten als relevant voor het onderzoeksonderwerp geacht en geanalyseerd;

- Beveiligingsvoorschrift Rijksdienst (BVR); (Rijksoverheid, 2013)
- Voorschrift Informatiebeveiliging Rijksdienst (VIR); (Rijksoverheid, 2007)
- Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie (VIRBI); (Rijksoverheid, 2013)
- Archiefwet; (Rijksoverheid, 2015)
- Algemeen Rijksambtenarenreglement; (Rijksoverheid, 2017)
- Baseline Informatiebeveiliging Rijksoverheid - Tactisch Normenkader (BIR-TNK); (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2012)
- Operationele Handreiking Informatiebeveiliging (BIR-OH); (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2013)
- BIR Quick Scan; (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2014)
- BIR comply or explainprocedure; (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2014)
- Handboek Beveiliging
- Intranet Huisregels en praktische zaken beveiliging
- Intranet communicatie phishing acties en resultaten
- Voorlichtingsmateriaal, o.a. “tips bij phishing” en “phishing voorbeelden”.

Casestudy

De casestudy zal worden ingevuld door middel van het interviewen van de individuele deelnemers in onderzoeksgroep 1. Een interview wordt geprefereerd boven andere technieken, zoals waarnemingen en vragenlijsten, doordat de onderzoeker dan meer invloed heeft op de richting van het onderzoeksvragen en tevens actief de kwaliteit van beantwoording kan bewaken. Voor het interview kan worden gekozen tussen ongestructureerde, semi-gestructureerde en gestructureerde interviews (Saunders, 2015). Door de brede omvang van het onderwerp kan een ongestructureerd interview tot lange discussies leiden over minder relevante zaken. Een volledig gestructureerd interview elimineert echter de mogelijkheid om verder te gaan met onderwerpen van grote relevantie die niet voorzien zijn. Daarom is voor dit onderzoek gekozen om semi-gestructureerde interviews af te nemen, om daarmee oog te houden voor de relevantie van de antwoorden op de specifieke onderzoeksvragen.

Om deze herhalingsstudie mogelijk te maken zijn de interviewvragen uit het eerder onderzoek van Laan gegeneraliseerd, waarbij specifieke termen en context-specifieke woorden zijn vervangen door Rijksbrede en daardoor meer herkenbare terminologie. Aanvullend zijn enkele interviewvragen opgenomen om het onderwerp ‘management buy-in’ in dit onderzoek uitvoeriger aan bod te laten komen. De structuur van het interview en de vragen zijn toegevoegd aan dit rapport als Bijlage D: Interview vragen.

De deelnemers in onderzoeksgroep 1 zullen persoonlijk, dan wel telefonisch en/of per mail worden benaderd om deel te nemen aan het interview. De geplande afspraak zal met een email worden bevestigd, waarbij tevens doel en achtergrond van het onderzoek zal worden verstrekt. Om het interview tijdsefficiënt te laten verlopen en de onderzoeker te laten concentreren op de inhoud van

de vragen, worden de interviewgesprekken opgenomen. Deelnemers krijgen achteraf het uitgewerkte interviewverslag ter controle aangeboden, zodat eventuele correcties kunnen worden doorgevoerd.

Survey onderzoek

Het survey onderzoek zal via een online vragenlijst worden afgenomen. Aangezien de populatie van onderzoeksgroep 2 bestaat uit alle medewerkers van het hoofdkantoor van de Rijksdienst, wordt het verzoek tot deelname aan de vragenlijst door de afdeling Beveiliging via een interne mailgroep verspreid. Door de mail via de afdeling Beveiliging te versturen, wordt de legitimiteit van het onderzoek onderstreept en zullen de deelnemers deze oproep eerder vertrouwen en bereid zijn mee te werken aan het onderzoek. Deze oproep tot deelname zal na 2 weken worden herhaald, gestreefd wordt naar een deelnamepercentage van minimaal 30% van de populatie.

Omdat het survey onderzoek ondersteunend is aan de diepte interviewvragen, ligt de focus van de survey op de breedte (kwantiteit). Om deze omvang te kunnen verwerken zijn de vragen in de vragenlijst alleen in een gesloten vorm gesteld. In de vragenlijst wordt gewerkt met dichotome Ja/Nee vragen, meerkeuze vragen en schaal (1 t/m 5) vragen. De vragen kennen een vluchtmogelijkheid in de vorm van “onbekend” of “wens ik niet te beantwoorden” .

De survey wordt anoniem afgenomen om binnen de onderzoeksgroep de bereidwilligheid om deel te nemen te vergroten en daarmee de respons te verhogen (CBS, 2012).

De social engineering aanvalstypen worden als niet algemeen bekend veronderstelt, daarom zal in de survey een korte toelichting op deze technieken worden gegeven. Mogelijk herkennen medewerkers wel het scenario c.q. de methode, maar zijn niet bekend met het technische of Engelstalige vakjargon. Door deze aanvulling gaat het onderwerp social engineering meer leven en kan het bijdragen aan een completer beeld op wat er wordt waargenomen op de werkvloer.

3.6. Betrouwbaarheid

Om de betrouwbaarheid van het onderzoek te verhogen zijn de volgende maatregelen genomen om fouten en/of vertekening (bias) problemen bij de online survey en het interview weg te nemen.

3.6.1. Deelnemers

De deelnemers, aan zowel de online survey als het interview, moeten vrijelijk antwoord kunnen geven op de gestelde vragen, zonder daarbij druk en/of sociale wenselijkheid te voelen. Om dit te waarborgen is de deelname aan de online survey en de interviews anoniem.

Om alle medewerkers in de gelegenheid te stellen om deel te kunnen nemen aan de online survey, is deze gedurende een periode van 6 weken opengesteld. In de aankondigingsmail gericht aan alle medewerkers van het hoofdkantoor is inzicht gegeven in het doel en de legitimiteit van het onderzoek, daarnaast is de anonimiteit van deelname benadrukt en tevens de geschatte duur van ca. 10 minuten benoemd. Ook is in de mail vermeld dat de onderzoeker een geheimhoudingsverklaring heeft getekend, zodat deelnemers geen belemmeringen voelen om informatie met de onderzoeker te delen. Om de legitimiteit van het onderzoek te vergroten is de mail vanaf het interne mailadres van de afdeling Beveiliging van de Rijksdienst verstuurd. In de vierde onderzoeksweek is een herinneringsmail verstuurd en de sluitingstermijn van de online survey gecommuniceerd.

Het moment van deelname aan het interview en de locatie is in overleg met de deelnemers tot stand gekomen. De deelnemers ontvingen een mail met de bevestiging van de afspraak en de opzet van interviewvragen, zodat geen misverstand kon ontstaan over het moment, het doel en de vorm van het interview.

Om de vertrouwelijke setting tijdens de interviews te waarborgen en ook interrupties te voorkomen vonden de interviews plaats in een afgesloten ruimte/vergaderzaal, waarin alleen deelnemer en onderzoeker aanwezig waren. Bij de start van het interview zijn de deelnemers gewezen op de anonimiteit, de mogelijkheid om een vraag onbeantwoord te laten en het aanbod het verslag van het interview, ter verificatie in te kunnen zien en eventueel nog aan te passen. Dit alles, om de deelnemers een omgeving te bieden, waarbinnen een open gesprek mogelijk is.

3.6.2. Onderzoeker

De vragen in zowel de online survey als de interviews, zijn gebaseerd op het referentieraamwerk social engineering, welke is voortgekomen uit het eerder uitgevoerde literatuuronderzoek.

De online survey kent alleen gesloten vragen en werkt met dichotome Ja/Nee vragen, meerkeuze vragen en schaal (1 t/m 5) vragen voor een eenduidige interpretatie. Deze dient ter ondersteuning bij het kunnen generaliseren van uitspraken in samenhang met de gehouden interviews (triangulatie).

De onderzoeker heeft zelf alle interviews afgenomen en daarmee bijgedragen aan een identiek verloop. Tijdens het interview is gewerkt met een vaste interviewstructuur/opzet, zodat alle deelnemers dezelfde voorwaarden hadden waarbinnen het interview plaats vond. Daarnaast bood de interviewstructuur de onderzoeker de mogelijkheid te controleren of alle noodzakelijke stappen waren doorlopen en daarmee rust, focus om het interview af te kunnen nemen.

De interviews zijn met toestemming van de deelnemers opgenomen, zodat tijdens het interview de onderzoeker zich kon richten op het interview. Wel heeft de onderzoeker tijdens de interviews in steekwoorden bij de vragen meegeschreven, dit om eventueel uitvallen van de opnamen te ondervangen. Daarnaast bood het de mogelijkheid om het antwoord te toetsen op volledigheid, door deze kernachtig samen te kunnen vatten of te herhalen indien het antwoord voor de onderzoeker niet voldoende duidelijk was, dan wel het nodig was een antwoord te verifiëren. Het uitgewerkte interviewverslag is aan de deelnemers aangeboden, zodat eventuele fouten in het verslag konden worden gecorrigeerd.

In alle communicatie is consequent het mailadres en mobiele nummer van de onderzoeker vermeld, zodat bij eventuele problemen, onduidelijkheid of vragen rechtstreeks contact kon worden opgenomen.

3.7. Validiteit

Het onderzoek kent de volgende interne en externe validiteitswaarborgen.

Interne validiteit

De resultaten van het onderzoek zijn intern valide als er gemeten wordt, wat er gemeten moet worden. Hieraan is voldaan door de juiste bronnen te koppelen aan de juiste onderzoeksstrategie.

Verder is er literatuuronderzoek verricht zodat de informatiebeveiligingsmaatregelen ten opzichte van de social engineering aanvallen duidelijk in kaart zijn gebracht.

Externe validiteit

De resultaten van het onderzoek zijn extern valide als wat er gemeten wordt, ook valide is voor vergelijkbare omgevingen en daarmee te generaliseren zijn.

Het onderzoek vindt plaats binnen een Rijksoverheidsdienst, waarbinnen tal van beleidsmaatregelen in het kader van informatiebeveiliging Rijksbreed zijn opgesteld. Dit maakt het mogelijk om resultaten van dit onderzoek te generaliseren daar waar het Rijksbeleid betreft.

De resultaten van dit onderzoek met betrekking tot de kennis van medewerkers over het informatiebeveiligingsbeleid en social engineering is niet generaliseerbaar. De mate van invulling van het te voeren beleid is Rijksdienst specifiek en sterk afhankelijk van de omgeving en de belangen waarbinnen deze dienst opereert.

3.8. Ethische aspecten

Aan het uitvoeren van wetenschappelijk onderzoek zijn ethische kwesties als privacy, vrijwilligheid, instemming, vertrouwelijkheid en objectiviteit verbonden (Saunders, 2015). Gedurende het onderzoek zijn de volgende maatregelen genomen om te anticiperen op ethische problemen;

- De onderzoeker verklaart de zes principes - eerlijkheid en zorgvuldigheid, betrouwbaarheid, controleerbaarheid onpartijdigheid, onafhankelijkheid en verantwoordelijkheid - en haar uitwerkingen van de Nederlandse Gedragscode Wetenschapsbeoefening (VSNU, 2014) te hebben gelezen en te respecteren in dit onderzoek.
- Alle deelnemers aan het onderzoek zijn vooraf schriftelijk en indien van toepassing bij het interview nogmaals mondeling, geïnformeerd over;
    - het doel en de duur van het onderzoek,
    - de vertrouwelijkheid en anonimiteit bij het verzamelen en verwerken van de onderzoeksgegevens,
    - de garantie dat alleen de onderzoeker toegang heeft tot de verzamelde data.
    - de onderzoeker geen ander belang heeft dan het onderzoeksbelang,
    - de onderzoeker niet in opdracht van de werkgever onderzoek uitvoert,
    - de onderzoeker niet werkzaam is voor de betreffende organisatie, maar wel een geheimhoudingsverklaring heeft ondertekend,
    - de vrijwillige basis en het recht niet deel te nemen aan het onderzoek,
    - het recht om vragen onbeantwoord te laten, dan wel de mogelijkheid te bieden niet van toepassing te selecteren.
- Aanvullend zijn de deelnemers aan de interviews vooraf;
    - geïnformeerd dat het doel niet is om goede en foute antwoorden in kaart te brengen, maar om het beeld te vangen dat de Rijksdienst zo goed mogelijk weerspiegeld,
    - geïnformeerd en om toestemming gevraagd om het interviewgesprek te mogen opnemen, met als enig doel het kunnen gesprek zo correct mogelijk te kunnen weergeven in het verslag, waarna het opgenomen gesprek zal worden gewist,
    - geïnformeerd over de mogelijkheid om het uitgewerkte gespreksverslag in te zien en de vrijheid daarin teksten te kunnen corrigeren of weg te halen, voordat deze met schriftelijke toestemming worden opgenomen in het onderzoek.
- Alle onderzoeksgegevens zijn beschikbaar in dit verslag. De onderzoeker heeft de onderzoeksgegevens geanonimiseerd, verwijzingen naar de Rijksdiensten, medewerkers en of locaties zijn verwijderd.

4. Uitvoering

De uitvoering van het onderzoek had wel wat meer voeten in aarde, dan ik op voorhand had gedacht. Hoewel we met elkaar al het onderwerp van onderzoek en de wijze van uitvoeren hadden verkend, bleken er bij het opstarten van het onderzoek toch nog wel de nodige vragen over de vertrouwelijkheid en de geboden waarborgen. Het heeft er toe geleid dat de daadwerkelijk start van het onderzoek binnen de Rijksdienst pas enkele weken later plaats kon vinden. Met het ondertekenen van een geheimhoudingsverklaring en toelichting op de onderzoeksmethode en wijze van opslag, was de weg vrij voor het empirisch onderzoek.

Geconfronteerd met deze gevoeligheden rondom het onderzoek, heb ik de waarborgen die ik had genomen tijdens de uitvoering van het onderzoek explicieter benoemd, om daarmee eventuele belemmeringen die kunnen ontstaan gedurende het onderzoek weg te nemen.

Om te voorkomen dat het gebruik van Google Forms voor de online survey vragen zou oproepen over het gebruik van gegevens en daarmee een mogelijke belemmering voor de deelname aan het onderzoek zou kunnen vormen, heb ik in de inleidende tekst bij de survey nadrukkelijk vermeld dat alleen de resultaten worden opgeslagen en er geen andere gebruikersgegevens worden verzameld. Daarbij tevens benadrukt dat voor de opslag gebruik wordt gemaakt van de afgeschermde OU omgeving en alleen de onderzoeker toegang heeft tot deze gegevens.

In de aankondigingsmail richting alle medewerkers van de Rijksdienst heb ik explicieter benadrukt wat de intenties van het onderzoek zijn en op welke wijze de resultaten zullen worden verwerkt en gebruikt. Ook heb ik vermeld dat ik als onderzoeker een geheimhoudingsverklaring heb getekend en alle informatie anoniem zal worden verzameld en vertrouwelijk met de gegevens zal worden omgegaan.

In de weken voorafgaand aan het onderzoek, bleken er een tweetal phishing-campagnes te zijn gehouden. Het was daarom noodzakelijk om duidelijk onderscheid te maken en niet vanaf een extern mailadres het verzoek “met een link naar het onderzoek” te mailen. De aankondigingsmail heb ik in overleg door de afdeling Beveiliging laten versturen, hierdoor werden de legitimiteit en de betrouwbaarheid van de mail en het onderzoek onderstreept.

De uitvoering van het onderzoek verliep met genomen waarborgen zeer voorspoedig, in de eerste week was de survey onder de medewerkers uitgezet en waren alle deelnemers aan de interviews benadert en de meeste afspraken daartoe al ingepland. Door de vakantieperiode waren niet alle geïnterviewden beschikbaar. In de uitvoering heb ik daarmee rekening gehouden door in twee rondes de interviews af te nemen, de eerste ronde half juli met medewerkers die nog op vakantie gingen en een tweede ronde met interviews begin augustus met medewerkers die net terug waren van vakantie. De online survey heb ik om dezelfde reden langer opgehouden, zodat alle medewerkers van de Rijksdienst in staat gesteld waren om deel te kunnen nemen.

Met het versturen van de herinneringsmail aan de mailgroep van het hoofdkantoor bleek uit de reactie van een medewerker werkzaam op een nevenvestiging dat deze ook de mail had ontvangen. De mail was duidelijk gericht aan alle medewerkers van het hoofdkantoor, ik kan echter niet uitsluiten dat mogelijk ook medewerkers van nevenvestigingen de mail hebben ontvangen en hebben deelgenomen aan de survey. Gezien de anonieme werkwijze, zijn de deelnemers hierop niet te filteren. Overigens verwacht ik niet dat het resultaat hierdoor veel anders is, de gehanteerde en onderzochte werkwijzen gelden immers binnen de gehele Rijksdienst. Wel kan het zijn dat bepaalde fysieke beveiligingsmaatregelen verschillen per locatie en dat hierop afwijkend is geantwoord.

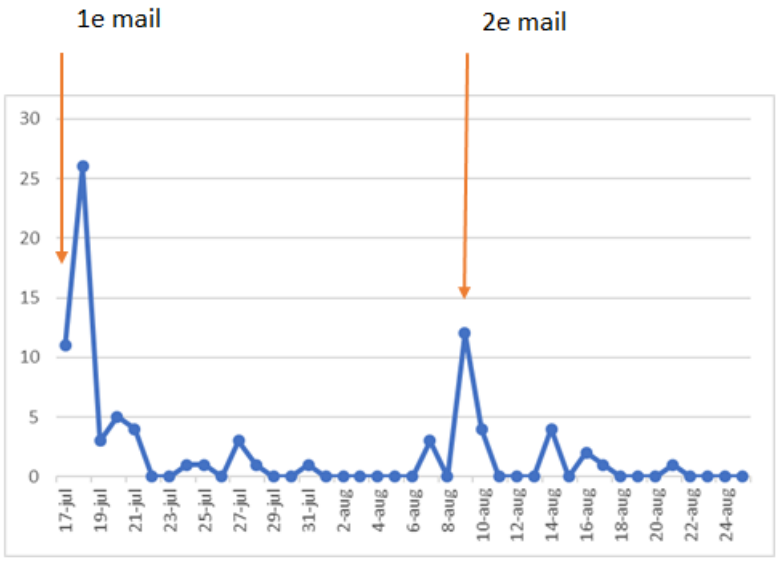
5. Resultaten

5.1. Response en respondenten

In totaal hebben in de onderzoeksperiode van 17 juli tot en met 25 augustus, 83 respondenten van de groep aselectief geselecteerde deelnemers deelgenomen aan de online survey. De antwoorden van één respondent bleken niet valide / tegenstrijdig in de meerkeuze vragen en zijn om die reden niet mee genomen in het verdere onderzoek.

Voor de online survey is op 17 juli een eerste mailing verstuurt aan de medewerkers die voorkwamen in de interne mailgroep van de hoofdlocatie van de onderzochte Rijksdienst.

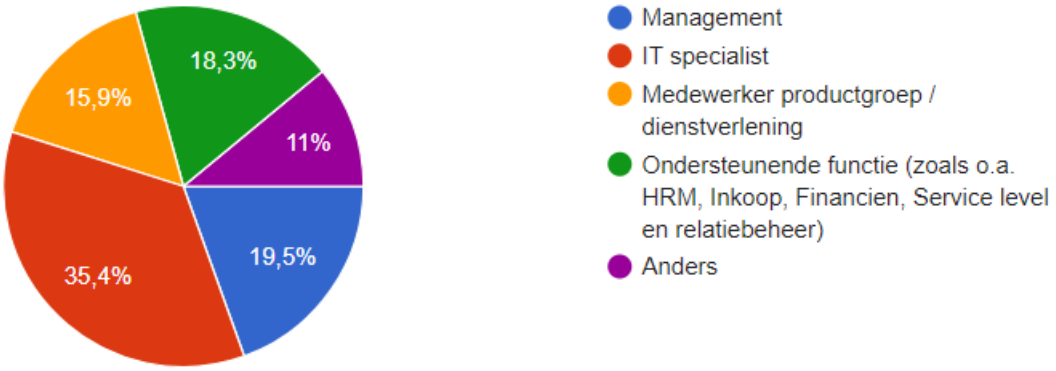
Op 9 augustus is dit verzoek herhaalt en tevens de sluitingsdatum van de survey op 25 augustus gecommuniceerd.



Figuur 2 Response online survey periode 17-7 t.m. 25-8

Figuur 2 laat de response aantallen van de online survey binnen de onderzoeksperiode zien. In de grafiek is het effect van de mailings met het verzoek tot deelname duidelijk waarneembaar.

De grootste groep deelnemers bestond uit medewerkers die zichzelf onder de categorie IT specialist scharen, te weten 29 deelnemers, gevolgd door de groep Management met 16 deelnemers.



Figuur 3 Achtergrond respondenten online survey

Van de 82 respondenten werkt bijna de helft (49%), 40 deelnemers, langer dan 5 jaar in de huidige functie. 30 respondenten (36%) werken 2 tot 5 jaar in de huidige functie, 12 deelnemers (15%) werken korter dan 2 jaar binnen de huidige functie. Van de deelnemers is het merendeel in dienst 69 (83%) tegenover 13 (16%) externe medewerkers.

Onder de respondenten heeft 71 % aangegeven toegang te hebben tot vertrouwelijke informatie vanuit zijn/haar functie. Een kwart (24%) van de respondenten heeft geen toegang tot vertrouwelijke informatie en 5% wenst deze vraag niet te beantwoorden.

Van de benaderde 8 deelnemers van selectief geselecteerd groep IBF medewerkers is het gelukt alle acht te interviewen. De geselecteerde IBF'ers werken op verschillende afdelingen binnen de Rijksdienst en kennen ook verschillende achtergronden, zie ook Figuur 4. Alle geïnterviewde medewerkers vervullen de IBF rol minimaal een jaar, het merendeel (5/8) minimaal 2 jaar. Daarbij moet opgemerkt worden dat de huidige inrichting van de beveiligingsorganisatie met ondersteunende IBF medewerkers ca. 2,5 jaar bestaat. De geïnterviewde medewerkers werken allen minimaal 3 jaar voor de organisatie, de meesten (6/8) 7 jaar of langer. De afdelingen waarvoor zij werken lopen qua medewerkers aantallen uitéén van 10 tot 45, waarbij op de grotere (> 40 medewerkers) afdelingen veelal met twee IBF'ers wordt gewerkt.

Management	1
IT specialist	3
Medewerker productgroep	3
Ondersteunende functie	1
Anders	0
Totaal	8

Figuur 4 Achtergrond respondenten interviews

Voor het archiefonderzoek zijn de volgende documenten over informatiebeveiliging en social engineering in het onderzoek betrokken;

- Beveiligingsvoorschrift Rijksdienst (BVR) (Rijksoverheid, 2013) ;
- Voorschrift Informatiebeveiliging Rijksdienst (VIR) (Rijksoverheid, 2007) ;
- Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie (VIRBI) (Rijksoverheid, 2013) ;
- Archiefwet (Rijksoverheid, 2015);
- Wet bescherming persoonsgegevens (Rijksoverheid, 2017);
- Algemeen Rijksambtenarenreglement (Rijksoverheid, 2017);
- Baseline Informatiebeveiliging Rijksoverheid - Tactisch Normenkader (BIR-TNK) (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2012);
- Operationele Handreiking Informatiebeveiliging (BIR-OH) (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2013);
- BIR Quick Scan (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2014);
- BIR comply or explainprocedure (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2014);
- Handboek Beveiliging Rijksdienst;
- Intranet Huisregels en praktische zaken beveiliging;
- Intranet communicatie phishing acties en resultaten;
- Voorlichtingsmateriaal, o.a. "tips bij phishing" en "phishing voorbeelden".

5.2. Informatiebeveiligingsbeleid en awareness

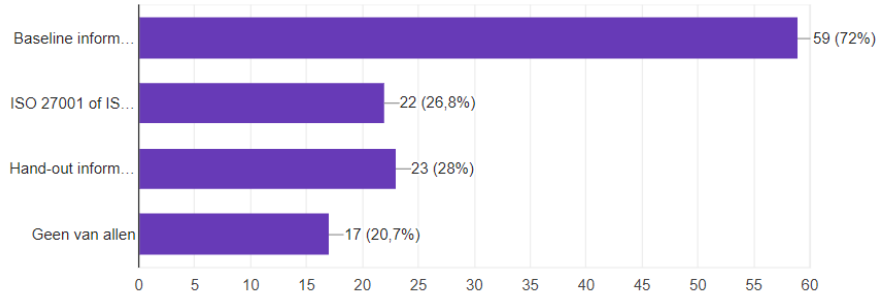
In deze paragraaf worden de resultaten van het onderzoek naar het gevoerde informatiebeveiligingsbeleid en de hierover aanwezige kennis binnen de organisatie behandeld en gepresenteerd. Binnen het onderwerp informatiebeveiligingsbeleid wordt, conform het opgestelde referentiemodel, specifiek stilgestaan bij de achtereenvolgende onderwerpen;

- Personele beveiliging,
- Fysieke toegangsbeveiliging,
- Informatiebeveiliging,
- Beveiligingsproces.

5.2.1. Bekendheid beleid

Uit de gevoerde interviews komt duidelijk het beeld naar voren dat het informatiebeveiligingsbeleid bestaat uit het naleven van de Baseline Informatiebeveiliging Rijk (BIR), het Handboek Beveiliging waarin organisatie specifiek beleid is beschreven en tal van huisregels en genomen maatregelen die voortvloeien uit de BIR. Een enkeling noemt daarbij ook de VIR-BI, het Voorschrift Informatie Rijksdienst – Bijzondere Informatie, waarin afhankelijk van de aard van de informatie er additionele eisen worden gesteld.

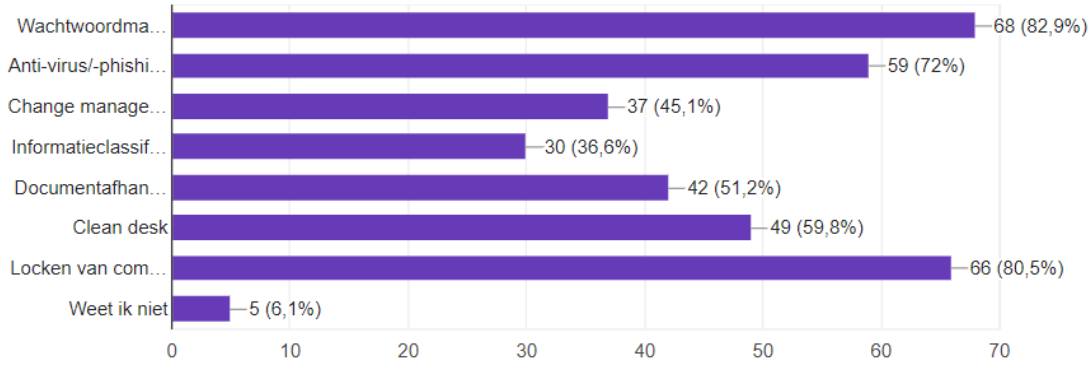
De online survey laat zien dat 72% van de medewerkers inhoudelijk bekend is met de BIR.



Figuur 5 Bekendheid met informatiebeveiligingsdocumenten

Verrassend is dat slechts een kwart (27%) van de medewerkers de ISO 27001/2 noemt, terwijl de BIR deze ISO norm als basis heeft. 21% van de medewerkers is met géén van de documenten bekend.

Op de vraag voor welke aspecten de organisatie een beveiligingsbeleid heeft, wordt door 83% van de medewerkers wachtwoordmanagement genoemd, ruim 80% noemt het locken van de computer en 72% noemt anti-virus/-phishing maatregelen.



Figuur 6 Bekendheid met aspecten van informatiebeveiligingsbeleid

In vergelijk met de vorige vraag, blijkt dat medewerkers eerder (83%) onderdelen van het beleid kunnen noemen dan de beleidsdocumenten zelf (72%). Slechts 6% geeft aan het niet te weten of de organisatie op genoemde punten beleid heeft.

5.2.2. Personele beveiliging

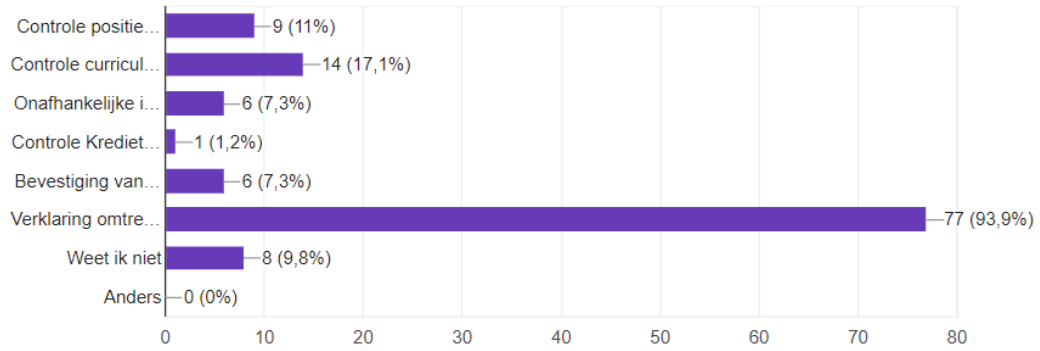
Start dienstverband, screening

Binnen Hoofdstuk II Aanstelling en loopbaanvorming zijn in de artikelen 9, 9a, 10 en 11 van het Algemeen Rijksambtenarenreglement (Rijksoverheid, 2017) de voorwaarden voor aanstelling beschreven. Relevante passages zijn o.a.;

“Teneinde vast te stellen of de betrokkene in voldoende mate geschikt of bekwaam is, wordt deze aan een onderzoek onderworpen, waaronder begrepen het verifiëren en zo nodig aanvullen van de gegevens die door de betrokkene desgevraagd zijn verstrekt.”

“Het bevoegd gezag kan, met uitzondering van de gevallen, bedoeld in het zevende en het achtste lid, van de betrokkene vergen dat deze een verklaring omtrent het gedrag als bedoeld in de Wet justitiële en strafvorderlijke gegevens overlegt.”

Op de vraag of nieuwe medewerkers worden gescreend voordat zij in dienst treden, beantwoordt ruim 90% deze vraag met Ja. De overige deelnemers geven aan dat dit niet zo is (2,4%), anders ligt (2,4%), of zegt het niet te weten (5%). Op de vraag waarop dan gescreend wordt, geeft bijna 94% van de respondenten aan dat een Verklaring omtrent Gedrag (VOG) noodzakelijk is om in dienst te kunnen treden.



Figuur 7 Bekendheid van screeningsmaatregelen bij indiensttreding

Overige screeningsmaatregelen bij het in dienst treden van nieuwe medewerkers, zoals het nagaan van referenties en/of vermelde zaken op het c.v. zijn minder gangbaar volgens de deelnemers van de online survey. De geïnterviewde IBF medewerkers bevestigen dit beeld, met de opmerking dat de afdeling HRM diploma’s controleert en er voor vertrouwensfuncties aanvullend onderzoek plaats vindt.

Verplichtingen Dienstverband, arbeidvoorwaarden en disciplinaire maatregelen

Medewerkers die in dienst treden leggen de eed of belofte af. Hierbij verklaren medewerkers bekend te zijn en zich te zullen houden aan de verplichtingen die horen bij het aanvaarden van de functie. Onderdelen van die verplichtingen zijn in het Algemeen Rijksambtenarenreglement (Rijksoverheid, 2017) vastgelegd. In Hoofdstuk VIIa. Overige rechten en verplichtingen van den ambtenaar, zijn de volgende relevante passages opgenomen;

Artikel 50.1: “De ambtenaar is gehouden de plichten uit zijn functie voortvloeiende nauwgezet en ijverig te vervullen en zich te gedragen, zoals een goed ambtenaar betaamt.”

Artikel 51.1-3: “De ambtenaar is verplicht een eed of een belofte af te leggen.” “Bij regeling van Onze Minister van Binnenlandse Zaken en Koninkrijksrelaties wordt het formulier vastgesteld dat wordt gebruikt voor het afleggen door de ambtenaar van de eed of de belofte.”

In hoofdstuk VIII. Disciplinaire straffen van het Algemeen Rijksambtenarenreglement (Rijksoverheid, 2017) , zijn in de artikelen 80 – 84 de maatregelen beschreven die opgelegd kunnen worden bij plichtsverzuim.

Ook in andere documenten zoals de Baseline Informatiebeveiliging Rijksdienst (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2012) zijn soortgelijk bepalingen opgenomen. Veelal verwijzen deze verplichtingen terug naar de wettelijke regeling Algemeen Rijksambtenarenreglement (Rijksoverheid, 2017).

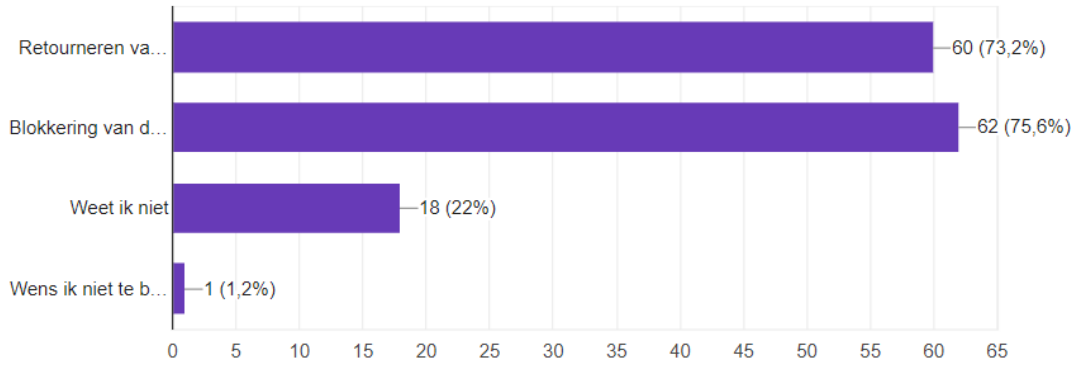
Beëindigen dienstverband, retourneren bedrijfsmiddelen en intrekken van toegangsrechten

In hoofdstuk X Schorsing en ontslag van het Algemeen Rijksambtenarenreglement (Rijksoverheid, 2017) , zijn in de artikelen 90-104a de verplichtingen rondom ontslag geregeld. In de Baseline Informatiebeveiliging Rijksdienst (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2012) is hierover het volgende opgenomen;

“Voor ambtenaren is in de ambtseed of belofte vastgelegd welke verplichtingen ook na beëindiging van het dienstverband of bij functiewijziging nog van kracht blijven en voor hoe lang. Voor ingehuurd personeel (zowel in dienst van een derde bedrijf als individueel) is dit contractueel vastgelegd. Indien nodig wordt een geheimhoudingsverklaring ondertekend. Het lijnmanagement heeft een procedure vastgesteld voor beëindiging van dienstverband, contract of overeenkomst waarin minimaal aandacht besteed wordt aan het intrekken van toegangsrechten, innemen van bedrijfsmiddelen en welke verplichtingen ook na beëindiging van het dienstverband blijven gelden.”

Uit het interviews blijkt dat er binnen de Rijksdienst een autorisatieproces is ingericht met stappen die bij wijzigingen in aanstelling doorlopen moeten worden, waaronder het inleveren van bedrijfsmiddelen, het intrekken gebruikersaccount en het inleveren / intrekken van de toegangspas.

Rondom het beëindigen of wijzigen van het dienstverband is bijna driekwart van de deelnemers bekend met maatregelen zoals het retourneren van bedrijfsmiddelen en het blokkeren van de toegangsrechten. Een kwart van de deelnemers weet het niet (22%) of wenst de vraag niet te beantwoorden (1%).



Figuur 8 Bekend met maatregelen bij beëindigen dienstverband

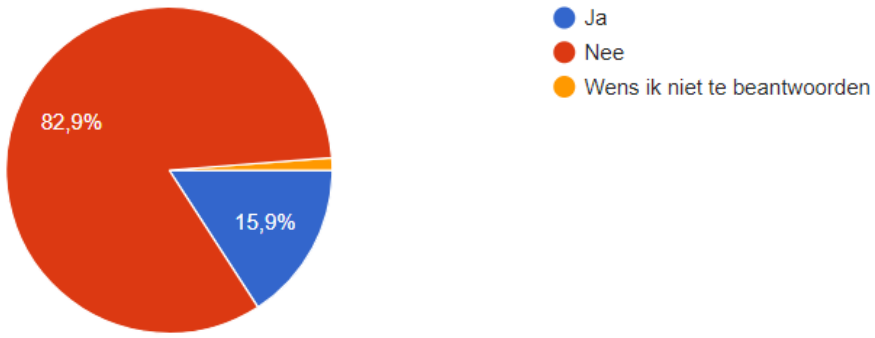
Opleiding, training medewerkers

Kennis opbouw wordt in de onderzochte literatuur genoemd als belangrijke pijler in de te nemen maatregelen in informatiebeveiliging en bij social engineering (Van der Laan, 2016) (Spijker, 2016). In paragraaf 8.2.2. van de Baseline Informatiebeveiliging Rijksdienst (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2012) wordt bewustzijn, opleiding en training ten aanzien van informatiebeveiliging als volgt verwoordt;

“Alle werknemers van de organisatie en, voorzover van toepassing, ingehuurd personeel en externe gebruikers, behoren geschikte training en regelmatige bijscholing te krijgen met betrekking tot beleid en procedures van de organisatie, voor zover relevant voor hun functie.”

Uit de interviews blijkt dat het uitdragen en communiceren over informatiebeveiliging binnen de organisatie een vast onderdeel is van het IBF overleg. De informatiebeveiligingsfunctionarissen (IBF) van de diverse afdelingen, aangevuld met de medewerkers van de afdeling Beveiliging, stemmen binnen dit overleg af over organisatiebrede communicatieonderwerpen, zoals het aandacht vragen voor thema’s als clean desk, het locken van de werkplek en het aanspreken van meelopers/onbekenden op de afdeling. Daarnaast vinden er Rijksbrede acties plaats zoals recent een phishing campagne.

Op de vraag of u ooit vanuit deze organisatie een cursus/training aangeboden heeft gekregen inzake informatiebeveiliging of social engineering, antwoordt 83% met Nee, 16% met Ja of 1% wenst dit niet te beantwoorden.



Figuur 9 Training of cursus gevolgd inzake informatiebeveiliging of social engineering

Op de vraag als u de mogelijkheid krijgt binnen de organisatie, om een training te volgen m.b.t. informatiebeveiliging / social engineering, beantwoordt 84% van de deelnemers deze vraag met Ja deze te willen volgen, 14% Nee of wenst dit niet te beantwoorden (2%).

Dit beeld wordt bevestigd in de afgenomen interviews, waarin wordt aangegeven dat het uitdragen van beleid vanuit de organisatie te weinig is en kan beter. “Bewustwording en ook privacy-aspecten moeten gewoon jaarlijks terugkerende thema’s zijn, zeker gezien de informatieverwerkende rol binnen het Rijk. Bij mijn vorige werkgever bijvoorbeeld, moest iedereen verplicht jaarlijks een online training volgen en het certificaat overleggen.” Een andere suggestie was om meer in te zetten op online trainingen met voorlichtingsfilmpjes, als maatregel om het bewustzijn op het informatiebeveiligingsbeleid en social engineering te vergroten.

Management buy-in

Het management vormt volgens de onderzochte literatuur (Van der Laan, 2016) (Spijker, 2016) een belangrijke factor in het dragen van het informatiebeveiligingsbeleid. In het Beveiligingsvoorschrift Rijksdienst (Rijksoverheid, 2013) is in artikel 5 het volgende opgenomen over de verantwoordelijkheid van het management;

“Binnen het geheel aan kaders is de lijnmanager verantwoordelijk voor de integrale beveiliging van zijn organisatie (onderdeel), de inrichting en werking van de organisatie daarvan, evenals de zorg voor en de beveiliging van het te beschermen belang die aan zijn onderdeel is toevertrouwd. De

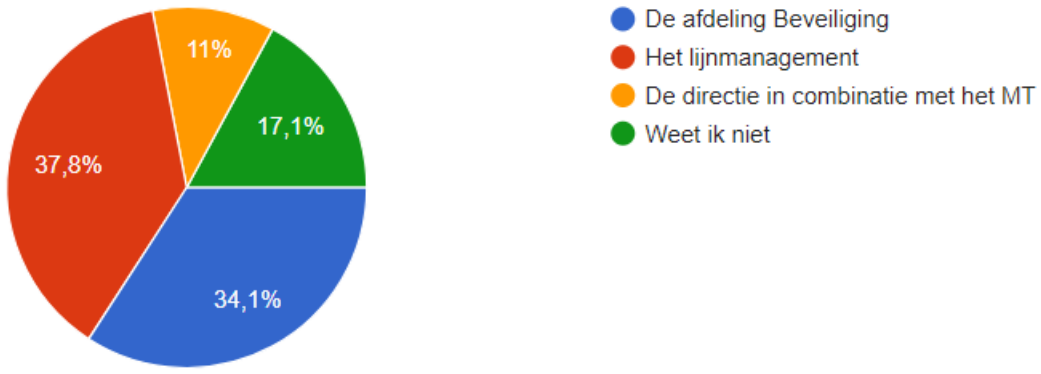
lijnmanager is verantwoordelijk voor het treffen van maatregelen voor de integrale beveiliging van het te beschermen belang op basis van risicomanagement."

Aanvullend wordt in de Baseline Informatiebeveiliging Rijksdienst (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2012) de verantwoordelijkheid van het management als volgt benoemd;

- 6.1.3.1. "Elke lijnmanager is verantwoordelijk voor de integrale beveiliging van zijn of haar dienstonderdeel. "
- 8.2.1.2 "Het lijnmanagement bevordert dat rijksambtenaren, ingehuurd personeel en (waar van toepassing) externe gebruikers van interne systemen algemene beveiligingsaspecten toepassen in hun gedrag en handelingen overeenkomstig vastgesteld beleid."

Volgens de Rijksbeleid en BIR is de manager binnen de Rijksdienst verantwoordelijk voor de uitvoering van het beleid op de afdeling. Conform het gevoerde three-lines of defence model[1], vormt de afdeling Beveiliging met advisering en beleid de tweede lijn en is de derde lijn de audit/control op dit proces.

Uit de interviews blijkt dat binnen de Rijksdienst het van afdeling tot afdeling kan verschillen hoe actief de eerste lijn wordt ervaren op het uitdragen van het informatiebeveiligingsbeleid op de afdeling. Het gevolg is dat de geïnterviewde informatiebeveiligingsfunctionarissen op verschillende wijze hun rol ervaren en inrichten, van het minimaal bijhouden van de status van de BIR maatregelen, tot het actief een verbindende rol vervullen en bijdragen aan het invullen van maatregelen op een afdeling.



Figuur 10 Verantwoordelijk voor uitvoering informatiebeveiligingsbeleid

Dit verdeelde beeld komt terug in de online survey. Op de vraag, wie is binnen uw organisatie en/of afdelingen verantwoordelijk voor het uitvoeren en controleren van het informatiebeveiligingsbeleid? Antwoordt 38% van de deelnemers dat het lijnmanagement verantwoordelijk is en 11% acht het management en directie gezamenlijk verantwoordelijk. Een derde (34%) noemt de afdeling Beveiliging en 17% weet het niet.

Aan de deelnemers van de survey is ook gevraagd of het beveiligingsbeleid actief uitgedragen / verspreid wordt binnen de afdeling en organisatie? Hierbij is hetzelfde verdeelde beeld waarneembaar, Ja zegt 44%, Nee 48%. 8% weet het niet.

[1] https://www.isaca.org/Journal/archives/2011/Volume-5/Pages/The-Three-Lines-of-Defence-Related-to-Risk-Governance.aspx

Opvallend detail is dat driekwart van de managers (12) zich zelf als verantwoordelijke voor het informatiebeveiligingsbeleid noemt, drie managers noemen de afdeling beveiliging verantwoordelijk en één noemt de directie in combinatie met het managementteam. Op de vraag of het beveiligingsbeleid actief wordt uitgedragen en verspreid binnen de afdeling en organisatie, antwoorden 4 van de 16 managers negatief. Hierbij steken twee managers de hand in eigen boezem, door zich wel verantwoordelijk te noemen, maar tevens aan te geven onvoldoende actief beleid te voeren op de afdeling.

Conclusie is dat de verantwoordelijkheid voor het uitvoeren van het informatiebeveiligingsbeleid onvoldoende bekend is binnen de Rijksdienst en binnen drie afdelingen niet conform het informatiebeveiligingsbeleid bij de manager belegd.

5.2.3. Fysieke toegangsbeveiliging

Zonering, toegangscontrole, toegangspassen en registratie

In het Vaststellingsbesluit Rijkshuisvestingsstelsel kantoren (Rijksoverheid, 2016) wordt als norm voor beveiliging van kantoren het Normenkader Beveiliging Rijkskantoren gehanteerd. Het is een referentiekader en baseline van de beveiligingsmaatregelen voor rijkskantoren met als doel de beveiliging voor rijkskantoren kwalitatief en uniform te borgen en te verantwoorden.

In het besluit worden drie zones en een openbaar gebied gedefinieerd:

- Openbaar gebied,
- Publiekszone,
- Standaard werkgebied,
- Bijzonder werkgebied.

Elk gebied kent haar eigen beveiligingsmaatregelen. Uitgaande van een standaard werkgebied, beschrijft de Baseline Informatiebeveiliging Rijksoverheid (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2012) de volgende eisen;

9.1.1. Fysieke beveiliging van de omgeving: “Er behoren toegangsbeveiligingen (barrières zoals muren, toegangspoorten met kaartsloten of een bemande receptie) te worden aangebracht om ruimten te beschermen waar zich informatie en ICT-voorzieningen bevinden.”

9.1.2. Fysieke toegangsbeveiliging: “Beveiligde zones behoren te worden beschermd door geschikte toegangsbeveiliging, om te bewerkstelligen dat alleen bevoegd personeel wordt toegelaten.”

1. Toegang tot gebouwen of beveiligingszones is alleen mogelijk na autorisatie daartoe.
2. De beveiligingszones en toegangsbeveiliging daarvan zijn ingericht conform het Kader Rijkstoegangsbeleid.
3. In gebouwen met serverruimtes houdt beveiligingspersoneel toezicht op de toegang. Hiervan wordt een registratie bijhouden.
4. De kwaliteit van toegangsmiddelen (deuren, sleutels, sloten, toegangspassen) is afgestemd op de zonering.
5. De uitgifte van toegangsmiddelen wordt geregistreerd.

Bezoekers aan een Rijksdienst dienen als zij van de publieke zone toegang willen tot een standaard werkgebied zich te legitimeren, de uitgifte van toegangspassen vindt gecoördineerd op één centrale plek bij de ingang plaats. De toegang tot de werkgebieden is afgeschermd met toegangsdeuren, welke alleen met geautoriseerde medewerkerspassen toegankelijk zijn.

De Rijksdienst heeft op intranet haar huisregels beschreven, hierin is onder andere een bezoekersregeling opgenomen, waarbij verplichtingen zoals het aanmelden en registreren van bezoek, het zichtbaar dragen van bezoekers- en medewerkerspassen en het begeleiden c.q. toezicht houden tijdens het bezoek is geregeld. Geconcludeerd kan worden dat op alle fysieke maatregelen uit het literatuuronderzoek informatiebeveiligingsbeleid aanwezig is.

5.2.4. Informatiebeveiliging

Informatieclassificatie, informatieverwerking en vernietiging

De Baseline Informatiebeveiliging Rijksoverheid (BIR) (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2012) beschrijft het minimale aan te treffen maatregelen waaraan een Rijksdienst moet voldoen. In hoofdstuk 15 van de BIR worden eisen aan de naleving van wettelijke voorschriften beschreven, hierbij zijn verwijzingen opgenomen met betrekking tot intellectuele eigendomsrechten, bescherming van bedrijfsdocumenten, bescherming van gegevens en geheimhouding van persoonsgegevens (Rijksoverheid, 2017), voorkomen van misbruik van IT voorzieningen en voorschriften voor het gebruik van cryptografische middelen.

Voor vertrouwelijke of bijzondere informatie binnen de Rijksoverheid gelden aanvullende eisen, het Voorschrift Informatie Rijksdienst – Bijzondere Informatie (VIR-BI) (Rijksoverheid, 2013) kent de volgende vier classificaties met betrekking tot informatie:

- Departementaal – vertrouwelijk
- Staatsgeheim – confidentieel
- Staatsgeheim –geheim
- Staatgeheim – Zeer geheim

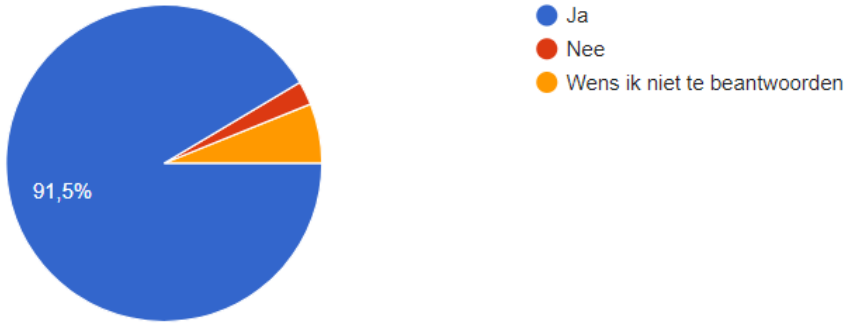
Afhankelijk van de rubricering van de informatie geldt een bepaald regime van additionele maatregelen met betrekking tot de behandeling van informatie. Hierbij worden aanvullende eisen gesteld aan a) medewerkers die in aanraking komen met bijzondere informatie, b) fysieke en omgevingsbeveiliging met betrekking tot ruimten waar zich bijzondere informatie bevindt, c) logische toegangsbeveiliging en beschikbaarheidseisen tot ICT-voorzieningen waarin zich bijzondere informatie bevindt en d) de verzending van gerubriceerde informatie.

Daarnaast worden er met betrekking tot het verwijderen van vertrouwelijke gegevens en/of documenten eisen gesteld in de Archiefwet; “De overheidsorganen zijn verplicht de onder hen berustende archiefbescheiden in goede, geordende en toegankelijke staat te brengen en te bewaren, alsmede zorg te dragen voor de vernietiging van de daarvoor in aanmerking komende archiefbescheiden” (Rijksoverheid, 2015).

Met betrekking tot het veilig verwijderen of het hergebruiken van informatiedragers worden in paragraaf 9.2.6. van de BIR specifieke tooling en richtlijnen beschreven.

Binnen de Rijksdienst is het werken of het in aanraking komen met vertrouwelijke informatie gemeen goed. Onder de respondenten van de survey heeft 71 % aangegeven toegang te hebben tot vertrouwelijke informatie vanuit zijn/haar functie. Een kwart (24%) van de respondenten heeft geen toegang tot vertrouwelijke informatie en 5% wenst deze vraag niet te beantwoorden.

Volgens de geïnterviewde medewerkers ligt het werken met vertrouwelijke informatie besloten in de aard van de Rijksdienst. Het bewustzijn over het werken met vertrouwelijke informatie is breed verspreid onder zowel leidinggevenden als medewerkers. Op de vraag, bent u in staat aan te geven welke informatie vertrouwelijk is op uw afdeling? Beantwoordt ruim 91% van deelnemers aan de survey deze vraag met Ja, 6% wenst deze niet te beantwoorden en 2% met Nee. Overigens is het bewustzijn op beleid rondom informatieclassificatie met 37% beduidend lager.



Figuur 11 Percentage medewerkers dat aangeeft in staat te zijn om vertrouwelijk informatie op afdeling te kunnen duiden.

Uit de interviews komt terug dat voor het vernietigen van papieren vertrouwelijke informatie er een werkprocedure aanwezig is, waarbij deze informatie in aparte containers/bakken wordt ingezameld om te worden vernietigd. Voor digitale informatiedragers verloopt dit proces van vernietigen via de afdeling systeembeheer, die zorgdraagt voor het vernietiging conform de eisen. Bij digitaal opgeslagen informatie is men zich bewust dat de gegevens met rechten zijn afgeschermd, dat informatie niet zomaar kan worden verwijderd en dat hiervoor wettelijke archiverings- en schoningstermijnen bestaan.

Binnen de Rijksdienst zijn er tal van informatiesystemen, het is ondoenlijk binnen de scope van dit onderzoek deze informatiesystemen afzonderlijk te analyseren. Generiek kan worden gesteld dat er conform de BIR en de VIR-BI er een invulling is van bovenstaande wettelijke verplichtingen en het merendeel (91%) van de medewerkers in de praktijk op de hoogte is van dit regime, met de kanttekening dat 63% van de medewerkers het beleid rondom informatieclassificatie zelf niet kent.

Email filtering, anti-virus, anti-phishing maatregelen

In de Baseline Informatiebeveiliging Rijksoverheid (BIR) (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2012) worden onder paragraaf 10.4. Bescherming tegen virussen en “mobile code” de volgende maatregelen voorgeschreven;

- Bij het openen van bestanden worden deze geautomatiseerd gecontroleerd op virussen, trojans en andere malware. De update voor de detectiedefinities vindt frequent, minimaal één keer per dag, automatisch plaats.
- Inkomende en uitgaande e-mails worden gecontroleerd op virussen, trojans en andere malware. De update voor de detectiedefinities vindt frequent, minimaal één keer per dag, (automatisch) plaats.
- In verschillende schakels van een keten binnen de infrastructuur van een organisatie wordt bij voorkeur antivirus programmatuur van verschillende leveranciers toegepast.
- Er zijn maatregelen om verspreiding van virussen tegen te gaan en daarmee schade te beperken (bijv. quarantaine en compartimentering).

- Er zijn continuïteitsplannen voor herstel na aanvallen met virussen waarin minimaal maatregelen voor back-ups en herstel van gegevens en programmatuur zijn beschreven.

Het bewustzijn onder medewerkers over deze anti-virus, anti-phishing maatregelen ligt op 72%. Een relatief hoge score gezien het feit dat het minder zichtbare maatregelen zijn, waarbij de controle op virussen, trojans en andere malware voor de gebruikers op de achtergrond plaats vindt.

Uit de interviews met ook IT specialisten blijkt het monitoren op mogelijke uitbraken of verspreiding van virussen een ingeregeld continu proces. Zo werd door actief ingrijpen tijdens de Rijksbrede phishingcampagne, ook deze website in eerste instantie binnen de Rijksdienst proactief geblokkeerd. Geconcludeerd kan worden dat deze maatregelen conform beleid zijn ingericht en bij het merendeel (72%) van de medewerkers bekend is.

Clean desk, locken van de computer, wachtwoordmanagement

Rondom de werkplek gelden tal van veiligheidsvoorschriften om het lekken van vertrouwelijke informatie te voorkomen. In de Baseline Informatiebeveiliging Rijksoverheid (BIR) (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2012) worden onder paragraaf 11.3 de volgende eisen c.q. verantwoordelijkheden aan gebruikers gesteld;

11.3.1. Gebruik van wachtwoorden

Gebruikers behoren goede beveiligingsgewoontes in acht te nemen bij het kiezen en gebruiken van wachtwoorden. Aan de gebruikers is een set gedragsregels aangereikt met daarin minimaal het volgende:

- Wachtwoorden worden niet opgeschreven.
- Gebruikers delen hun wachtwoord nooit met anderen.
- Een wachtwoord wordt onmiddellijk gewijzigd indien het vermoeden bestaat dat het bekend is geworden aan een derde.
- Wachtwoorden worden niet gebruikt in automatische inlogprocedures (bijv. opgeslagen onder een functietoets of in een macro).

11.3.2. Onbeheerde gebruikersapparatuur

Gebruikers behoren te bewerkstelligen dat onbeheerde apparatuur passend is beschermd. De gebruiker vergrendelt de werkplek tijdens afwezigheid.

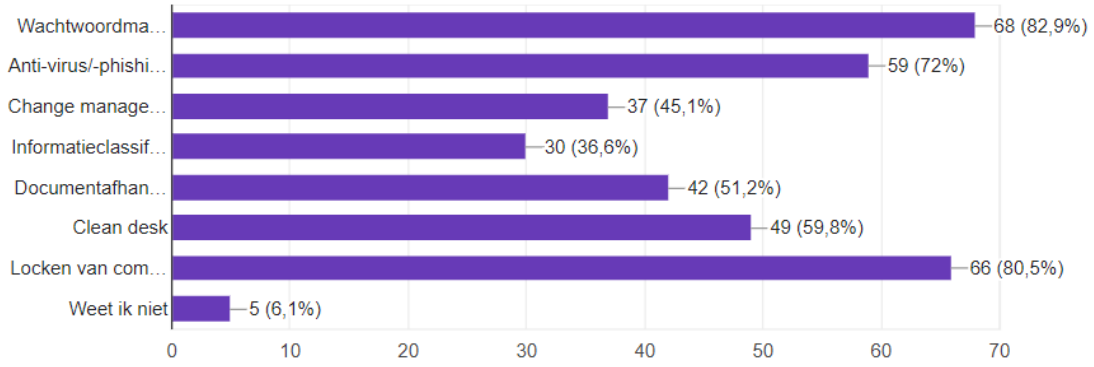
11.3.3. Clear desk en clear screen

Er behoort een ‘clear desk’-beleid voor papier en verwijderbare opslagmedia en een ‘clear screen’-beleid voor ICT-voorzieningen te worden ingesteld.

1. In het clear desk beleid staat minimaal dat de gebruiker geen vertrouwelijke informatie op het bureau mag laten liggen. Deze informatie moet altijd worden opgeborgen in een afsluitbare opbergmogelijkheid (kast, locker, bureau of kamer).
2. Bij afdrukken van gevoelige informatie wordt, wanneer mogelijk, gebruik gemaakt van de functie “beveiligd afdrukken” (pincode verificatie).
3. Schermbeveiligingsprogrammatuur (een screensaver) maakt na een periode van inactiviteit van maximaal 15 minuten alle informatie op het beeldscherm onleesbaar en ontoegankelijk.
4. Toegangsbeveiliging lock wordt automatisch geactiveerd bij het verwijderen van een token (indien aanwezig).

Op het intranet van de Rijksdienst staan de voorschriften met betrekking tot het gebruik van wachtwoorden, vergrendelen van de computer en clear desk, clear screen gepubliceerd.

De awareness van medewerkers op deze maatregelen varieert van 83% met betrekking tot wachtwoord gebruik en het locken van de computer (81%), tot de clean desk procedure met slechts 60% bekendheid.



Figuur 12 Awareness op aspecten van het informatiebeveiligingsbeleid

De relatief lage score op clean desk ligt mogelijkerwijs aan de heersende veiligheidscultuur en de gewoontes van een afdeling. Volgens een geïnterviewde zou de boodschap hetzelfde moeten zijn, maar is de waarde die er aan wordt gehecht niet op alle afdelingen hetzelfde.

5.2.5. Beveiligingsproces

Incidentafhandeling

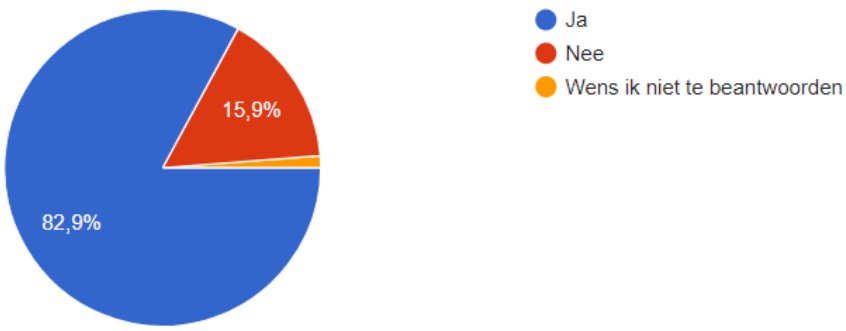
Volgens de onderzochte literatuur naar social engineering (Van der Laan, 2016) en informatiebeveiliging (Spijker, 2016) is een incidentproces essentieel in het kunnen vaststellen van de aard de omvang van een (social engineerings-)aanval, opdat de meest passende opvolging gegeven kan worden. Zowel qua incidentresponse met correctieve maatregelen, als later met het aanbrengen van aanvullende preventieve maatregelen.

In de Baseline Informatiebeveiliging Rijksoverheid (BIR) (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2012) wordt in hoofdstuk 13 het beheerproces van informatiebeveiligings-incidenten beschreven. Hierbinnen is aandacht voor de volgende punten;

- Rapportage van informatiebeveiligingsgebeurtenissen
- Rapportage van zwakke plekken in de beveiliging
- Verantwoordelijkheden en procedures
- Leren van informatiebeveiligingsincidenten
- Verzamelen van bewijsmateriaal.

Op het intranet van de Rijksdienst staat beschreven hoe en wanneer een beveiligingsincident gemeld kan worden. Uit de interviews blijkt dat het over het algemeen medewerkers zelf melding maken van incidenten bij de afdeling Beveiliging, ook komt voor dat eerst de leidinggevende wordt geraadpleegd, alvorens een melding te maken van een incident op de afdeling. Maandelijks wordt door de afdeling Beveiliging van alle incidenten een incidentrapportage opgesteld, op basis hiervan worden eventuele vervolgacties uitgezet.

Op de vraag in de online survey, bent u bekend hoe u dient om te gaan met een beveiligingsincident binnen uw afdeling / organisatie? Antwoordt 83% van de medewerkers Ja, 16% Nee en 1% wenst deze vraag niet te beantwoorden.



Figuur 13 Bekendheid van incidentafhandelingsproces

Geconcludeerd kan worden dat er een proces van Incidentafhandeling aanwezig is en 83% van de medewerkers op de hoogte is van dit beleid.

Controle, Auditing

In de Baseline Informatiebeveiliging Rijksoverheid (BIR) (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2012) worden de volgende eisen gesteld aan het auditen en de controle op naleving van het beleid;

Beoordeling van het informatiebeveiligingsbeleid

- Het informatiebeveiligingsbeleid wordt minimaal één keer in de drie jaar geëvalueerd (door een onafhankelijke deskundige) en desgewenst bijgesteld.
- Over het functioneren van de informatiebeveiliging wordt, conform de Planning & Control-cyclus, jaarlijks gerapporteerd aan het lijnmanagement.

Naleving van beveiligingsbeleid en normen

- Het lijnmanagement is verantwoordelijk voor uitvoering en beveiligingsprocedures en toetsing daarop. In de Planning & Control-cyclus wordt gerapporteerd over informatiebeveiliging aan de hand van het in control statement.
- Controle op technische naleving, informatiesystemen worden regelmatig gecontroleerd op naleving van beveiligingsnormen. Dit kan door bijv. kwetsbaarheidsanalyses en penetratietesten.

Uit de interviews blijkt dat één keer per jaar de balans wordt opgemaakt van de status van de verschillende afdelingsspecifieke BIR sheets. Hieruit wordt een overal beeld op de voortgang van het implementeren van maatregelen binnen de Rijksdienst opgemaakt, op basis waarvan de jaarlijkse in control statement kan worden afgegeven.

Het auditen van het beleid kent niet overal een driejarig cyclus, sommige afdelingen kennen een jaarlijkse of tweejaarlijkse audit i.v.m. gecertificeerde dienstverlening welke hogere (controle-)eisen stellen aan werkprocessen.

Geconcludeerd kan worden dat beleid op dit punt bekend is en nageleefd wordt.

5.3. Social Engineering

5.3.1. Awareness

Begrip social engineering

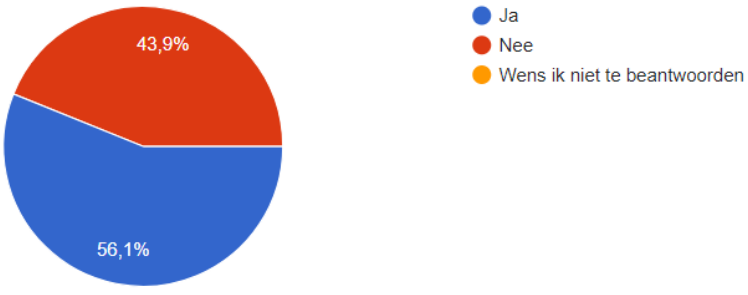
De deelnemers aan de interviews kregen zowel de definitie (A) van social engineering zoals deze werd gehanteerd in het eerdere onderzoek (Van der Laan, 2016) als de definitie (B) in het kader van dit herhalingsonderzoek te lezen. Hen is gevraagd of zij zich konden vinden in beide definities, dan wel er een voorkeur bestond, of dat er mogelijk aanvullende punten zijn te benoemen.

Definitie A: *"Social engineering is een set van methoden waarmee het gedrag van een individu of groep individuen wordt gemanipuleerd zodanig dat deze toegang verleent tot bepaalde informatie, met als doel deze informatie te gebruiken om de slachtoffers uit te buiten. Deze techniek maakt gebruik van de intrinsieke aard van de mensheid om slachtoffers uit te buiten, om gevoelige informatie te verkrijgen en hen te manipuleren en van het overtuigen van mensen om deze informatie te onthullen door het inzetten van uitzonderlijk goede communicatieve vaardigheden. Boven alles maakt social engineering gebruik van de zwakste schakel in de beveiliging: de menselijke factor* (Van der Laan, 2016) ."

Definitie B: *"Social engineering is een aanvalstechniek waarbij de aanvaller probeert informatiesystemen te hacken door de zwakste schakel in de informatiebeveiliging, namelijk de mens, te manipuleren. Hierbij wordt misbruik gemaakt van menselijke eigenschappen als nieuwsgierigheid, vertrouwen en hebzucht, om daarmee het slachtoffer een bepaalde handeling uit te laten voeren of vertrouwelijke informatie te verkrijgen, waardoor de aanvaller dichter bij het aan te vallen informatiesysteem kan komen."*

De rode draad die uit de interviews is te halen, is dat beide definities samen de lading dekken en in de kern de mens als zwakste schakel typeren, die kan worden verleid tot het ontlokken van informatie. Definitie A wordt als breder omschreven ervaren, waarbij definitie B specifiek spreekt over informatiesystemen en aanvalstechnieken. Daarbij wordt opgemerkt dat beide definities niet vermelden wat de methoden en kanalen zijn die worden gebruikt en daarmee het begrip minder tastbaar maakt.

De deelnemers aan de online survey kregen voorafgaand aan de vragen m.b.t. social engineering, de volgende verkorte toelichting op de term social engineering te lezen; *"Social Engineering is een verzamelnaam van aanvalstactieken en methoden, gericht op het manipuleren van medewerkers om zo toegang te verkrijgen tot vertrouwelijke bedrijfsinformatie."*



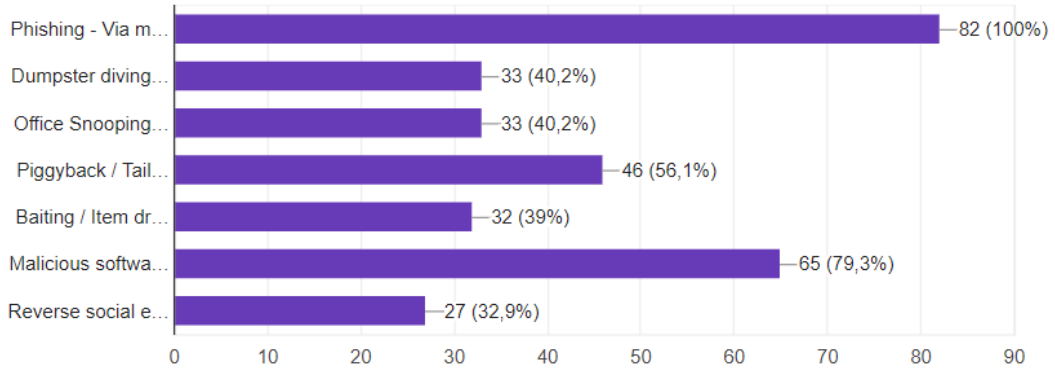
Figuur 14 Bekend met het begrip social engineering

Vervolgens is aan de medewerkers gevraagd of deze bekend zijn met het begrip social engineering, hierop antwoorden 46 deelnemers Ja (56%) en 36 deelnemers Nee (44%).

Geconcludeerd kan worden dat op basis van de interviews het komen tot een eenduidige begrip van social engineering nog niet zo gemakkelijk is en zeker nog aanvullende duiding vraagt. Daarnaast laat de online survey zien dat het begrip social engineering niet zo breed bekend is onder medewerkers, iets meer dan de helft (56%) geeft aan bekend te zijn met het begrip social engineering.

Aanvalsmethoden

De deelnemers aan de online survey is gevraagd met welke van de genoemde social engineeringsaanvallen men bekend is. Per aanvalstechniek is een korte toelichting op de Engelstalige termen gegeven, zodat de respondenten die bijvoorbeeld wel bekend zijn met het gevaar van meelopen ook in staat werden gesteld Tailgating te benoemen.



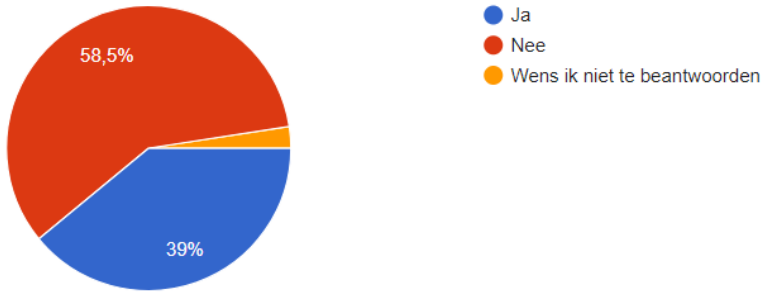
Figuur 15 Bekendheid van social engineering aanvalstechnieken

Op de term phishing na, geeft het merendeel van de medewerkers (60 ~ 67%) aan de genoemde technieken niet te kennen. Malicious software wordt door 79% van de medewerkers herkend, echter is dit een mogelijk middel bij een social engineeringsaanval en geen aanvalsmethode.

Geconcludeerd kan worden dat de term phishing onder alle medewerkers (100%) bekend is en daarmee duidelijk een bekender begrip is dan social engineering zelf. Kennis over andere methoden is slechts onder 33% ~ 40% van de medewerkers bekend.

Werkwijzen, motieven en misbruik

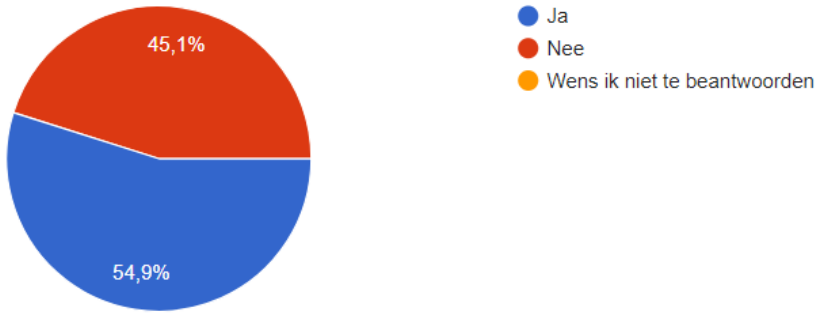
Op de vraag, Kunt u beschrijven hoe een social engineeringsaanval wordt uitgevoerd? Antwoordt 59% Nee, 39 Ja en 2% wenst deze vraag niet te beantwoorden.



Figuur 16 Bekend met werkwijze van social engineers

Ook de meeste deelnemers aan de interviews vonden, ondanks de informatiebeveiligings-achtergrond, het lastig om een social engineeringsaanval te beschrijven. Het feit dat een social engineeringsaanval veelal niet op zich zelf staat, maar een poging is binnen een reeks van meerdere verschillende aanvalsvormen, blijkt weinig bekend. De fasering - voorbereiding, manipulatie, exploitatie en uitvoering - uit de social engineering aanvalscyclus, zoals ook weergegeven in het referentieraamwerk, was geheel niet bekend.

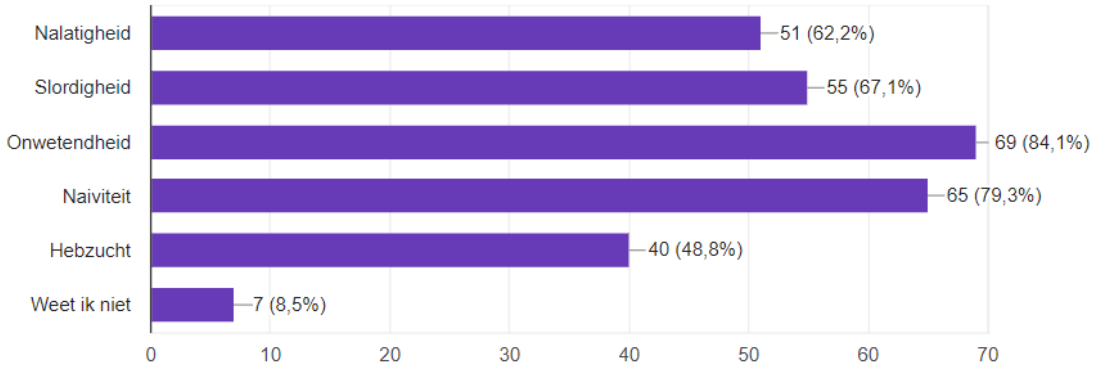
In de online survey is ook gevraagd naar het bekend zijn met de meest voorkomende motieven van social engineers. Hierop antwoordt 55% van de deelnemers Ja, 45% Nee .



Figuur 17 Bekend met motieven van social engineers

De geïnterviewde medewerkers noemden in eerste instantie voornamelijk geld als motief. Gevraagd naar de motieven om de Rijksoverheid aan te vallen, worden veelal vertrouwelijke dossiers en/of persoonsinformatie genoemd.

Gevraagd naar welke menselijke aspecten een social engineer misbruik maakt. Antwoordt 84% van de deelnemers aan de online survey, Onwetendheid en 79% Naïviteit.



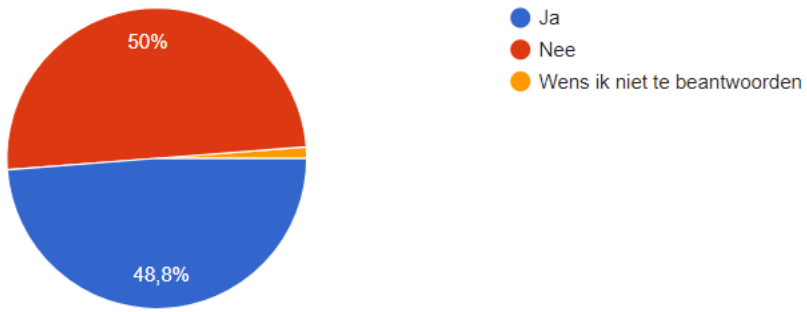
Figuur 18 Genoemde aspecten van misbruik

Geconcludeerd kan worden dat het merendeel van de medewerkers onvoldoende bekend is met de werkwijzen van social engineers. Bekeken naar de aspecten van misbruik, zou de focus van het beleid op social engineering binnen de Rijksoverheid moeten liggen op het wegnemen van de onwetendheid en naïviteit van medewerkers.

5.3.2. Potentieel doelwit

Slachtoffer

In welke mate is de Rijksoverheid zelf het doelwit van social engineeringsaanvallen. In de online survey is onderzocht of medewerkers denken in de afgelopen 6 maanden het slachtoffer te zijn geweest van een social engineeringaanval.



Figuur 19 Percentage deelnemers potentieel doelwit afgelopen 6 maanden

49% van de deelnemers geeft aan afgelopen 6 maanden doelwit te zijn geweest van een social engineeringaanval, 50% Niet of wenst deze vraag niet te beantwoorden (1%).

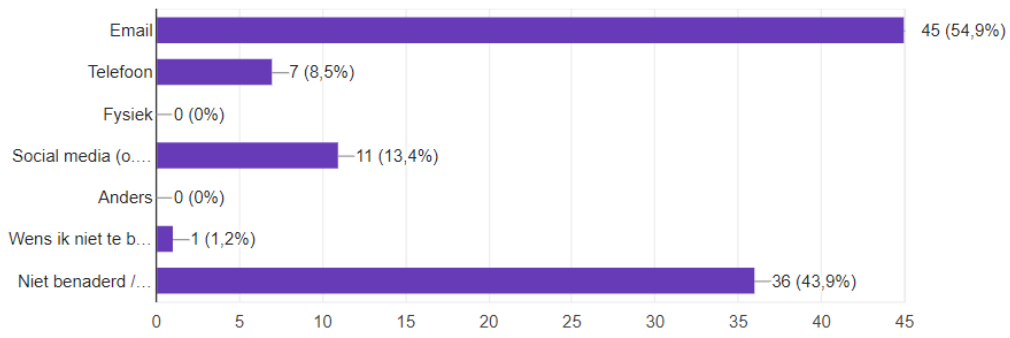
Onder de geïnterviewden is ook gevraagd of er recent incidenten zijn geweest rondom social engineeringsaanvallen. Geen van de informatiebeveiligingsfunctionarissen heeft hierop bevestigend beantwoord.

Logischerwijs zou hetzelfde beeld onder medewerkers als onder informatiebeveiligings-functionarissen zichtbaar moeten zijn geweest. Mogelijk zijn informatiebeveiligingsfunctionarissen terughoudend in de beantwoording geweest of wordt een poging niet tot als incident beschouwd. Nader onderzoek zal moeten uitwijzen waarom dit verschil in waarneming, 0 vs. 50%, zo groot is.

Communicatiekanalen

Vervolgens is de vraag gesteld via welke kanalen de pogingen werden ondernomen. Hierop geeft 55% van de deelnemers aan de online survey via email te zijn benaderd, ruim 13% via social media en bijna 9% telefonisch.

Fysieke of andere wijze van benaderen zijn niet genoemd.



Figuur 20 Social engineeringskanalen

Van de benaderde medewerkers, geven 7 deelnemers (8%) aan via twee kanalen te zijn benaderd, 5 deelnemers (6%) geven aan via drie kanalen te zijn benaderd de afgelopen 6 maanden.

Kans van slagen

Op de vraag hoe groot de kans wordt geacht dat organisatie kwetsbaar is voor bepaalde social engineeringsaanvallen, is in de online survey als volgt beantwoord;

- De kans op het slagen van een phishing aanval wordt door 72% van de medewerkers geschat op middel of groot.
- De kans van slagen dat iemand het gebouw van de Rijksdienst binnenkomt zonder autorisatie, wordt door 61% van de medewerkers geschat op middel of groot.
- De kans van slagen dat een medewerker een gevonden USB stick gaat bekijken, wordt door 63% van de medewerkers geschat op middel of groot.

Uit de interviews blijkt dat de effectieve kans van slagen in het geval van item dropping met een USB stick of cdrom, gezien de reeds getroffen maatregelen, nihil zal zijn. De werkplekken beschikken niet meer over een USB of cdrom ingang.

Geschatte kans van slagen	Klein	Middel	Groot
Phishing	28%	59%	13%
Tailgating	39%	39%	22%
Item dropping	37%	49%	14%

Tabel 3 Geschatte kans van slagen social engineersaanval

Geconcludeerd kan worden dat de helft van de medewerkers (49%) van de Rijksoverheid de afgelopen zes maanden te maken heeft gehad met social engineeringsaanvallen. 14% van de medewerkers is in deze periode via meerdere kanalen benaderd. De “populairste” wijze van benaderen van slachtoffers is via email (55%). De kans van slagen van een phishing aanval wordt door 72% van de medewerkers op middel of groot geschat.

Geconcludeerd kan worden dat de informatiebeveiligingsfunctionarissen hiervan niet of onvoldoende op de hoogte zijn. De vraag rijst of deze signalen wel als incidenten worden gezien en gemeld door de medewerkers, dan wel er onvoldoende opvolging is op deze signalen.

5.4. Samenvatting resultaten

Informatiebeveiligingsbeleid

Samenvatting van de resultaten van het onderzoek op het aanwezige informatiebeveiligingsbeleid en het percentage van de medewerkers dat op de hoogte is van dit beleid.

Nr	Maatregel	Beleid aanwezig	Awareness beleid
Personele beveiliging			
1	Screening CV, referenties	Ja	90%
2	Arbeidsvoorwaarden / VOG	Ja	93%
3	Management buy-in	Ja	44%*
4	Opleiding en bewustwording	Ja	16%/84%**
5	Disciplinaire maatregelen	Ja	Niet gevraagd
6	Retourneren bedrijfsmiddelen	Ja	73%
7	Blokkering toegangsrechten	Ja	76%
Toegangsbeveiliging * **			
8	Beveiligingscamera's	Ja	Niet gevraagd
9	Aanmeldprocedure bezoekers	Ja	Niet gevraagd
10	Bezoekerspasjes	Ja	Niet gevraagd
11	Foto-identificatiepasjes	Ja	Niet gevraagd
12	Toegangsdeuren	Ja	Niet gevraagd
Informatiebeveiliging			
13	Informatie classificatie	Ja	37%
14	Documentafhandeling/-vernietiging	Ja	51%
15	Beperken publieke informatie	Ja	92% ****
16	Wachtwoord management	Ja	83%
17	Locken van computer	Ja	81%
18	Clean desk	Ja	60%
19	Antivirus / antiphishing	Ja	72%
20	E-mailfiltering	Ja	Niet gevraagd
Beveiligingsproces			
21	Incident afhandeling	Ja	83%
22	Audit beleid / audit controles	Ja	Niet gevraagd

Tabel 4 Overzicht beleid en awareness

*Bij management buy-in is getoetst of dit beleid werd ervaren op de afdeling, dan wel binnen de organisatie.

** Bij opleiding en bewustwording is gevraagd of medewerkers een opleiding m.b.t. informatiebeveiliging of social engineering hebben gevolgd en of zij deze zouden willen volgen.

*** Door een fout in de online survey, zijn de fysieke maatregelen niet getoetst op awareness onder medewerkers.

**** Bij beperken publieke informatie is getoetst of medewerkers in staat zijn aan te geven wat vertrouwelijk informatie is.

Social engineering

Samenvatting van de resultaten van het onderzoek naar kennis over social engineering en mogelijke aanvalspogingen binnen de Rijksoverheid, in vergelijk tot het in 2016 uitgevoerde onderzoek (Van der Laan, 2016). De groene arcering benadrukt de positieve uitkomst m.b.t. de gemiddelde awareness binnen de onderzochte Rijksorganisaties, de rood/oranje arcering duidt op een potentieel risico in relatie tot social engineeringsaanvallen.

	2017		2016
Awareness			
Begrip social engineering	56%		54%
Aanvalsverloop	39%		39%
Motieven	55%		53%
Awareness aanvalstechnieken/methoden			
Phishing	100%		100%
Dumpster diving	40%		18%
Office snooping	40%		14%
Tailgating	56%		18%
Baiting / Item dropping	39%		Niet gevraagd
Malicious software	79% *		61%
Reverse social engineering	33%		4%
Genoemde aspecten van misbruik			
Nalatigheid	62%		57%
Slordigheid	67%		68%
Onwetendheid	84%		71%
Naïviteit	79%		71%
Hebzucht	49%		46%
Doelwit afgelopen 6 maanden	49%		61%
Aanvalskanalen			
Email	55%		57%
Telefoon	9%		7%
Fysiek	0%		0%
Social media	13%		7%
Anders	0%		0%
Geschatte kans van slagen	Klein	Middel	Groot
Phishing	28%	59%	13%
Tailgating	39%	39%	22%
Item dropping	37%	49%	14%

Tabel 5 Overzicht resultaten social engineering

* Malicious software wordt door 79% van de medewerkers herkend, echter is dit een middel bij een social engineeringsaanval en geen methode.

6. Conclusies en aanbevelingen

In dit hoofdstuk worden met de resultaten van het onderzoek (Hoofdstuk 5), conclusies getrokken aan de hand van de opgestelde onderzoeksvragen (paragraaf 1.5). In de paragraven 6.1 tot en met 6.7 worden de deelvragen rondom de onderwerpen informatiebeveiligingsbeleid en social engineering behandeld, en aansluitend de onderzoeksvragen en hypothesen in paragraaf 6.8. In paragraaf 6.9 volgt een eindconclusie en in paragraaf 6.10 aanbevelingen voor mogelijk vervolgonderzoek en praktische invulling.

6.1. Informatiebeveiligingsbeleid

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

Er zijn een aantal Rijksbrede wettelijke regelingen en kaders die het proces van informatiebeveiliging binnen een Rijksoverheidsorganisatie bepalen en ondersteunen;

- Beveiligingsvoorschrift Rijksdienst (BVR); (Rijksoverheid, 2013)
- Voorschrift Informatiebeveiliging Rijksdienst (VIR); (Rijksoverheid, 2007)
- Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie (VIRBI); (Rijksoverheid, 2013)
- Archiefwet; (Rijksoverheid, 2015)
- Algemeen Rijksambtenarenreglement; (Rijksoverheid, 2017)
- Baseline Informatiebeveiliging Rijksoverheid - Tactisch Normenkader (BIR-TNK); (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2012)
- Operationele Handreiking Informatiebeveiliging (BIR-OH); (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2013)
- BIR Quick Scan; (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2014)
- BIR comply or explainprocedure; (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2014)

Het Beveiligingsvoorschrift Rijksdienst (BVR) is van toepassing op de integrale beveiliging van de Rijksdienst en geeft de verantwoordelijkheden voor de integrale beveiliging weer. Het Voorschrift Informatiebeveiliging Rijksdienst (VIR) geldt voor het gehele proces van informatievoorziening en de gehele levenscyclus van informatiesystemen. De Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie (VIRBI) is een aanvulling op het VIR regels voor de beveiliging van bijzondere (vertrouwelijke) informatie. De Archiefwet kent bepalingen rondom opslag en vernietiging van informatie. De baseline omvat een verplicht tactisch normenkader (BIR-TNK) en een ondersteunende operationele handreiking (BIR-OH) die een groot deel van het tactisch kader dekt. De BIR is gebaseerd op ISO 27001 normering. De BIR Quick Scan is bedoeld als instrument om te bepalen of de risico's voor een proces met ondersteunende systemen voldoende door de BIR worden afgedekt. De BIR comply or explainprocedure omvat een explainprocedure waarom bepaalde BIR maatregelen wel of niet zijn genomen.

Daarbij kennen Rijksdiensten veelal een eigen informatiebeveiligingsbeleid dat aanhaakt op het hiervoor benoemde bredere Rijksbeleid en invulling geeft aan context specifieke bepalingen en maatregelen. Binnen deze onderzochte Rijksdienst zijn deze bepalingen ingevuld met een vastgesteld Handboek Beveiliging en gepubliceerde maatregelen op het intranet.

6.2. Awareness informatiebeveiligingsbeleid

Deelvraag 2: Zijn de medewerkers binnen de Rijksoverheid inhoudelijk bekend met deze informatiebeveiligingsdocumenten?

De online survey laat zien dat 72% van de medewerkers zegt inhoudelijk bekend te zijn met de Baseline Informatiebeveiliging Rijk (BIR). Opmerkelijk is dat slechts een kwart (27%) van de medewerkers de ISO 27001/2 noemt, terwijl de BIR deze ISO norm als basis heeft. 21% van de medewerkers geeft aan met géén van de documenten bekend te zijn.

Uit de gevoerde interviews, met specifiek op informatiebeveiligingskennis geselecteerde medewerkers (IBF-rol vervullen), is de kennis over het gevoerde informatiebeveiligingsbeleid onder alle deelnemers bekend (100%). Meest genoemde documenten zijn de Baseline Informatiebeveiliging Rijk (BIR), het Handboek Beveiliging waarin organisatie specifiek beleid is beschreven en tal van huisregels en genomen maatregelen die voortvloeien uit de BIR. Een enkeling noemt daarbij ook de VIR-BI, het Voorschrift Informatie Rijksdienst – Bijzondere Informatie, waarin afhankelijk van de aard van de informatie er additionele eisen worden gesteld.

Binnen deze Rijksdienst ligt de kennis over informatiebeveiligingsdocumenten met een score van 72%, in vergelijk met de 46% van het in 2016 uitgevoerde onderzoek, beduidend hoger. Mogelijk ligt dit aan de verschillende taakstellingen van de onderzochte Rijksdiensten en de mate van het in contact staan met informatieverwerkende toepassingen, die maken dat kennis over informatiebeveiliging onder medewerkers binnen deze Rijksdienst meer algemeen goed is of mogelijk ook een beroepsmatige interesse kent. Dit laatste wordt ondersteund door het feit dat 16% van de medewerkers aangeeft een opleiding m.b.t. informatiebeveiliging of social engineering te hebben gevolgd en 84% van de medewerkers aangeeft graag een opleiding of training op dit vlak zou willen volgen.

De conclusie is dat medewerkers binnen de Rijksoverheid voldoende op de hoogte zijn van het informatiebeveiligingsbeleid en de inhoudelijke documenten.

6.3. Awareness social engineering

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

In de onderstaande tabel (Tabel 6) worden de resultaten van dit onderzoek en het in 2016 uitgevoerde onderzoek (Van der Laan, 2016) m.b.t. awareness op het begrip social engineering, het aanvalsverloop, de motieven en de technieken weergegeven. De gemeten awareness over het begrip social engineering, het aanvalsverloop en de motieven is in vergelijking met het onderzoek in 2016 onveranderd te noemen.
De bekendheid met aanvalstechnieken laat in 2017 wel hogere percentages zien, dit ligt vermoedelijk aan de verkozen wijze van onderzoek. Er is per aanvalstechniek een korte toelichting op de Engelstalige termen gegeven, zodat de respondenten die bijvoorbeeld wel bekend zijn met het gevaar van meelopen ook in staat werden gesteld Tailgating te benoemen.

De bekendheid van het begrip social engineering is in vergelijking met de term phishing laag te noemen is. Ongeveer de helft van de medewerkers (56%) is bekend met het begrip en de motieven (55%). Op de term phishing na, geeft het merendeel van de medewerkers (60 ~ 67%) aan de genoemde technieken niet te kennen. Malicious software wordt door 79% van de medewerkers herkend, echter is dit een mogelijk middel bij een social engineeringsaanval en geen methode.

De conclusie is dat het merendeel van de medewerkers binnen de Rijksoverheid onvoldoende op de hoogte is van het begrip en de gebruikte methoden van social engineering.

	2017	2016
Awareness		
Begrip social engineering	56%	54%
Aanvalsverloop	39%	39%
Motieven	55%	53%
Awareness aanvalstechnieken/methoden		
Phishing	100%	100%
Dumpster diving	40%	18%
Office snooping	40%	14%
Tailgating	56%	18%
Baiting / Item dropping	39%	Niet gevraagd
Malicious software*	79%	61%
Reverse social engineering	33%	4%

Tabel 6 Overzicht awareness social engineering

* Malicious software wordt door 79% van de medewerkers herkend, echter is dit een middel bij een social engineeringsaanval en geen methode.

6.4. Informatiebeveiligingsbeleid op social engineering

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

In de onderstaande tabel (Tabel 7) is per maatregel weergegeven of er informatiebeveiligingsbeleid aanwezig is.

Nr	Maatregel	Beleid aanwezig
1	Screening CV, referenties	Ja
2	Arbeidsvoorwaarden / VOG	Ja
3	Management buy-in	Ja
4	Opleiding en bewustwording	Ja
5	Disciplinaire maatregelen	Ja
6	Retourneren bedrijfsmiddelen	Ja

7	Blokkering toegangsrechten	Ja
8	Beveiligingscamera's	Ja
9	Aanmeldprocedure bezoekers	Ja
10	Bezoekerspasjes	Ja
11	Foto-identificatiepasjes	Ja
12	Toegangsdeuren	Ja
13	Informatie classificatie	Ja
14	Documentafhandeling/-vernietiging	Ja
15	Beperken publieke informatie	Ja
16	Wachtwoord management	Ja
17	Locken van computer	Ja
18	Clean desk	Ja
19	Antivirus / antiphishing	Ja
20	E-mailfiltering	Ja
21	Incident afhandeling	Ja
22	Audit beleid / audit controles	Ja

Tabel 7 Aanwezige informatiebeveiligingsmaatregelen

De conclusie is dat op alle 22 punten er informatiebeveiligingsbeleid is of dat er onderliggende richtlijnen aanwezig zijn.

6.5. Awareness social engineeringsmaatregelen

Deelvraag 5: Wat is de mate van awareness van de medewerkers binnen de Rijksoverheid van het informatiebeveiligingsbeleid met betrekking tot social engineering?

In de onderstaande tabel (Tabel 8) is de mate van awareness van de gemiddelde medewerker (inclusief management) per maatregel weergegeven. Van de bevraagde informatiebeveiligingsmaatregelen, 11 in totaal, is de gemiddelde medewerker awareness 66%. Hierbij zijn alle 11 maatregelen gelijk gewogen.
Ter referentie, het in 2016 uitgevoerde onderzoek (Van der Laan, 2016) kende een gemiddelde awareness van 65%. Gemeten over alleen de 11 gevraagde punten in dit onderzoek moet het resultaat uit 2016 worden gecorrigeerd naar 67%.

Nr	Maatregel	Awareness beleid
1	Screening CV, referenties	90%
2	Arbeidsvoorwaarden / VOG	93%
3	Management buy-in	44%*
4	Opleiding en bewustwording	16%/84%**
5	Disciplinaire maatregelen	Niet gevraagd
6	Retourneren bedrijfsmiddelen	73%
7	Blokkering toegangsrechten	76%
8	Beveiligingscamera's	Niet gevraagd***
9	Aanmeldprocedure bezoekers	Niet gevraagd***
10	Bezoekerspasjes	Niet gevraagd***
11	Foto-identificatiepasjes	Niet gevraagd***

12	Toegangsdeuren	Niet gevraagd***
13	Informatie classificatie	37%
14	Documentafhandeling/-vernietiging	51%
15	Beperken publieke informatie	92% ****
16	Wachtwoord management	83%
17	Locken van computer	81%
18	Clean desk	60%
19	Antivirus / antiphishing	72%
20	E-mailfiltering	Niet gevraagd
21	Incident afhandeling	83%
22	Audit beleid / audit controles	Niet gevraagd

Tabel 8 Awareness informatiebeveiligingsmaatregelen

*Bij management buy-in is getoetst of dit beleid werd ervaren op de afdeling, dan wel binnen de organisatie.

** Bij opleiding en bewustwording is gevraagd of medewerkers een opleiding m.b.t. informatiebeveiliging of social engineering hebben gevolgd en of zij deze zouden willen volgen.

*** Door een fout in de online survey, zijn de fysieke maatregelen niet getoetst op awareness onder medewerkers.

**** Bij beperken publieke informatie is getoetst of medewerkers in staat zijn aan te geven wat vertrouwelijk informatie is.

6.6. Management buy-in

Deelvraag 6: Is er een verschil waarneembaar tussen het management en de medewerkers, qua bekendheid met het informatiebeveiligingsbeleid en de kennis over social engineering?

In Tabel 9 en Tabel 10 zijn respectievelijk de awareness over informatiebeveiligingsmaatregelen en social engineering weergegeven, gegroepeerd naar management en medewerkers.

Maatregel	Gemiddelde Awareness	Awareness Management	Awareness Medewerkers
Screening CV, referenties	22%	44%	17%
Arbeidsvoorwaarden / VOG	93%	100%	92%
Retourneren bedrijfsmiddelen	73%	88%	70%
Blokkering toegangsrechten	76%	94%	71%
Informatie classificatie	37%	69%	29%
Documentafhandeling/-vernietiging	51%	63%	48%
Wachtwoord management	83%	88%	82%
Locken van computer	81%	100%	76%
Clean desk	60%	81%	55%
Antivirus / antiphishing	72%	88%	68%
Incident afhandeling	83%	100%	79%

Tabel 9 Overzicht awareness management en medewerkers m.b.t. informatiebeveiligingsmaatregelen

De gemiddelde awareness van het management en de medewerkers, over de 11 gelijk gewogen informatiebeveiligingsmaatregelen in Tabel 9, komt uit op respectievelijk 83% en 62%.

	Gemiddelde Awareness	Awareness Management	Awareness Medewerkers
Awareness			
Begrip social engineering	56%	56%	56%
Aanvalsverloop	39%	56%	35%
Motieven	55%	81%	49%
Awareness aanvalstechnieken/methoden	51%*	53%*	51%*
Phishing	100%	100%	100%
Dumpster diving	40%	44%	39%
Office snooping	40%	44%	39%
Tailgating	56%	69%	53%
Baiting / Item dropping	39%	38%	39%
Malicious software	79%	81%	79%
Reverse social engineering	33%	25%	35%
Totaal Gemiddelde Awareness	50%**	62%**	48%**

Tabel 10 Overzicht awareness management en medewerkers m.b.t. social engineering

* gemiddelde awareness over opgesomde social engineering aanvalstechnieken/methoden, zonder malicious software.
** de totaal gemiddelde awareness is de som over de vier onderwerpen begrip, verloop, motieven en methoden, gedeeld door 4.

De gemiddelde awareness bij management en medewerkers over social engineering, uitgaande van het gemiddelde over de 4 gelijk gewogen onderwerpen begrip, verloop, motieven en methoden in Tabel 10, is respectievelijk 62% en 48% .

De conclusie is dat het management op beide onderwerpen, zowel over informatiebeveiligingsmaatregelen als social engineering, hoger scoren qua gemiddelde awareness dan medewerkers. Het gemiddelde verschil op beide onderwerpen bedraagt respectievelijk 21% en 14%.

6.7. Doelwit social engineeringsaanvallen

Deelvraag 7: Van welke social engineering aanvallen is de Nederlandse Rijksoverheid in het afgelopen jaar slachtoffer geweest en welk medium gebruikten deze aanvallen?

Van de deelnemers aan de online survey, geeft bijna de helft (49%) aan doelwit te zijn geweest van social engineeringsaanvallen in de afgelopen 6 maanden. De aanvallen vonden voornamelijk plaats via email (55%). Benadering via social media en telefoon werd in respectievelijk 13% en 9% van de aanvallen genoemd als kanaal. Fysieke of andere wijze van benaderen zijn niet genoemd.

In vergelijk met het in 2016 uitgevoerde onderzoek (Van der Laan, 2016) is er sprake van een daling in het percentage deelnemers dat aangaf benadert te zijn, 61% in 2016 tegenover 49% nu. Wel blijft email het belangrijkste kanaal (55%, 57% in 2016) en is social media als medium in opkomst, met 7% in 2016 tegenover 13% nu.

6.8. Onderzoeksvragen en hypothesen

Onderzoeksvraag 1: Wat is het verschil tussen de mate waarin informatiebeveiligingsbeleid is doorgevoerd binnen de Rijksoverheid omtrent de geïdentificeerde social engineering maatregelen uit het literatuuronderzoek en de mate waarin de medewerkers en management op de hoogte zijn van dit informatiebeveiligingsbeleid?

Geconcludeerd kan worden dat op alle 22 geïdentificeerde social engineering maatregelen (Tabel 11) uit het literatuuronderzoek beleid aanwezig is.
Geconcludeerd kan worden dat van de bevraagde informatiebeveiligingsmaatregelen, 11 in totaal, de gemiddelde medewerker awareness 66% bedraagt. De mate waarop medewerkers en management op de hoogte zijn van dit beleid verschilt sterk per maatregel. Bij drie maatregelen, rood gearceerd in Tabel 11, blijkt de kennis bij slechts de helft of minder van de medewerkers aanwezig te zijn. Op alle maatregelen scoort het management beduidend beter dan de gemiddelde medewerker.

Maatregel	Beleid aanwezig	Awareness Beleid		
		Gemiddeld	Management	Medewerkers
Screening CV, referenties	Ja	22%	44%	17%
Arbeidsvoorwaarden / VOG	Ja	93%	100%	92%
Retourneren bedrijfsmiddelen	Ja	73%	88%	70%
Blokkering toegangsrechten	Ja	76%	94%	71%
Informatie classificatie	Ja	37%	69%	29%
Documentafhandeling/-vernietiging	Ja	51%	63%	48%
Wachtwoord management	Ja	83%	88%	82%
Locken van computer	Ja	81%	100%	76%
Clean desk	Ja	60%	81%	55%
Antivirus / antiphishing	Ja	72%	88%	68%
Incident afhandeling	Ja	83%	100%	79%

Tabel 11 Overzicht aanwezige beleidsmaatregelen en awareness

Hypothese 1: Het informatiebeveiligingsbeleid met betrekking tot social engineering binnen de Rijksoverheid is niet bekend bij het merendeel van de medewerkers.

Gesteld wordt dat minimaal de helft van de medewerkers (50%) bevestigend moet kunnen antwoorden op de vragen rondom het bekend zijn met het gevoerde informatiebeveiligingsbeleid op social engineering.

De gemiddelde awareness van het management en de medewerkers, over de 11 gelijk gewogen informatiebeveiligingsmaatregelen in Tabel 11, komt uit op respectievelijk 83% en 62%. Gesteld kan worden dat meer dan de helft van de medewerkers (62%) op de hoogte is van het beleid, daarmee wordt deze hypothese verworpen.

Hypothese 2: Het informatiebeveiligingsbeleid met betrekking tot social engineering binnen de Rijksoverheid wordt niet uitgedragen door het management.

Uitdragen wordt geïnterpreteerd als het actief informeren van medewerkers over het beleid. Gesteld wordt dat minimaal de helft van medewerkers (50%) bevestigend moet antwoorden om te kunnen spreken over het uitdragen van informatiebeveiligingsbeleid binnen de afdelingen.

Deelnemers aan de online survey is gevraagd of het beveiligingsbeleid actief uitgedragen / verspreid wordt binnen de afdeling en organisatie? Hierbij antwoordt 44% met Ja, 48% met Nee en 8% weet het niet. Als hierbij wordt ingezoomd op de reacties van medewerkers en management, dan geeft 36% van de medewerkers en 75% van het management aan te vinden dat het beleid actief wordt uitgedragen. Geconcludeerd kan worden dat er tussen medewerkers en management een groot verschil (36% vs. 75%) waarneembaar is of beleid wordt uitgedragen. Gesteld kan worden dat minder dan de helft van de medewerkers (36%) vindt dat het beleid wordt uitgedragen, daarmee houdt deze hypothese stand.

Onderzoeksvraag 2: In hoeverre is de Rijksoverheid zelf het doelwit of slachtoffer van social engineering aanvallen?

In de online survey is onderzocht of medewerkers denken in de afgelopen 6 maanden het slachtoffer te zijn geweest van een social engineeringaanval. 49% van de deelnemers geeft aan afgelopen 6 maanden doelwit te zijn geweest van een social engineeringaanval.
Op de vraag via welke kanalen deze pogingen werden ondernomen, antwoordt 55% van de deelnemers via email te zijn benaderd, ruim 14% via social media en bijna 10% telefonisch. 7 Deelnemers (8%) geven aan via twee kanalen te zijn benaderd, 5 deelnemers (6%) geven aan via drie kanalen te zijn benaderd de afgelopen 6 maanden.

Hypothese 3: Meer dan 50 procent van de onderzochte Rijksoverheid-medewerkers is in de afgelopen zes maanden slachtoffer geweest van een social engineering aanval.

Gesteld kan worden dat 49% van de medewerkers doelwit is van social engineering aanvallen, daarmee houdt deze hypothese geen stand.

6.9. Eindconclusie

Geconcludeerd kan worden dat gemiddeld 62% van de medewerkers en 83% van de managers van de Rijksoverheid op de hoogte is van het geldende informatiebeveiligingsbeleid en de gemeten 11 informatiebeveiligingsmaatregelen. Positief valt op dat bij 8 van de 11 maatregelen de score onder managers op bekendheid met de maatregel op 92% ligt. In veel van de genomen maatregelen heeft de manager een bepalende rol, denk aan de procedures rondom in- en uitdiensttreding, het acteren op incidenten, maar vooral als het gaat om het vervullen van een voorbeeldfunctie en het handelen in de geest van de maatregelen. Medewerkers scoren gemiddeld genomen lager dan managers, toch is op 8 van de 11 maatregelen de score 74% op bekendheid met de maatregel. Negatieve uitschieters zitten op het vlak van kennis over het beleid rondom informatieclassificatie en documentafhandeling/-vernietiging, deze is maar bij respectievelijk 29% en 48% van de medewerkers en 69% / 63% van de managers bekend. Opvallend is dat het controleren van het CV en de referenties bij nieuwe medewerkers met een awareness van 22% onder medewerkers en 44% onder managers laag scoort. Mogelijke verklaring zou kunnen zijn, dat het merendeel van de medewerkers niet betrokken is bij sollicitatieprocedures en het lijkt er op dat managers vooral vertrouwen op de voorwaarde dat nieuwe medewerker een verklaring omtrent gedrag (VOG) voor het in dienst treden moeten kunnen overleggen. Deze arbeidsvoorwaardelijke maatregel wordt door 100% van de managers genoemd.

Hoewel de in de literatuurstudie benoemde maatregelen terugkomen op verschillende plekken in het Rijksbreed geldende informatiebeveiligingsbeleid, is in de onderzochte stukken geen specifiek beleid op social engineering gevonden. Geconcludeerd kan worden dat er in het Rijksbeleid en de informatiebeveiligingsmaatregelen onvoldoende aandacht is voor social engineering. Het onderzoek laat zien dat 52% van de medewerkers en 38% van de managers onvoldoende bekend is met het begrip, de motieven, de methoden en het aanvalsverloop van social engineering. Het bewustzijn op een mogelijk poging tot social engineering is een belangrijke factor om een aanvalspoging te voorkomen. De recente phishing campagnes binnen de Rijksoverheid hebben een direct effect op de alertheid rondom phishingmails, alle respondenten (100%) in dit onderzoek hebben aangegeven deze aanvalsmethode te herkennen. Er ligt dus nog een taak om de bekendheid van de andere methoden, welke met de gegeven toelichting gemiddeld door 42% van de respondenten wordt herkend, te vergroten. Dit sluit aan bij de wens van veel medewerkers en managers (84%) om een training op het vlak van social enginering en informatiebeveiliging te kunnen volgen. De noodzaak tot handelen wordt vergroot door het feit dat ongeveer de helft (49%) van de medewerkers binnen de Rijksoverheid heeft aangegeven dat deze het afgelopen half jaar te maken heeft gehad met één of meerdere social engineeringsaanvallen.

6.10. Aanbevelingen

Gezien de beperkingen in de beschikbare tijd en middelen, maar ook de scope van het onderzoek, volgen in deze paragraaf aanbevelingen voor mogelijk vervolgonderzoek en andere praktische invullingen.

Scope

De scope van dit onderzoek is gelimiteerd tot het onderzoek binnen één Rijksdienst. Om bepaalde contextuele invloeden uit te sluiten, verdient het de aanbeveling om het onderzoek op grotere en /of bredere schaal te herhalen, om daarmee de onderzoeksresultaten generaliseerbaar te maken

voor de Rijksoverheid als geheel. Verbreding van de scope zou kunnen door een andere Rijksdienst binnen een ander ministerie te onderzoeken en vergelijken. Vergroten van de schaal van het onderzoek kan door binnen meerdere ministeries en/of rijksdiensten het onderzoek te herhalen.

Onderzoeksmethode
Aanvullende waarnemende onderzoeksmethoden, zoals action research, kunnen worden ingezet om meer achtergrond over het proces van veranderen bij de implementatie van het informatiebeveiligingsbeleid en de informatiebeveiligingsmaatregelen te onderzoeken. Maar denk ook aan de leercurve die medewerkers hebben bij het vergaren van kennis over social engineering, dan wel welke effect dit heeft op het handelen van medewerkers en mogelijke best practices te destilleren.

Referentieraamwerk
Het ontwikkelde referentieraamwerk vormt een eerste aanzet voor het plaatsen van relevante maatregelen op betreffende social engineeringsaanvallen en kan op tal van wijzen worden uitgebreid. Mogelijke aanvullingen op het model liggen in het uitbreiden met nog niet onderzochte maatregelen, te groeperen op thema's en eventuele classificatie van risico's. Ook voegt het waarde toe om bij maatregelen een indeling naar de incidentencyclus (preventief, detectief, repressief en correctief) op te nemen, zodat inzichtelijk wordt welke maatregel zinvol is in relatie tot het effect van een potentieel social engineeringsincident. Daarnaast vindt er doorontwikkeling plaats op de ISO 27001 norm, de meest recente versie van de standaard wordt nog niet binnen de Rijksoverheid toegepast, maar zodra deze wordt geadopteerd en uitgerold, zou het raamwerk hierop aangepast moeten worden.

Praktijk
De huidige lijst met BIR maatregelen zoals deze binnen alle Rijksdiensten wordt gehanteerd, zou op basis van het refererentieraamwerk een praktische uitwerking kunnen krijgen door de maatregelen ook te groeperen op thema's van potentiele dreigers, waaronder social engineering. Hiermee zou het voor de Rijksdiensten inzichtelijk moeten maken hoe zij zich gericht kunnen wapen en effort kunnen steken in die maatregelen die vooral deze dreiging afdekken.

Een social engineeringsaanval kent vaak verschillende fases, van verkennende stappen tot aan het daadwerkelijk bereiken van de gewilde informatie. Elke fase kent weer verschillende methode/technieken of combinaties om de medewerker te manipuleren/beïnvloeden. Om daar zicht op te krijgen, is het belangrijk dat losstaande voorvallen worden herkend en daarmee gemeld. Met de resultaten van dit onderzoek, pleit dit voor het inzetten op twee zaken; a. werk door trainingen, voorlichting aan het vergroten van de awareness op social engineering en b. werk aan de bekendheid van de incidentenprocedure binnen de organisatie, zodat ogenschijnlijke losse incidenten een signaal vormen waarop de organisatie kan gaan acteren.

7. Reflectie

In dit hoofdstuk een reflectie op de kwaliteit van het onderzoek en de houdbaarheid van de conclusies. Daarnaast een terugblik op het verloop van het onderzoeksproces.

Product

Voor dit onderzoek is gebruik gemaakt van triangulatie, door de bevindingen uit het archiefonderzoek te combineren met kwalitatieve semi-gestructureerde interviews en kwantitatieve gegevens uit de online survey, ontstaat een vrij accuraat beeld op het informatiebeveiligingsbeleid rondom social engineering binnen de Rijksoverheid. Hoewel het onderzoek plaats heeft gevonden binnen de context van één Rijksdienst en daarmee niet direct te generaliseren is naar de toestand van andere diensten, geeft het in dit geval wel een inkijk door de generieke Rijksbrede opzet van het informatiebeveiligingsbeleid en de uitvoering hiervan binnen de Rijksoverheid.

Het aangetroffen beleid kent qua opzet geen veranderingen ten opzichte van het uitgevoerde onderzoek in 2016, hierdoor is het mogelijk een vergelijk te maken en aanvullende inzichten te vergaren. Ook bleek mijn eerder uitgevoerde literatuuronderzoek naar een context gedreven informatiebeveiligingsaanpak (Spijker, 2016) waardevol te zijn, bij het kunnen neerzetten van het referentiemodel. Het onderwerp informatiebeveiliging en de binnen de Rijksoverheid gehanteerd ISO 27001 norm vormden daarvoor een bruikbaar aanvullend deel. Ik meen dat het onderzoek nu sterker onderbouwd is en het referentiemodel een solide basis vormt voor het prioriteren van maatregelen. Daarbij is met inbedding van de ISO 27001 normering het referentieraamwerk ook in bredere context, buiten de overheid inzetbaar.

Tijdens het uitwerken van de resultaten bleek dat het referentieraamwerk meer op maatregelthema's geclusterd had kunnen worden. Hierbij denk ik aan het detail zoals bijvoorbeeld weergegeven bij de fysieke beveiliging of rondom informatieverwerking/vernietiging. Deze maatregelen kennen een onderlinge samenhang, die prima als groep onderzocht had kunnen worden en waarbinnen toetsbare eigenschappen zijn op te nemen zoals camera's, bezoekerspassen en toegangsdeuren zijn benoemd. Dit bied ook kansen om het model op meer punten qua maatregelen aan te vullen en toch het raamwerk als stuurmechanisme overzichtelijk te houden.

Door een fout in het opstellen en verwerken van de online survey is de vraag rondom fysieke beveiligingsmaatregelen weggevallen. Hierdoor is het niet mogelijk geweest om in dit onderzoek ook de awareness op deze maatregelen (nr. 8 t.m. 12) te meten. Mogelijk valt de totale berekende awareness binnen dit onderzoek daarmee lager uit, aangezien fysieke maatregelen direct zichtbaar zijn en opgemerkt worden.

Rondom het onderwerp management buy-in, vrij vertaald betrokkenheid van het management, had achteraf het concept meer geoperationaliseerd kunnen worden. Wat is nu betrokkenheid, hoe meet ik die? Het huidige verkregen resultaat leunt nu op het kunnen benoemen van verantwoordelijkheden en het actief uitgedragen, dit kan sterker door bijvoorbeeld meer kwantificeerbaar te maken hoe vaak aandacht wordt besteed aan informatiebeveiliging op de afdeling.

Ook rondom het meten van de awareness, op zowel informatiebeveiliging als social engineering, zijn verdere slagen in het operationaliseren mogelijk. Ik heb er bewust voor gekozen om een toelichting op de social engineeringsmethoden weer te geven bij het survey onderzoek, zodat herkenning van de gebruikte techniek centraal staat en niet of de term een bekend begrip is onder medewerkers.

Een vervolg onderzoek zou zich daarom meer moeten richten op het operationaliseren van het concept opleiding/educatie, een belangrijke pijler volgens de literatuur en het referentieraamwerk.

Daarnaast blijft de vraag hoe medewerkers uiteindelijk handelen, met of zonder kennis. Het kwantificeren van het daadwerkelijk handelen, zou vorm kunnen krijgen met het voorleggen van een aantal casussen en mogelijke oplossingsrichtingen. Hierdoor zou ook inzichtelijk kunnen worden, of medewerkers met een opleiding/training anders handelen dan medewerkers zonder opleiding.

Het onderzoeksmodel biedt tal van aanvullende onderzoeksvragen, om bijvoorbeeld de “werkelijke” dekking van een maatregel te onderzoeken. Een dergelijk inductief onderzoek vraagt uiteraard een andere opbouw van het onderzoek. Een grounded theory onderzoek, om het gedrag van medewerkers aan de hand van waarneming en testen te voorspellingen, vormt dan een betere aanpak om het management vraagstuk rondom informatiebeveiliging op social engineering te onderzoeken.

Overal, meen ik dat de conclusies stand houden. Het onderzoek laat zien dat het informatiebeveiligingsbeleid op social engineering binnen de Rijksoverheid onvoldoende overkomt bij de medewerkers. De resultaten van het onderzoek laten zien op welke punten er winst valt te behalen. Het referentieraamwerk social engineering biedt een overzichtelijk vertrekpunt voor het bepalen van aanvullend informatiebeveiligingsbeleid en te nemen maatregelen op de verschillende dreigingen, methoden en technieken.

Proces

Mede op aanraden van de begeleiders bij de OU heb ik uiteindelijk besloten om niet mijn eigen onderzoekswerk voor te zetten, maar af te studeren op een concreter en verwant onderzoeksonderwerp rondom informatiebeveiliging.

Door onvoldoende focus in de onderzoeksvragen bij de uitwerking van mijn literatuuronderzoek naar de contextuele eigenschappen bij informatiebeveiliging , ontstond daarmee ook onvoldoende basis voor het kunnen vervolgen met een empirisch onderzoek. Althans parttime niet realistisch haalbaar binnen de gestelde periode van een jaar. Ik heb achteraf bezien in het literatuuronderzoek te veel tijd en mezelf verloren in het verzamelen en ordenen van alle mogelijk relevante informatie. Wel jammer, ik had graag mijn ideeën en de haalbaarheid van een contextueel model getoetst.

Op voorhand stond ik niet te juichen om een herhalingsonderzoek uit te gaan voeren, natuurlijk had ik liever op basis van mijn eigen verzamelde literatuur het geheel, literatuur en onderzoek, in eigen lijn afgemaakt. Tijdens het opzetten en uitvoeren van dit herhalingsonderzoek bleek al snel dat ik nog steeds voldoende ruimte had om het onderzoek naar eigen hand te kunnen zetten. Sterker nog, het bleek heel waardevol om zowel de redenaties en afweging van het eerdere onderzoek te lezen en daaraan mijn eigen gedachten en werkwijze te kunnen spiegelen.

Het scherp krijgen en houden van de onderzoeksvraag is een lastig item. Al snel ben ik geneigd er tal van zaken bij te betrekken en daarmee af te dwalen van de onderzoeksvraag. Binnen het literatuuronderzoek speelde dit, maar ook in dit empirisch onderzoek en het interpreteren van de resultaten, moet ik me zelf scherp houden om niet aan de haal te gaan met interessante bevindingen die geen direct relatie hebben met de onderzoeksvragen.

Voor de uitvoering van het onderzoek was het prettig om wel een achtergrond te hebben bij de Rijksoverheid, maar niet in dienst te zijn van de te onderzoeken organisatie. Dat maakt dat je als onderzoeker wel gevoel hebt voor de context waarbinnen het onderzoek zich afspeelt, maar tegelijk een voor het onderzoek wenselijke afstand houdt tot de praktijk en niet verleid wordt om als

deelnemer te acteren op een besproken situatie. Een nadeel van extern zijn, is dat je in het schakelen en het maken van de afspraken met betrekking tot de uitvoering onderzoek binnen de organisatie, meer tijd en ruimte moet incalculeren.

Overigens verliep het proces van empirisch onderzoek doen aanzienlijk meer volgens mijn eigen planning. Met de ervaring van het literatuuronderzoek nog in mijn achterhoofd, heb ik scherper op doelstellingen binnen het onderzoek gestuurd. Waar ik mij op verkeken heb is het uitwerken van de acht afgenomen interviews. Het terugluisteren en verwoorden kostte mij al snel 5 a 6 uur per interview. Wat zeker heeft bijgedragen aan het proces, is dat ik binnen de organisatie zeer warm en open ontvangen werd ontvangen. Ik heb alle medewerking gekregen, wat maakte dat het onderzoek eenmaal gestart, goed door kon lopen.

De aanpak met het in teamverband werken aan de uitvoeren van het empirisch onderzoek heeft voor mij voor een positieve aanjagende en relativerende wisselwerking gezorgd. Hoewel je je eigen onderzoeksopdracht hebt, is het prettig bepaalde gedachten of aanpak met elkaar te kunnen delen.

Terugblikkend, ook op het literatuuronderzoek, zou ik meer sturing en leidraad willen hebben gehad, om de “bril” waardoor ik naar het onderzoek moet kijken fijn te slijpen. Dat proces van leren focussen is in mijn ogen essentieel in het zelfstandig en succesvol kunnen opzetten en uitvoeren van wetenschappelijk onderzoek. Ik verwacht dat de Open Universiteit meer rendement uit haar onderzoekers in opleiding kan halen, door dat opleidingsonderdeel meer te belichten. Ik denk hierbij aan een klassikaal of online webinar waarin gedoceerd wordt rondom het thema “hoe bouw ik mijn onderzoek?”. Praktisch zou dit kunnen worden ingevuld, door met de eindpresentatie terug te werken naar de start van het onderzoek, wat heb ik te doen en in te vullen om mijn resultaten te kunnen presenteren. De theorie gaat dan direct “leven”.

8. Bibliografie

CBS. (2012). *Peilingen beoordelen.* Opgehaald van www.cbs.nl: https://www.cbs.nl/nl-nl/publicatie/2012/34/peilingen-beoordelen

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. (2012). *Baseline Informatiebeveiliging Rijksoverheid - Tactisch Normenkader (BIR:2012 TNK).* http://www.earonline.nl/index.php/BIR_2012.

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. (2013). *Operationele Handreiking Informatiebeveiliging (BIR-OH:2013).* https://www.earonline.nl/images/earpub/5/5c/BIR_Operationele_Handreiking_v1_0.pdf.

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. (2014). *BIR comply or explainprocedure.* https://www.earonline.nl/images/earpub/a/a9/04._A_BIR_explainprocedure_1.0_voor_ICCIO-1-.pdf.

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. (2014). *BIR Quick Scan.* https://www.earonline.nl/images/earpub/9/90/04._B_QuickScan_BIR_20140121_v10-1-.pdf.

Rijksoverheid. (2007). *Voorschrift Informatiebeveiliging Rijksdienst (VIR:2007).* Opgehaald van Overheid.nl Wet- en regelgeving: http://wetten.overheid.nl/BWBR0022141/2007-07-01

Rijksoverheid. (2013). *Beveiligingsvoorschrift Rijksdienst (BVR:2013).* Opgehaald van Overheid.nl Wet- en regelgeving: http://wetten.overheid.nl/BWBR0033512/2013-06-01

Rijksoverheid. (2013). *Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie (VIRBI:2013).* Opgehaald van Overheid.nl Wet- en regelgeving: http://wetten.overheid.nl/BWBR0033507/2013-06-01

Rijksoverheid. (2015). *Archiefwet.* Opgehaald van Overheid.nl Wet- en regelgeving: http://wetten.overheid.nl/BWBR0007376/2015-07-18

Rijksoverheid. (2017). *Algemeen Rijksambtenarenreglement.* Opgehaald van Overheid.nl Wet- en regelgeving: http://wetten.overheid.nl/BWBR0001950/2017-01-01

Saunders, L. T. (2015). *Methoden en technieken van onderzoek, 7e Editie.* Amsterdam: Pearson.

Spijker, D. (2016). *Een passende informatiebeveiligingsaanpak.* Opgehaald van Open Universiteit: http://www.open.ou.nl/hjo/supervision/2016-BPMIT-Dennis.Spijker-literatuuronderzoek.pdf

Van der Laan, K. (2016). *Social engineering binnen de Nederlandse Rijksoverheid*. Opgehaald van Open Universiteit: http://www.open.ou.nl/hjo/supervision/2016-BPMIT-krijn.van.der.laan-scriptie.pdf

Bijlage A: Aanvalstactieken social engineering

Social engineeringstactieken (Granger, 2010; Krombholz et al., 2015; Mitnick & Simon, 2003).

Nr	Aanvalstactiek	Aard	Toelichting
Voorbereiding, verzamelen			
1	Dumpster diving	M	Dumpster diving is het doorzoeken van de prullenbak/afvalcontainer van particulieren of bedrijven met als doel weggegooide items te vinden met gevoelige informatie. Deze informatie kan vervolgens worden gebruikt om toegang tot een systeem of een specifieke gebruikersaccount te bemachtigen.
2	People spotting	M	People spotting is het bestuderen en observeren van een slachtoffer of een groep slachtoffers om na te gaan wat hun gewoontes zijn.
3	Physical reconnaissance / Shoulder surfing	M	Shoulder surfing verwijst naar het gebruik van directe-observatietechnieken om informatie te krijgen, zoals meekijken over iemands schouder naar zijn scherm of toetsenbord.
4	Pretexting / Profiling	M	Pretexting is wanneer een social engineer een verhaal ontwikkelt dat hem in staat stelt om zich een beeld te verwerven van de doelgroep. Het biedt de rechtvaardiging voor de vragen die bij de echte aanval gesteld kunnen worden.
5	Mail-outs	T	Er bestaan verschillende soorten mail-outs, bijvoorbeeld in de vorm van enquêtes. Deze worden gebruikt om bedrijfs- en persoonlijke informatie te verzamelen. Deelname aan deze enquêtes wordt verhoogd door het aanbieden van prijzen. Maar mail-outs kunnen ook gebruikt worden om mensen te misleiden voor reverse social engineering of malicious software aanvallen.
6	Phishing	T	Phishing is de poging om gevoelige informatie te verwerven of om iemand te laten handelen op een gewenste manier door zich voor te doen als een betrouwbare entiteit. De aanvallen zijn meestal gericht op grote groepen mensen. Phishing-aanvallen kunnen worden uitgevoerd op bijna elk kanaal, van websites, fysieke benadering, sociale netwerken tot zelfs cloud-diensten. Aanvallen gericht op specifieke personen of bedrijven worden aangeduid als spear phishing. Als een phishing-aanval is gericht op high-profile doelen in ondernemingen, wordt de aanval aangeduid als de whale fishing.
7	Phreaking / Vishing	T	Phreaking of Vishing is het misbruiken van een bedrijfstelefoon of telefooncentrale, zodanig dat iemand intern kan bellen, of gesprekken af kan luisteren. De aanvaller kan daarbij zich voordoen als een collega, belt immers intern en verschaft zich daarmee de legitimiteit om gewebste informatie (uit) te vragen.

Nr	Aanvalstactiek	Aard	Toelichting
8	Virtual reconnaissance / Waterholing	T	Waterholing beschrijft een gerichte aanval waarin de aanvallers een website overnemen die waarschijnlijk bezocht gaat worden door het gekozen slachtoffer. De aanvallers wachten vervolgens „bij de waterpoel" op hun slachtoffer.
9	Web search	T	Web search is het zoeken naar online informatie over het slachtoffer of de organisatie. Hiermee wordt het voorwerk gedaan voor een verdere aanval.
Manipulatie			
10	Physical Impersonation	M	Impersonatie is het zich voordoen als een werknemer met als doel de slachtoffers te misleiden. De meeste mensen zijn sneller bereid te helpen of regels te omzeilen als het om een collega gaat.
11	Reverse social engineering	M	Reverse social engineering is een aanval waarbij eerst een vertrouwensrelatie tot stand wordt gebracht tussen de aanvaller en het slachtoffer. De aanvaller creëert een situatie waarin het slachtoffer hulp nodig heeft waarna hij zichzelf presenteert als de persoon die de situatie kan oplossen. Dit zorgt ervoor dat het slachtoffer hem vertrouwt en eerder op zijn verzoeken zal ingaan.
12	Virtual impersonation / Fake profiles	T	Fake profiles is het opzetten van onechte profielen met het doel informatie van de slachtoffers te bemachtigen.
Exploitatie			
13	Direct approach	M	Direct approach is de directe benadering van slachtoffers om informatie te bemachtigen die nodig is voor de daadwerkelijke aanval. Dit kan door simpelweg te bellen en te vragen naar informatie.
14	Office Snooping / Desk sniffing	M	Office snooping/Desk sniffing is het doorzoeken van een kantoor en de werkplekken binnen het kantoor van bedrijven met als doel het vinden van gevoelige informatie. Deze informatie kan vervolgens worden gebruikt om toegang tot een systeem of een specifieke gebruikersaccount te bemachtigen.
15	Piggybacking / Tailgating	M	Piggybacking of tailgating is een aanval waarmee met een andere persoon wordt meegelopen om in een besloten gebied te komen. De persoon met wie wordt meegelopen heeft wel de juiste autorisatie.
16	Baiting / Item dropping	T	Baiting is een aanval waarbij een met malware geïnfecteerd opslagmedium wordt achtergelaten op een plaats waar het beoogde slachtoffer dit zal vinden.
17	Data leakage	T	Data leakage is het met opzet achterlaten van een bestand op een systeem of in de cloud met de bedoeling dat andere individuen dit bestand openen. Op het moment van openen, kan kwaadaardige software worden geïnstalleerd.
Uitvoering			

Nr	Aanvalstactiek	Aard	Toelichting
18	Identity theft	M / T	Identity theft is het gebruiken van informatie van een persoon zonder diens medeweten, zoals zijn naam, bankrekeningnummer, geboortedatum of zijn BSN-nummer. Dit kan op verschillende wijzen worden bewerkstelligd, variërend van het dragen van een uniform, phishing-aanvallen tot het aanpassen van de DNS-setting.
19	Malicious software	T	Malicious software is kwaadaardige software die door een social engineer wordt geïnstalleerd of wordt aangeboden. Als de software eenmaal op het systeem van de slachtoffer is geïnstalleerd, kan vaak de controle op het systeem worden overgenomen of wordt bepaalde informatie verzameld en opgehaald.

Bijlage B: Maatregelen Informatiebeveiliging

Relevante informatiebeveiligingsmaatregelen (Allen, 2006; Gulati, 2003; Hinson, 2008).

Nr	Maatregel	Norm	Toelichting
Personele beveiliging			
1	Screening CV, referenties	8.1.2	Verificatie van de achtergrond van alle kandidaten voor een dienstverband, ingehuurd personeel en externe gebruikers behoren te worden uitgevoerd overeenkomstig relevante wetten, voorschriften en ethische overwegingen. Dit behoort evenredig te zijn aan de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend en de waargenomen risico's.
2	Arbeids- voorwaarden	8.1.3	Als onderdeel van hun contractuele verplichting behoren werknemers, ingehuurd personeel en externe gebruikers de algemene voorwaarden te aanvaarden en te ondertekenen van hun arbeidscontract waarin hun verantwoordelijkheden en die van de organisatie ten aanzien van informatiebeveiliging behoren te zijn vastgelegd.
3	Management buy-in	8.2.1	Managers moeten een duidelijk begrip krijgen van wat hun rol is in het definiëren van de benodigde beveiligingsmaatregelen. Dit inzicht moet ervoor zorgen dat de juiste beschermende maatregelen worden getroffen met betrekking tot de risico's van social engineering . De directie behoort van werknemers, ingehuurd personeel en externe gebruikers te eisen dat ze de beveiliging toepassen overeenkomstig vastgesteld beleid en vastgestelde procedures van de organisatie.
4	Opleiding en bewustwording	8.2.2	Alle werknemers van de organisatie, ingehuurd personeel en externe gebruikers, behoren geschikte training en regelmatige bijscholing te krijgen met betrekking tot beleid en procedures van de organisatie, voor zover relevant voor hun functie.
5	Disciplinaire maatregelen	8.2.3	Er behoort een formeel disciplinair proces te zijn vastgesteld voor werknemers die inbreuk op de beveiliging hebben gepleegd.
6	Retourneren bedrijfsmiddelen	8.3.2	Alle werknemers, ingehuurd personeel en externe gebruikers behoren alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben te retourneren bij beëindiging van hun dienstverband, contract of overeenkomst.

Nr	Maatregel	Norm	Toelichting
7	Blokkering toegangsrechten	8.3.3	De toegangsrechten van alle werknemers, ingehuurd personeel en externe gebruikers tot informatie en IT-voorzieningen behoren ter worden geblokkeerd bij beëindiging van het dienstverband, het contract of de overeenkomst, of behoort na de wijziging te worden aangepast.
Toegangsbeveiliging			
8	Beveiligings- camera's	9.1.1	Een essentieel controlemiddel voor het beperken van de fysieke toegang van medewerkers, aannemers en bezoekers tot computerfaciliteiten en -systemen. De organisatie moet effectieve fysieke beveiligingsmaatregelen nemen, zoals bezoekerslogs, begeleide toegang en antecedentenonderzoek. Hier vallen onder: • Foto-identificatiepasjes • Toegangsdeuren • Beveiligingscamera's • Bezoekerspasjes • Aanmeldformulieren
9	Aanmeldprocedure bezoekers	9.1.2	
10	Bezoekerspasjes	9.1.2	
11	Foto-identificatiepasjes	9.1.2	
12	Toegangsdeuren	9.1.3	
Informatiebeveiliging			
13	Informatie classificatie	7.2.1	Een classificatiebeleid dient duidelijk te beschrijven welke informatie als gevoelig wordt beschouwd en hoe met deze informatie om moet worden gegaan.
14	Documentafhandeling/-vernietiging	10.7.3	Gevoelige documenten en media moeten veilig worden afgevoerd/vernietigd en niet gewoon worden weggegooid in de reguliere kantoorprullenbak.
15	Beperken publieke informatie	10.9.3	Het verminderen van de hoeveelheid beschikbare specifieke gegevens zorgt ervoor dat een aanval niet de moeite waard is. Websites, openbare databases, internetregisters en andere publiek toegankelijke bronnen dienen alleen algemene informatie te bevatten.
16	Wachtwoord management	11.3.1	Richtlijnen zoals het aantal karakters dat en de aard daarvan die elk wachtwoord moet bevatten, hoe vaak een wachtwoord moet worden gewijzigd en zelfs een eenvoudige verklaring dat de medewerkers geen wachtwoorden moeten bekendmaken aan anderen.
17	Locken van computer	11.3.2	Wanneer een medewerker niet in de buurt van zijn computer is, dient hij de computer te locken zodat andere personen hier geen gebruik van kunnen maken.
18	Clean desk	11.3.3	Documenten dienen niet open en bloot op de bureaus van medewerkers te liggen. De documenten dienen veilig in kasten, achter slot en grendel, te worden opgeborgen.

Nr	Maatregel	Norm	Toelichting
19	Antivirus / antiphishing	10.4.1	Meerdere lagen van virusafweer, zoals bij e-mailgateways en eindgebruiker-desktop, kunnen de dreiging van phishing- en andere socialengineeringaanvallen minimaliseren.
20	E-mailfiltering	10.8.4	Het opzetten en onderhouden van e-mail-spamfilters zal ervoor zorgen dat gebruikers minder snel ten prooi vallen aan phishing-aanvallen, ketting-e-mails, virussen of wormen die schade zouden kunnen veroorzaken.
Beveiligingsproces			
21	Incident afhandeling	13.1.1	Een gedocumenteerde incidentreactiestrategie zal ervoor zorgen dat een gebruiker onder druk precies weet welke procedures hij dient te volgen.
22	Audit beleid / audit controles	15.2.1	Als procedures, richtlijnen en beleid zijn opgesteld binnen een organisatie maar niemand zich hier aan houdt, dan levert dit beleid weinig toegevoegde waarde aan het verminderen van de risico's met betrekking tot social engineeringaanvallen.

Bijlage C: Online survey vragen

Online survey social engineering

Deze enquête peilt het bewustzijn van de medewerkers op het informatiebeveiligingsbeleid en social engineering.
Een organisatie kan voor alle gevaren maatregelen en procedures hebben genomen, als deze maatregelen en procedures echter niet bekend zijn bij de medewerkers, hebben deze niet het effect wat wordt verwacht.
Hiermee wordt dan ook getracht inzicht te krijgen in hoe de theorie aansluit bij de praktijk.

De enquête wordt anoniem afgenomen, bestaat uit 25 multiplechoicevragen, waarbij één of meerdere antwoorden gekozen dienen te worden.
Rondje = één antwoord mogelijk
Vierkant = meerdere antwoorden zijn mogelijk

De verwachte duur van de enquête is +- 10 minuten.

Alleen de antwoorden op de vragen worden opgeslagen, er worden geen andere gebruikersgegevens verzameld. De Open Universiteit slaat de gegevens op in een afgeschermde omgeving, alleen de onderzoeker heeft toegang tot deze gegevens.

*Vereist

Algemene vragen

1. **1. In welke categorie zou u uw functie plaatsen?** *
   Markeer slechts één ovaal.

   - ◯ Management
   - ◯ IT specialist
   - ◯ Medewerker productgroep / dienstverlening
   - ◯ Ondersteunende functie (zoals o.a. HRM, Inkoop, Financien, Service level en relatiebeheer)
   - ◯ Anders

2. **2. Hoeveel jaar werkt u in uw huidige functie?** *
   Markeer slechts één ovaal.

   - ◯ < 2 jaar
   - ◯ 2 tot 5 jaar
   - ◯ > 5 jaar

3. **3. Bent u een interne of externe medewerker?** *
   Markeer slechts één ovaal.

   - ◯ Intern
   - ◯ Extern

4. **4. Worden nieuwe medewerkers gescreend voor ze worden aangenomen?** *
Markeer slechts één ovaal.

- ◯ Ja
- ◯ Nee
- ◯ Weet ik niet
- ◯ Anders

5. **5. Op welke onderstaande aspecten worden nieuwe medewerkers gescreend?** *
Vink alle toepasselijke opties aan.

- ☐ Controle positieve referenties
- ☐ Controle curriculum vitae
- ☐ Onafhankelijke identiteitscontrole
- ☐ Controle Kredietwaardigheid
- ☐ Bevestiging van diploma's/certificaten
- ☐ Verklaring omtrent goed gedrag
- ☐ Weet ik niet
- ☐ Anders

6. **6. Heeft u toegang tot vertrouwelijke informatie vanuit uw functie?** *
Markeer slechts één ovaal.

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

Vragen informatiebeveiliging

7. **7. Met welke onderstaande informatiebeveiligingsdocumenten bent u inhoudelijk bekend?** *
Vink alle toepasselijke opties aan.

- ☐ Baseline informatiebeveiliging Rijksdienst (BIR)
- ☐ ISO 27001 of ISO 27002
- ☐ Hand-out informatiebeveiliging
- ☐ Geen van allen

8. **8. Voor welke aspecten heeft de organisatie een beveiligingsbeleid** *
   Vink alle toepasselijke opties aan.

   - [ ] Wachtwoordmanagement
   - [ ] Anti-virus/-phishing
   - [ ] Change management
   - [ ] Informatieclassificatie
   - [ ] Documentafhandeling/-vernietiging
   - [ ] Clean desk
   - [ ] Locken van computer
   - [ ] Weet ik niet

9. **9. Bent u in staat aan te geven welke informatie vertrouwelijk is op uw afdeling?** *
   Markeer slechts één ovaal.

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

10. **10. Wie is binnen uw organisatie en/of afdelingen verantwoordelijk voor het uitvoeren en controleren van het informatiebeveiligingsbeleid?** *
    Markeer slechts één ovaal.

    - ◯ De afdeling Beveiliging
    - ◯ Het lijnmanagement
    - ◯ De directie in combinatie met het MT
    - ◯ Weet ik niet

11. **11. Heeft u ooit vanuit deze organisatie een cursus/training aangeboden gekregen inzake informatiebeveiliging of social engineering?** *
    Markeer slechts één ovaal.

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

12. **12. Zou u, als u de mogelijkheid krijgt binnen de organisatie, een training volgen m.b.t. informatiebeveiliging / social engineering?** *
    Markeer slechts één ovaal.

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

13. **13. Met welke van de onderstaande aspecten wordt rekening gehouden bij het beëindigen of wijzigen van het dienstverband?** *
Vink alle toepasselijke opties aan.

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

14. **14. Bent u bekend hoe u dient om te gaan met een beveiligingsincident binnen uw afdeling / organisatie?** *
Markeer slechts één ovaal.

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

15. **15. Wordt het beveiligingsbeleid actief uitgedragen / verspreid binnen de afdeling en organisatie?** *
Markeer slechts één ovaal.

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

Vragen social engineering

Social Engineering is een verzamelnaam van aanvalstactieken en methoden, gericht op het manipuleren van medewerkers om zo toegang te verkrijgen tot vertrouwelijke bedrijfsinformatie.

16. **16. Bent u bekend met het begrip social engineering?** *
Markeer slechts één ovaal.

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

17. **17. Met welke van de onderstaande aanvallen bent u bekend?** *
Vink alle toepasselijke opties aan.

- [ ] Phishing - Via mail, telefoon hengelen naar informatie
- [ ] Dumpster diving - Doorzoeken van de prullenbak / afvalcontainer
- [ ] Office Snooping / Desk sniffing - Doorzoeken van een kantoor / werkplekken
- [ ] Piggyback / Tailgaiting - Met een andere persoon meelopen
- [ ] Baiting / Item dropping - Malware geïnfecteerd opslagmedium wordt bewust neergelegd/achtergelaten
- [ ] Malicious software - Malware, virus op de werkplek
- [ ] Reverse social engineering - De sympathieke hulp die je kan "helpen" bij een gecreëerde situatie/probleem.

18. **18. Kunt u beschrijven hoe een social engineeringsaanval wordt uitgevoerd?** *
Markeer slechts één ovaal.

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

19. **19. Bent u in de afgelopen 6 maanden benaderd via email, brief, telefonisch, social media, dan wel in persoon (fysiek), waarvan u denkt dat dit een poging was tot het verkrijgen van (gevoelige) bedrijfsinformatie ?** *
Markeer slechts één ovaal.

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

20. **20. Via welke kanalen werd deze poging ondernomen?** *
Vink alle toepasselijke opties aan.

- ☐ Email
- ☐ Telefoon
- ☐ Fysiek
- ☐ Social media (o.a. facebook, linkedin, whatsapp)
- ☐ Anders
- ☐ Wens ik niet te beantwoorden
- ☐ Niet benaderd / Niet van toepassing

21. **21. Bent u bekend met de meest voorkomende motieven van social engineers?** *
Markeer slechts één ovaal.

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

22. **22. Van welke menselijke aspecten maakt een social engineer misbruik?** *
Vink alle toepasselijke opties aan.

- ☐ Nalatigheid
- ☐ Slordigheid
- ☐ Onwetendheid
- ☐ Naiviteit
- ☐ Hebzucht
- ☐ Weet ik niet

23. **23. Hoe groot is de kans dat één of meerdere medewerkers van uw organisatie in een phishing mail trappen?** *

Markeer slechts één ovaal.

- Klein
- Middel
- Groot

24. **24. Hoe groot is de kans dat een persoon het gebouw van uw organisatie binnenkomt als deze zelf geen toegang heeft?** *

Markeer slechts één ovaal.

- Klein
- Middel
- Groot

25. **25. Hoe groot is de kans dat, wanneer een medewerker van uw organisatie een USB stick vindt, deze ook daadwerkelijk probeert te bekijken?** *

Markeer slechts één ovaal.

- Klein
- Middel
- Groot

Bijlage D: Interview vragen

Interview m.b.t. social engineering binnen de Rijksoverheid

Algemene vragen

1. *Wat is uw rol als IB functionaris (IBF) en kunt u deze in het kort omschrijven?*

2. *Hoeveel jaar bent u in dienst en hoeveel jaar vervult u de IBF rol voor uw afdeling?*

3. *Hoeveel medewerkers telt uw afdeling?*

Informatiebeveiligingsbeleid

4. *Hoe wordt binnen uw Rijksdienst omgegaan met informatiebeveiliging. Hoe wordt dit vastgelegd?*

5. *Hoe verhoudt het informatiebeveiligingsbeleid zich tot de BIR / ISO 27001 normering?*

6. *Zijn er directe of indirecte informatiebeveiligingsmaatregelen tegen social engineering vastgelegd in het huidige informatiebeleid van uw organisatie? Kunt u hiervan een voorbeeld geven?*

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

8. *Hoe gaat men binnen de organisatie om met het verwijderen van vertrouwelijke gegevens en/of documenten?*

9. *Worden medewerkers gescreend voordat deze aangenomen, op welke zaken?*

10. *Is er bij het beëindigen van een dienstverband controle op het retourneren van bedrijfsapparatuur, toegangspassen en het afsluiten van voorzieningen?*

11. *Hoe wordt omgegaan met een beveiligingsincident binnen uw afdeling/organisatie? Hoe worden incidenten afgewikkeld? Wordt er een incidentrapport opgemaakt na een beveiligingsinbreuk?*

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

13. *In hoeverre is uw directe lijnverantwoordelijke van uw organisatie betrokken bij het informatiebeveiligingsbeleid?*

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

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

16. *Is er het afgelopen jaar een controle/audit uitgevoerd op de beveiligingsbeleidspunten?*

Social engineering

17. *Wat verstaat u onder social engineering? Wat is de kern hiervan? Kunt u zich vinden in de volgende definities van social engineering?*

18. *Kunt u beschrijven hoe een social engineeringaanval in zijn werk gaat?*

19. *Welke motieven zou een social engineer kunnen hebben?*

20. *Bent u in staat om een aantal verschillende social engineeringsaanvallen te beschrijven?*

21. *Waar maakt een social engineer misbruik van?*

22. *Ziet u vanuit uw eigen medewerkers en/of externe partijen bedreigingen binnen de organisatie?*

23. *Zijn er recent incidenten geweest rondom social engineeringsaanvallen? Via welk (communicatie)kanaal werd deze poging ondernomen?*

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

25. *Is naar uw mening uw organisatie momenteel voldoende beschermd tegen social engineeringsaanvallen? Welke verbeteringen kunnen worden doorgevoerd?*

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

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

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

29. *Hoe groot is de kans dat wanneer een medewerker een data medium (USB stick, cdrom) vindt, deze ook daadwerkelijk bekijkt?*

30. *Weet je welke trends er spelen op het gebied van social engineering?*

31. *Reageert de organisatie snel genoeg op nieuwe ontwikkelingen, in dit geval social engineering. Is het een nieuwe ontwikkeling?*

Bijlage E: Uitgewerkte Interviews

Interview IBF 1 m.b.t. social engineering binnen de Rijksoverheid

Algemene vragen

1. *Wat is uw rol als IB functionaris (IBF) en kunt u deze in het kort omschrijven?*
   De IBF rol richt zich voornamelijk op het bijhouden en actualiseren van de BIR sheet met de IB maatregelen voor de afdeling.

2. *Hoeveel jaar bent u in dienst en hoeveel jaar vervult u de IBF rol voor uw afdeling?*
   24 jaar in dienst en 1 jaar als IBF voor de afdeling

3. *Hoeveel medewerkers telt uw afdeling?*
   10 medewerkers

Informatiebeveiligingsbeleid

4. *Hoe wordt binnen uw Rijksdienst omgegaan met informatiebeveiliging. Hoe wordt dit vastgelegd?*
   Op intranet is organisatiebreed het informatiebeveiligingsbeleid gepubliceerd, daarnaast legt elke afdeling haar eigen vorderingen en status op het vlak van de BIR vast in de BIR sheet. Voor de afdeling specifieke processen vindt tevens vastlegging plaats om aan bepaalde certificering te kunnen voldoen.

5. *Hoe verhoudt het informatiebeveiligingsbeleid zich tot de BIR / ISO 27001 normering?*
   Het BIR tactisch normenkader komt overeen met de ISO normering, daarnaast zijn er aanvullend Rijks specifieke maatregelen die worden met een R aangeduid in het kader. Het informatiebeveiligingsbeleid is breder en organisatie specifieker, wel is deze enigszins gedateerd.

6. *Zijn er directe of indirecte informatiebeveiligingsmaatregelen tegen social engineering vastgelegd in het huidige informatiebeleid van uw organisatie? Kunt u hiervan een voorbeeld geven?*
   Alleen in algemene zin, dat de mens een kwetsbare factor is. Er worden geen specifieke maatregelen genoemd op het vlak van social engineering.

7. *Wat is waardevolle informatie voor uw organisatie? Weten uw manager en de medewerkers dat? Is er binnen de organisatie bekend welke informatie het belangrijkst is?*
   Per afdeling is dat bewustzijn er zeker, medewerkers weten heel goed wat waardevolle informatie is. Het werken met vertrouwelijke informatie ligt besloten in de aard van de Rijksdienst, hierbij is geen onderscheid in leidinggevende en medewerkers.

8. *Hoe gaat men binnen de organisatie om met het verwijderen van vertrouwelijke gegevens en/of documenten?*

Papieren en andere informatiedragers worden apart ingezameld en volgens strikte werkwijze vernietigd.

9. *Worden medewerkers gescreend voordat deze aangenomen, op welke zaken?*
   Er is een controle bij het in diensttreden op het kunnen overleggen van een VOG, voor bepaalde vertrouwensfuncties ook nog een verklaring van geen bezwaar. Vanuit IBF rol geen zicht op welke checks HRM bij het in dienst treden uitvoert.

10. *Is er bij het beëindigen van een dienstverband controle op het retourneren van bedrijfsapparatuur, toegangspassen en het afsluiten van voorzieningen?*
    Er is een werkproces ingericht met stappen die doorlopen moeten worden, waaronder het inleveren van bedrijfsmiddelen, intrekken accounts, toegangspas ed.

11. *Hoe wordt omgegaan met een beveiligingsincident binnen uw afdeling/organisatie? Hoe worden incidenten afgewikkeld? Wordt er een incidentrapport opgemaakt na een beveiligingsinbreuk?*
    Op intranet staat beschreven op welke wijze beveiligingsincident gemeld moet worden. De leidinggevende maakt zelf de afweging of het meldenswaardig is of niet, in overleg met de afdeling Beveiliging wordt er dan een incidentrapport opgesteld.

12. *Wie is binnen uw organisatie en/of afdelingen verantwoordelijk voor het uitvoeren en controleren van het informatiebeveiligingsbeleid?*
    Binnen de afdeling is er een specifieke adviseur bedrijfsvoering die zich richt op het naleven en intern auditen van maatregelen. Tevens is er een organisatiebrede beveiligingscoördinator die verantwoordelijk is voor het opstellen en controleren van het beleid. De leidinggevende is uiteindelijke eindverantwoordelijk voor het beleid op de afdeling, de uitvoering en het voldoen aan BIR maatregelen.

13. *In hoeverre is uw directe lijnverantwoordelijke van uw organisatie betrokken bij het informatiebeveiligingsbeleid?*
    De leidinggevende is uiteindelijke eindverantwoordelijk voor het beleid op de afdeling, de uitvoering en het voldoen aan BIR maatregelen. Tweewekelijks vindt er afstemming plaatst met de leidinggevende, de IBF'er en de adviseur bedrijfsvoering over actuele en lopende zaken.

14. *Worden er risico analyses gemaakt op het informatiebeveiligingsbeleid? Wie is hier verantwoordelijk voor? Hoe vaak worden deze gemaakt?*
    De adviseur bedrijfsvoering maakt bij elke wijziging in werkprocessen op de afdeling een korte risico / impact analyse.

15. *Wordt het beveiligingsbeleid uitgedragen/verspreid binnen de afdeling en organisatie? Wordt op alle afdelingen het beleid op dezelfde manier uitgedragen?*
    Merendeel van het beveiligingsbeleid wordt organisatiebreed gepubliceerd op intranet, o.a. handboeken en ondersteunend materiaal. Daarnaast vinden er afdeling-overstijgende IBF overleggen plaats, waarin het IB beleid wordt besproken en bepaald onderwerpen/thema's worden uitgelicht om daar binnen de organisatie aandacht voor te vragen/creëren. Het oppakken, vervolgen hangt af van de relevantie, prioritering binnen de afdeling, de afstemming hierover is een samenspel van IBF'er en leidinggevende.

16. *Is er het afgelopen jaar een controle/audit uitgevoerd op de beveiligingsbeleidspunten?*
    De afdeling kent een aantal gecertificeerde processen die elk jaar worden ge-audit.

Social engineering

17. *Wat verstaat u onder social engineering? Wat is de kern hiervan? Kunt u zich vinden in de volgende definities van social engineering?*
    Het verleiden van mensen om bij hen vertrouwelijke informatie te ontfutselen. Dit kan bedrijfsinformatie zijn, maar ook persoonlijke informatie in de privésfeer.
    Beide definities samen dekken de lading en hebben in de kern de mens als zwakste schakel.
    Definitie 1 is breder omschreven, definitie 2 is agressiever, spreekt over aanvalstechniek en gaat specifieker over informatiesystemen.
    Beide definities vermelden niet wat de methoden en kanalen zijn die worden gebruikt, dit maakt dat het nu minder tastbaar wat social engineering nu precies is.

18. *Kunt u beschrijven hoe een social engineeringaanval in zijn werk gaat?*
    Het is heel breed, van een link via de mail, tot een “win”-actie die rond gaat via social media met het doel het verkrijgen van informatie.

19. *Welke motieven zou een social engineer kunnen hebben?*
    Voornamelijk criminele activiteiten, financieel gewin.

20. *Bent u in staat om een aantal verschillende social engineeringsaanvallen te beschrijven?*
    Voorbeeld van social engineering zoals phishing mail, meelopen, telefonisch benaderen, voordoen als iemand anders, “win”-acties via social media.

21. *Waar maakt een social engineer misbruik van?*
    Het misbruik van vertrouwen van mensen.

22. *Ziet u vanuit uw eigen medewerkers en/of externe partijen bedreigingen binnen de organisatie?*
    Nee, geen redenen om aan te nemen dat interne of externe medewerkers een bedreiging vormen.

23. *Zijn er recent incidenten geweest rondom social engineeringsaanvallen? Via welk (communicatie)kanaal werd deze poging ondernomen?*
    Nee.

24. *Is naar uw mening uw organisatie voldoende op de hoogte/bewust van social engineering?*
    Medewerkers zijn zich steeds meer bewust, alleen al door de berichtgeving in de media over ransomware en/of voorlichting door banken rondom phishing. Ook binnen het Rijk zijn er nu regelmatig bewustzijnscampagnes en worden proeven met phishing mail uitgevoerd. Op de afdeling hebben we ook met alle medewerker de phishing-test van de consumentenbond doorlopen.

25. *Is naar uw mening uw organisatie momenteel voldoende beschermd tegen social engineeringsaanvallen? Welke verbeteringen kunnen worden doorgevoerd?*
    In een onachtzaam moment is het altijd mogelijk dat een medewerker op een link klikt. Of het voldoende beschermd is blijft lastig, het gaat immers om het individuele gedrag. Het blijft nodig om regelmatig aandacht te vragen voor het onderwerp, zodat men alert blijft.

26. *Wat zijn de mogelijke gevolgen voor de organisatie als vertrouwelijke informatie op straat komt te liggen?*
    De vertrouwelijkheid van informatie is groot en daarmee de gevolgen van het eventueel uitlekken ook. Naast (politieke) reputatieschade en het beschadigde vertrouwen in het functioneren van de overheid , kan als de omvang aanzienlijk is ook het bestaansrecht van de organisatie in het geding komen.

27. *Hoe groot is de kans dat een medewerker in een phishing mailt trapt?*
    De kans is reëel, de mails worden steeds geavanceerder en lastiger te herkennen.

28. *Hoe groot is de kans dat een persoon het gebouw binnenkomt als deze zelf geen toegang heeft?*
    De kans is reëel, meelopen zou kunnen.

29. *Hoe groot is de kans dat wanneer een medewerker een data medium (USB stick, cdrom) vindt, deze ook daadwerkelijk bekijkt?*
    Dit is minder aannemelijk, het vraagt immers een bewuste handeling om de cdrom of stick te gaan bekijken.

30. *Weet je welke trends er spelen op het gebied van social engineering?*
    Er wordt meer gebruik gemaakt van social media, zoals facebook en whatsapp. Technieken worden geavanceerder, professioneler opgezet, waardoor het lastiger wordt deze te herkennen.

31. *Reageert de organisatie snel genoeg op nieuwe ontwikkelingen, in dit geval social engineering. Is het een nieuwe ontwikkeling?*
    De organisatie kent veel IT-technische professionals, die beroepsmatig al dergelijke ontwikkelingen volgen. Wel kan de organisatie zelf meer aandacht vragen voor het onderwerp en daarmee de kennis breder onder alle medewerkers verspreiden.

Interview IBF 2 m.b.t. social engineering binnen de Rijksoverheid

Algemene vragen

1. *Wat is uw rol als IB functionaris (IBF) en kunt u deze in het kort omschrijven?*
   Binnen deze afdeling zijn er twee IBF'ers, deze hebben naast het bijhouden en actualiseren van de BIR sheet met beveiligingsmaatregelen, ook een controlerende rol bij voorgestelde van wijzigingen op de IT infrastructuur.

2. *Hoeveel jaar bent u in dienst en hoeveel jaar vervult u de IBF rol voor uw afdeling?*
   7 jaar in dienst en 1,5 jaar als IBF'er voor de afdeling.

3. *Hoeveel medewerkers telt uw afdeling?*
   12 medewerkers

Informatiebeveiligingsbeleid

4. *Hoe wordt binnen uw Rijksdienst omgegaan met informatiebeveiliging. Hoe wordt dit vastgelegd?*
   De Rijksbrede BIR maatregelen zijn opgenomen in een BIR excelsheet, waarin elke afdeling haar eigen vorderingen en status op het vlak van de BIR vastlegt. De BIR sheet fungeert als een index, waarin naast de status van maatregelen, ook een verwijzing is opgenomen naar de onderliggende documentatie/wiki naar de feitelijke invulling van de maatregelen.

5. *Hoe verhoudt het informatiebeveiligingsbeleid zich tot de BIR / ISO 27001 normering?*
   De BIR is een Rijks specifieke vertaling van de ISO 27001 normering. Daarnaast heeft de organisatie haar eigen afwegingen te maken, deze invulling vormt het organisatie specifieke informatiebeveiligingsbeleid. Denk aan operationele risicoafwegingen die samenhangen met functiescheiding maatregelen en of invulling van toegangsbeleid.

6. *Zijn er directe of indirecte informatiebeveiligingsmaatregelen tegen social engineering vastgelegd in het huidige informatiebeleid van uw organisatie? Kunt u hiervan een voorbeeld geven?*
   Er zijn, voor zover ik weet, geen direct expliciete beleidsmaatregelen die samenhangen met social engineering.

7. *Wat is waardevolle informatie voor uw organisatie? Weten uw manager en de medewerkers dat? Is er binnen de organisatie bekend welke informatie het belangrijkst is?*
   Alle informatie die binnen de organisatie wordt verwerkt heeft het kenmerk departementeel vertrouwelijk. Iedereen die werkzaam is binnen deze Rijksdienst is daar van op de hoogte en bewust van de waarde die dat heeft en hoe daar mee om te gaan.

8. *Hoe gaat men binnen de organisatie om met het verwijderen van vertrouwelijke gegevens en/of documenten?*
   Vertrouwelijke informatie wordt via aparte papiercontainers vernietigd. Informatiedragers worden apart ingezameld en volgens procedure vernietigd. Het verwijderen van informatie

in informatiesystemen kan alleen door geautoriseerde personen met geregistreerde verzoeken.

9. *Worden medewerkers gescreend voordat deze aangenomen, op welke zaken?*
   Er is een controle bij het in diensttreden op het kunnen overleggen van een VOG.
   Geen beleid op het checken van diploma's en referenties, dit verschilt per leidinggevende / afdeling.

10. *Is er bij het beëindigen van een dienstverband controle op het retourneren van bedrijfsapparatuur, toegangspassen en het afsluiten van voorzieningen?*
    Er is een werkproces ingericht met stappen die doorlopen moeten worden, waaronder het inleveren van bedrijfsmiddelen, intrekken accounts, toegangspas ed. Niet altijd verloopt dit vlekkeloos, met name verzoek tot het intrekken van accounts bereikt niet altijd de beheerders.

11. *Hoe wordt omgegaan met een beveiligingsincident binnen uw afdeling/organisatie? Hoe worden incidenten afgewikkeld? Wordt er een incidentrapport opgemaakt na een beveiligingsinbreuk?*
    De medewerkers toetsen over het algemeen met de leidinggevende of het meldenswaardig is of niet, in overleg met de afdeling Beveiliging wordt er dan een incidentrapport opgesteld.

12. *Wie is binnen uw organisatie en/of afdelingen verantwoordelijk voor het uitvoeren en controleren van het informatiebeveiligingsbeleid?*
    De leidinggevende is conform de BIR verantwoordelijk voor het beleid op de afdeling, de uitvoering en het voldoen aan BIR maatregelen. Controle op het beleid vindt plaats d.m.v. (interne) audits.

13. *In hoeverre is uw directe lijnverantwoordelijke van uw organisatie betrokken bij het informatiebeveiligingsbeleid?*
    De leidinggevende prioriteert inzet en is eindverantwoordelijk op voortgang van de uitvoering. De inhoudelijk invulling van het beleid en initiatie vindt veelal plaats vanuit afdeling Beveiliging.

14. *Worden er risico analyses gemaakt op het informatiebeveiligingsbeleid? Wie is hier verantwoordelijk voor? Hoe vaak worden deze gemaakt?*
    Operationele risicoafwegingen op beveiligingsaspecten vinden veelal plaats in de projecten en de ingediende wijzigingsverzoeken. Daarnaast heeft de afdeling een adviesrol op nieuw te vormen beveiligingsbeleid.

15. *Wordt het beveiligingsbeleid uitgedragen/verspreid binnen de afdeling en organisatie? Wordt op alle afdelingen het beleid op dezelfde manier uitgedragen?*
    In het IBF-overleg vindt afstemming plaats over mogelijk onderwerpen die aandacht verdienen binnen de organisatie. De boodschap moet hetzelfde zijn, maar binnen de afdeling kan het wel anders worden gebracht. Dit hangt sterk af van de heersende veiligheidscultuur en de gewoontes van een afdeling.

16. *Is er het afgelopen jaar een controle/audit uitgevoerd op de beveiligingsbeleidspunten?*

Eén keer per jaar wordt de balans opgemaakt van de status van de verschillende afdelingsspecifieke BIR sheets.

Social engineering

17. *Wat verstaat u onder social engineering? Wat is de kern hiervan? Kunt u zich vinden in de volgende definities van social engineering?*
    Door sociale interactie kennis vergaren, waarmee het mogelijk wordt gevoelige bedrijfsinformatie te verkrijgen. Dit kan op tal van wijzen, directe (telefonische) benadering, linkjes via mail, briefjes achterlaten, etc.
    Beide definities dekken de lading, niet direct iets aan toe te voegen.

18. *Kunt u beschrijven hoe een social engineeringaanval in zijn werk gaat?*
    Je zoekt kontakt op een bepaalde manier, prikt op zoek naar zwakheden en probeert verschillende wijzen, net zolang tot je binnen bent.

19. *Welke motieven zou een social engineer kunnen hebben?*
    Elke motief die een reguliere hacker zou hebben, zoals financieel gewin, informatie vergaren wraak actie. Met de hedendaagse technische beveiligingsmaatregelen vormt social engineering een logische en laagdrempelige werkwijze om toch door de “beveiligde” lagen aan informatie te kunnen komen.

20. *Bent u in staat om een aantal verschillende social engineeringsaanvallen te beschrijven?*
    Dat kan op tal van wijzen, overal waar interactie met mensen mogelijk is, zoals door het bellen of mailen met valse voorwendselen, het gericht benaderen, reclame maken met lokkertjes, voordoen als iemand anders.

21. *Waar maakt een social engineer misbruik van?*
    De social engineer maakt misbruik van alles wat een mens beweegt, emoties. De nieuwsgierigheid van mensen, inspelen op gevoelens, misbruiken van empathie, maar ook plat financieel gewin / verleiding.

22. *Ziet u vanuit uw eigen medewerkers en/of externe partijen bedreigingen binnen de organisatie?*
    Ik denk dat iedereen ontvankelijk is, mits je maar het juiste drukpunt weet te vinden. Nu weten medewerkers wel dat we hier in een gevoelige omgeving werken en niet op elke “goed” verhaal moeten in gaan.

23. *Zijn er recent incidenten geweest rondom social engineeringsaanvallen? Via welk (communicatie)kanaal werd deze poging ondernomen?*
    Nee, niet dat ik weet.

24. *Is naar uw mening uw organisatie voldoende op de hoogte/bewust van social engineering?*
    Ik denk het niet. Er is recent vanuit het Rijk een bewustzijnscampagne met phishing mail uitgevoerd, dit is een goede eerste stap, er moet veel meer aan bewustzijn worden gedaan.

25. *Is naar uw mening uw organisatie momenteel voldoende beschermd tegen social engineeringsaanvallen? Welke verbeteringen kunnen worden doorgevoerd?*
    Aanvullend op de vorige vraag, de bewustwordingscampagnes moeten meer worden ingezet, denk ook aan het gebruik van voorlichtingsfilmpjes.

26. *Wat zijn de mogelijke gevolgen voor de organisatie als vertrouwelijke informatie op straat komt te liggen?*
    Het effect van het uitlekken van informatie is voor direct betrokkene groot. De gevolgen van het uitlekken kunnen ook het vertrouwen in de Rijksdienst / Overheid schaden.

27. *Hoe groot is de kans dat een medewerker in een phishing mailt trapt?*
    De kans is groot, n.a.v. de phishing mail campagne bleek op de proxy dat tientallen de link hadden aangeklikt. Door actief IT ingrijpen tijdens de lopende Rijksbrede phishing campagne, werd de website tijdelijk geblokkeerd en zijn de uiteindelijke campagneresultaten voor deze organisatie hierdoor helaas positief vertekend.

28. *Hoe groot is de kans dat een persoon het gebouw binnenkomt als deze zelf geen toegang heeft?*
    De kans is reëel, het succesvol meelopen met groepen rondom pauzes is zeer aannemelijk.

29. *Hoe groot is de kans dat wanneer een medewerker een data medium (USB stick, cdrom) vindt, deze ook daadwerkelijk bekijkt?*
    Dit is niet reëel, de werkplekken hebben geen cd-drive en usb poorten meer.

30. *Weet je welke trends er spelen op het gebied van social engineering?*
    Ik verwacht dat we meer social engineeringsaanvallen zullen zien in de toekomst, doordat de technische beveiliging toeneemt en “de mens” in verhouding relatief lastiger te beschermen en daarmee makkelijke te “kraken” is.

31. *Reageert de organisatie snel genoeg op nieuwe ontwikkelingen, in dit geval social engineering. Is het een nieuwe ontwikkeling?*
    Als organisatie loop je altijd achter de feiten aan, het is een wapenwedloop en daarom noodzakelijk de kennis over social engineeringmethoden onder alle medewerkers te verspreiden. Social engineering is van alle tijden, maar methoden evolueren en richt zich nu op het verkrijgen van toegang tot de gedigitaliseerde informatie / kennis.

Interview IBF 3 m.b.t. social engineering binnen de Rijksoverheid

Algemene vragen

1. *Wat is uw rol als IB functionaris (IBF) en kunt u deze in het kort omschrijven?*
   Als IBF'er het aanspreekpunt binnen de afdeling op het gebied van informatiebeveiliging. Een coördinerende rol op het vlak van de BIR en samen met de afdelingsmanager aanjager van bewustwording en sturen op maatregelen, zorgen dat het onderwerp leeft en op de kaart staat op de afdeling. Daarnaast ook afstemming over de afdeling heen met andere IBF'ers.

2. *Hoeveel jaar bent u in dienst en hoeveel jaar vervult u de IBF rol voor uw afdeling?*
   8 jaar in dienst en 2,5 jaar als IBF voor de afdeling

3. *Hoeveel medewerkers telt uw afdeling?*
   20 medewerkers

Informatiebeveiligingsbeleid

4. *Hoe wordt binnen uw Rijksdienst omgegaan met informatiebeveiliging. Hoe wordt dit vastgelegd?*
   Organisatiebreed is er een handboek beveiliging, zijn er IT beveiligingsmaatregelen, beveiligingsprocedures en regelingen. Daarnaast kunnen afdeling specifieke invullingen van de maatregelen hanteren, zoals omgang bijvoorbeeld rondom informatiesystemen en het gebruik / gedrag op de werkplek.

5. *Hoe verhoudt het informatiebeveiligingsbeleid zich tot de BIR / ISO 27001 normering?*
   Het handboek beveiliging is opgebouwd rondom de onderwerpen/hoofdstukken van de BIR. De BIR is een Rijks specifieke invulling van de ISO 27001 normering.

6. *Zijn er directe of indirecte informatiebeveiligingsmaatregelen tegen social engineering vastgelegd in het huidige informatiebeleid van uw organisatie? Kunt u hiervan een voorbeeld geven?*
   Er is niet direct een set aan maatregelen in de BIR aanwijsbaar, wel zitten in de verschillende individuele BIR maatregelen beschermende factoren die maken dat social engineering aanvallen niet of lastiger zijn uit te voeren. Besluitvorming in de procedures en processen maakt dat bijvoorbeeld alleen geautoriseerde personen wijzigingen kunnen initiëren.

7. *Wat is waardevolle informatie voor uw organisatie? Weten uw manager en de medewerkers dat? Is er binnen de organisatie bekend welke informatie het belangrijkst is?*
   Op basis van een quickscan BIR worden de risico's , dreigingen op de beschikbaarheid, integriteit en vertrouwelijkheid per informatiesysteem en haar omgeving geanalyseerd. Hieruit volgen de prioritering van maatregelen op en rondom een informatiesysteem. Deze afweging vindt plaats samen met de manager en de medewerkers op de afdeling.

8. *Hoe gaat men binnen de organisatie om met het verwijderen van vertrouwelijke gegevens en/of documenten?*
   Het verwijderen in informatiesystemen vindt plaats via de schermen door geautoriseerde medewerkers, of via een wijzigingsprocedure waarbij een geautoriseerde aan functioneel beheer opdracht tot verwijdering kan geven. Daarnaast vindt er geautomatiseerd een schoning conform de geldende regel en wetgeving plaats.

9. *Worden medewerkers gescreend voordat deze aangenomen, op welke zaken?*
   Er is een controle bij het in diensttreden op het kunnen overleggen van een VOG, en het kunnen overleggen van een ID.

10. *Is er bij het beëindigen van een dienstverband controle op het retourneren van bedrijfsapparatuur, toegangspassen en het afsluiten van voorzieningen?*
    Er is een procedure voor het inleveren van bedrijfsmiddelen, het intrekken van accounts, en de toegangspas.

11. *Hoe wordt omgegaan met een beveiligingsincident binnen uw afdeling/organisatie? Hoe worden incidenten afgewikkeld? Wordt er een incidentrapport opgemaakt na een beveiligingsinbreuk?*
    Het komt gelukkig niet zo heel vaak voor op onze afdeling. Belangrijk is dat we op de juiste wijze met alle betrokkenen communiceren. Om rondom een incident de juiste zorgvuldigheid te betrachten, overleggen we al vrij snel met de afdeling Beveiliging. Op basis van deze gezamenlijke afweging worden dan de eventuele vervolgstappen ingezet.

12. *Wie is binnen uw organisatie en/of afdelingen verantwoordelijk voor het uitvoeren en controleren van het informatiebeveiligingsbeleid?*
    De verantwoordelijk voor de uitvoering van informatiebeveiliging op de afdeling ligt bij de afdelingsmanager. Hiërarchisch volgt dan de lijn richting directie.
    Als IBF'er stuur en controleer ik op de inhoudelijke invulling van de BIR en rapporteren hierover richting de manager.

13. *In hoeverre is uw directe lijnverantwoordelijke van uw organisatie betrokken bij het informatiebeveiligingsbeleid?*
    De leidinggevende is uiteindelijke eindverantwoordelijk voor het beleid op de afdeling, de uitvoering en het voldoen aan BIR maatregelen. In onderling overleg tussen manager en IBF'er vindt er afstemming plaatst over de invulling van het informatiebeveiligingsbeleid op de afdeling.

14. *Worden er risico analyses gemaakt op het informatiebeveiligingsbeleid? Wie is hier verantwoordelijk voor? Hoe vaak worden deze gemaakt?*
    Minimaal één keer in de drie jaar wordt er rondom de informatiesystemen een quickscan BIR uitgevoerd, waarbij de potentiele risico's en de BIR maatregelen als baseline opnieuw worden vastgesteld. Daarnaast prioriteren we de kosten/baten afweging van de te nemen BIR maatregelen op basis van deze vastgestelde risico's.

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

Het beveiligingsbeleid wordt organisatiebreed gepubliceerd via intranet, of mail verspreid. Binnen de IBF overleggen worden onderwerpen behandeld met als doel hierin gezamenlijk op te trekken en uit te dragen. Het oppakken, vervolgen binnen de afdeling hangt ook af van de wijze van het zelf invulling geven aan de IBF rol, i.o.m. je leidinggevende.

16. *Is er het afgelopen jaar een controle/audit uitgevoerd op de beveiligingsbeleidspunten?*
    Nee er vindt geen audit plaats dit jaar, wel heeft er een collegiale peer review plaats gevonden op onderdelen van de BIR.

Social engineering

17. *Wat verstaat u onder social engineering? Wat is de kern hiervan? Kunt u zich vinden in de volgende definities van social engineering?*
    Op basis van sociale contacten het ongeautoriseerde toegang verkrijgen tot vertrouwelijke informatie.
    Beide definities benoemen de mens als zwakste schakel. Definitie 1 is passiever en methodisch omschreven, definitie 2 is actiever en spreekt over aanvalstechnieken. Geen voorkeur of aanvullingen op de definities, beide zijn compleet/goed.

18. *Kunt u beschrijven hoe een social engineeringaanval in zijn werk gaat?*
    Een social engineeringsaanval kenmerkt zich vooral door het planmatige en langdurige karakter, waarbij men de tijd neemt om op slinkse wijze vertrouwen te winnen, om vervolgens toe te kunnen slaan.

19. *Welke motieven zou een social engineer kunnen hebben?*
    Geld is een motief, maar ook het kunnen manipuleren van informatie in de informatiesystemen van de Rijksoverheid.

20. *Bent u in staat om een aantal verschillende social engineeringsaanvallen te beschrijven?*
    Voorbeelden van social engineering zoals phishing mail, voordoen als iemand anders, verleiden tot het aanklikken van ransomware.

21. *Waar maakt een social engineer misbruik van?*
    Het misbruik van vertrouwen van mensen, maar ook onachtzaamheid.

22. *Ziet u vanuit uw eigen medewerkers en/of externe partijen bedreigingen binnen de organisatie?*
    Nee, geen redenen om aan te nemen dat interne of externe medewerkers een bedreiging vormen.

23. *Zijn er recent incidenten geweest rondom social engineeringsaanvallen? Via welk (communicatie)kanaal werd deze poging ondernomen?*
    Nee.

24. *Is naar uw mening uw organisatie voldoende op de hoogte/bewust van social engineering?*
    Medewerkers zijn zich steeds bewuster. Op de afdeling hebben we met alle medewerkers een IB training gevolgd, waarin ook social engineering aan bod kwam.

Daarnaast zijn er binnen het Rijk regelmatig bewustzijnscampagnes en worden phishing mail testen gehouden.

25. *Is naar uw mening uw organisatie momenteel voldoende beschermd tegen social engineeringsaanvallen? Welke verbeteringen kunnen worden doorgevoerd?*
    Over het algemeen wel. Verbeteringen zijn mogelijk door het generiek maken van de identificatie en authenticatieprocedures, nu is dit nog informatiesysteem specifiek. Het zou goed zijn als dit een generieke werkwijze werd voor alle informatiesystemen.

26. *Wat zijn de mogelijke gevolgen voor de organisatie als vertrouwelijke informatie op straat komt te liggen?*
    De gevolgen van het uitlekken van het informatie liggen op vlak van het beschadigde vertrouwen in de overheid en kan ook politieke consequenties hebben. Daarnaast kan de persoonsinformatie van betrokkenen ook burgers schaden in hun persoonlijke levenssfeer.

27. *Hoe groot is de kans dat een medewerker in een phishing mailt trapt?*
    De kans is klein, de meeste medewerker zijn zich na de phishing campagnes wel bewust op het zomaar klikken op linkjes in mails.

28. *Hoe groot is de kans dat een persoon het gebouw binnenkomt als deze zelf geen toegang heeft?*
    De kans op deze afdeling is klein, medewerkers zullen een onbekend persoon snel aanspreken. Om het gebouw binnen te komen is een toegangspas nodig.

29. *Hoe groot is de kans dat wanneer een medewerker een data medium (USB stick, cdrom) vindt, deze ook daadwerkelijk bekijkt?*
    Ik acht de kans niet groot, maar durf het niet uit te sluiten. Zeker als het een type stick is die intern ook wordt gebruikt, dan kan de nieuwsgierigheid het winnen van de bedachtzaamheid.

30. *Weet je welke trends er spelen op het gebied van social engineering?*
    De hoeveelheid aan phishing mails neemt toe, ook prive.

31. *Reageert de organisatie snel genoeg op nieuwe ontwikkelingen, in dit geval social engineering. Is het een nieuwe ontwikkeling?*
    Ja, er is meer aandacht voor informatiebeveiliging dan een paar jaar terug. Er worden meer voorlichting sessies gehouden, mensen zijn zich bewuster en weten hoe te handelen.

Interview IBF 4 m.b.t. social engineering binnen de Rijksoverheid

Algemene vragen

1. *Wat is uw rol als IB functionaris (IBF) en kunt u deze in het kort omschrijven?*
   De IBF'er ondersteunt de afdelingsmanager bij het uitvoeren van het informatiebeveiligingsbeleid op de afdeling, adviseert in deze en stemt af over de BIR maatregelen.

2. *Hoeveel jaar bent u in dienst en hoeveel jaar vervult u de IBF rol voor uw afdeling?*
   17 jaar in dienst en 2,5 jaar als IBF voor de afdeling

3. *Hoeveel medewerkers telt uw afdeling?*
   40 medewerkers

Informatiebeveiligingsbeleid

4. *Hoe wordt binnen uw Rijksdienst omgegaan met informatiebeveiliging. Hoe wordt dit vastgelegd?*
   Er zijn een aantal voorschriften en kaders waaraan de organisatie moet voldoen, o.a. de VIR, VIRBI, BIR. Op intranet is het actuele informatiebeveiligingsbeleid gepubliceerd, waarin een organisatie specifieke vertaling is gemaakt van genoemde richtlijnen.

5. *Hoe verhoudt het informatiebeveiligingsbeleid zich tot de BIR / ISO 27001 normering?*
   De BIR is één van de kaders binnen het informatiebeveiligingsbeleid van de organisatie.

6. *Zijn er directe of indirecte informatiebeveiligingsmaatregelen tegen social engineering vastgelegd in het huidige informatiebeleid van uw organisatie? Kunt u hiervan een voorbeeld geven?*
   Het bewustzijn in algemene zin onder medewerkers vergroten, en specifiek op het vlak van bijvoorbeeld phishing met phishingmail campagnes. Daarnaast is bewustzijn een terugkerend onderwerp op het IBF overleg en worden deze daarbinnen besproken. Daarnaast ook aandacht vragen voor het melden van voorvallen bij beveiliging, zodat mogelijke social engineeringsactiviteiten niet onopgemerkt blijven.

7. *Wat is waardevolle informatie voor uw organisatie? Weten uw manager en de medewerkers dat? Is er binnen de organisatie bekend welke informatie het belangrijkst is?*
   Alle informatie die in de primaire processystemen zit en persoonlijke informatie zoals bijvoorbeeld HRM gegevens, zijn vertrouwelijk en waardevol voor deze organisatie. Alle informatie die een persoon zou kunnen schaden, als deze wordt gedeeld. Mijn indruk is wel dat alle medewerkers zich bewust zijn van en weten welke informatie vertrouwelijk is.

8. *Hoe gaat men binnen de organisatie om met het verwijderen van vertrouwelijke gegevens en/of documenten?*
   Volgens wettelijke archiverings- en schoningstermijnen.

9. *Worden medewerkers gescreend voordat deze aangenomen, op welke zaken?*

Er is een controle bij het in diensttreden op het kunnen overleggen van een VOG, daarnaast controleert HRM de diploma's. Ook leggen nieuwe medewerkers de eed/belofte af.
Voor sommige functies binnen de Rijksdienst (bepaalde afdelingen) is de screening uitgebreider.

10. *Is er bij het beëindigen van een dienstverband controle op het retourneren van bedrijfsapparatuur, toegangspassen en het afsluiten van voorzieningen?*
    Er is een autorisatieproces ingericht met stappen die doorlopen moeten worden, waaronder het inleveren van bedrijfsmiddelen, intrekken accounts, toegangspas ed.

11. *Hoe wordt omgegaan met een beveiligingsincident binnen uw afdeling/organisatie? Hoe worden incidenten afgewikkeld? Wordt er een incidentrapport opgemaakt na een beveiligingsinbreuk?*
    Op intranet staat beschreven hoe en wanneer een beveiligingsincident gemeld kan worden. Over het algemeen maken medewerkers zelf melding, eventueel in overleg met leidinggevende en/of afdeling Beveiliging. Maandelijks wordt door Beveiliging van alle incidenten een incidentrapportage opgesteld.

12. *Wie is binnen uw organisatie en/of afdelingen verantwoordelijk voor het uitvoeren en controleren van het informatiebeveiligingsbeleid?*
    De leidinggevende is verantwoordelijk voor het beleid op de afdeling, de uitvoering en het voldoen aan BIR maatregelen. Het monitoren, controleren op de uitvoering van het beleid ligt bij de afdeling Beveiliging.

13. *In hoeverre is uw directe lijnverantwoordelijke van uw organisatie betrokken bij het informatiebeveiligingsbeleid?*
    De leidinggevende is uiteindelijke eindverantwoordelijk voor het beleid op de afdeling, de uitvoering en het voldoen aan BIR maatregelen. Daarnaast vindt er afstemming plaatst met de leidinggevende, de IBF'er en de afdeling Beveiliging over actuele en lopende zaken.

14. *Worden er risico analyses gemaakt op het informatiebeveiligingsbeleid? Wie is hier verantwoordelijk voor? Hoe vaak worden deze gemaakt?*
    Op de door te voeren BIR maatregelen vindt een prioritering o.b.v. risico's plaats. Dit is een continu proces, waarin wordt afgestemd met leidinggevende, andere afdelingen, afdeling Beveiliging en de IBF'ers.

15. *Wordt het beveiligingsbeleid uitgedragen/verspreid binnen de afdeling en organisatie? Wordt op alle afdelingen het beleid op dezelfde manier uitgedragen?*
    Het uitdragen/communiceren binnen de organisatie is een terugkerende thema tijdens de IBF overleggen. Hierbinnen wordt het IB beleid besproken en worden organisatiebrede communicatieonderwerpen bepaald, denk aan clean desk, locken van de werkplek, etc. Het oppakken binnen een afdeling hangt af van de ruimte die de leidinggevende hiervoor geeft.

16. *Is er het afgelopen jaar een controle/audit uitgevoerd op de beveiligingsbeleidspunten?*
    De afdeling kent een aantal werkprocessen die elk jaar worden gecontroleerd, hierin zitten ook een aantal BIR maatregelen, zoals bijvoorbeeld functiescheidingsmaatregelen.

Social engineering

17. *Wat verstaat u onder social engineering? Wat is de kern hiervan? Kunt u zich vinden in de volgende definities van social engineering?*
    Social engineering is het bewerkstelligen dat mensen informatie prijs geven die vertrouwelijk had moeten blijven. Dat kan van alles zijn, zoals het delen van pincodes, wachtwoorden, locaties of vertrouwelijke stukken.

    Definitie 1 is breder omschreven en slaat ook op de omgeving thuis, definitie 2 is specifieker zoals die ook in een Rijksorganisatie van toepassing is.

18. *Kunt u beschrijven hoe een social engineeringaanval in zijn werk gaat?*
    Het benaderen van een hele brede groep mensen, in de hoop zoveel mogelijk informatie te vergaren, waarmee het mogelijke wordt financieel voordeel te behalen of vertrouwelijke informatie te verkrijgen.

19. *Welke motieven zou een social engineer kunnen hebben?*
    Binnen deze organisatie het verkrijgen van vertrouwelijke informatie, daar buiten vermoedelijk eerder een financieel motief.

20. *Bent u in staat om een aantal verschillende social engineeringsaanvallen te beschrijven?*
    Voorbeeld van social engineering zoals phishing mail, telefonisch benaderen, voordoen als iemand anders, ook via social media, gebruiken van ‘fake’ online profielen.

21. *Waar maakt een social engineer misbruik van?*
    Het misbruik van het vertrouwen van mensen.

22. *Ziet u vanuit uw eigen medewerkers en/of externe partijen bedreigingen binnen de organisatie?*
    Nee, geen redenen om aan te nemen dat interne of externe medewerkers een bedreiging vormen. (En uiteraard zijn er wel maatregelen (vanuit allerlei kaders waaronder de BIR) om die bedreiging zo klein mogelijk te maken)

23. *Zijn er recent incidenten geweest rondom social engineeringsaanvallen? Via welk (communicatie)kanaal werd deze poging ondernomen?*
    Nee, niet dat ik weet.

24. *Is naar uw mening uw organisatie voldoende op de hoogte/bewust van social engineering?*
    Ja, volgens mij zijn medewerkers zijn zich steeds meer bewust. Vanuit het Rijk zijn er regelmatig bewustzijnscampagnes en phishing mail testen. Ook vanuit de IBF-groep hebben we regelmatig aandacht en communicatie over bewustzijn van gedragingen.

25. *Is naar uw mening uw organisatie momenteel voldoende beschermd tegen social engineeringsaanvallen? Welke verbeteringen kunnen worden doorgevoerd?*
    Of we technisch voldoende beschermd zijn, daar heb ik geen zicht op en kan ik niet inschatten. Wel denk ik dat we voldoende aan bewustwording doen en daarmee medewerkers alert houden.

26. *Wat zijn de mogelijke gevolgen voor de organisatie als vertrouwelijke informatie op straat komt te liggen?*
    De vertrouwelijkheid van informatie is groot en kan eventueel vermelde betrokkenen in de gelekte informatie persoonlijk schaden. Daarnaast is het mogelijk dat er reputatieschade is voor de Rijksdienst.

27. *Hoe groot is de kans dat een medewerker in een phishing mailt trapt?*
    Die kans acht ik niet zo groot meer, de laatste phishingcampagne liet weinig medewerkers zien die de link aan klikten. Belangrijk is wel hier structureel aandacht voor te blijven houden.

28. *Hoe groot is de kans dat een persoon het gebouw binnenkomt als deze zelf geen toegang heeft?*
    Niet groot. Kan nog wel verbeterd worden.

29. *Hoe groot is de kans dat wanneer een medewerker een data medium (USB stick, cdrom) vindt, deze ook daadwerkelijk bekijkt?*
    Ik verwacht niet dat medewerkers dit zullen doen, daarnaast is het volgens mij technisch ook niet mogelijk.

30. *Weet je welke trends er spelen op het gebied van social engineering?*
    De e-mails worden geavanceerder, professioneler opgezet, waardoor het lastiger wordt deze te herkennen.

31. *Reageert de organisatie snel genoeg op nieuwe ontwikkelingen, in dit geval social engineering. Is het een nieuwe ontwikkeling?*
    Ik verwacht van wel, binnen de organisatie zijn er IT professionals en adviseurs beveiliging, die beroepsmatig dergelijke ontwikkelingen volgen en nieuwe ontwikkelingen zullen signaleren. Daarnaast staat de organisatie niet alleen en krijgt het vanuit het Rijk ook de nodige informatie en ondersteuning op het vlak van informatiebeveiliging.

Interview IBF 5 m.b.t. social engineering binnen de Rijksoverheid

Algemene vragen

1. *Wat is uw rol als IB functionaris (IBF) en kunt u deze in het kort omschrijven?*
   De IBF rol is vooral procedureel van aard en richt zich voornamelijk op het actualiseren van de status van de BIR maatregelen. Ik had daar persoonlijk liever een meer technische inhoud en bijdrage in willen zien en is voor mij de reden om de rol neer te leggen.

2. *Hoeveel jaar bent u in dienst en hoeveel jaar vervult u de IBF rol voor uw afdeling?*
   7 jaar in dienst en 2 jaar als IBF voor de afdeling

3. *Hoeveel medewerkers telt uw afdeling?*
   20 medewerkers

Informatiebeveiligingsbeleid

4. *Hoe wordt binnen uw Rijksdienst omgegaan met informatiebeveiliging. Hoe wordt dit vastgelegd?*
   Elke afdeling documenteert haar eigen vorderingen op het vlak van de te nemen BIR maatregelen, deze status wordt vastgelegd in de BIR lijst/sheet.

5. *Hoe verhoudt het informatiebeveiligingsbeleid zich tot de BIR / ISO 27001 normering?*
   Ik ben onvoldoende bekend met het informatiebeveiligingsbeleid en durf dat niet te zeggen. Vanuit mijn rol lag de focus op de invulling van de technische BIR maatregelen.

6. *Zijn er directe of indirecte informatiebeveiligingsmaatregelen tegen social engineering vastgelegd in het huidige informatiebeleid van uw organisatie? Kunt u hiervan een voorbeeld geven?*
   Zou ik niet weten.

7. *Wat is waardevolle informatie voor uw organisatie? Weten uw manager en de medewerkers dat? Is er binnen de organisatie bekend welke informatie het belangrijkst is?*
   De kernsystemen bevatten de meeste waardevolle informatie voor de organisatie. De technische inrichting en het beheer kent een generiek model volgens veilige methoden /maatregelen, alle informatiesystemen liften hierop mee.

8. *Hoe gaat men binnen de organisatie om met het verwijderen van vertrouwelijke gegevens en/of documenten?*
   Geen zicht op/betrokkenheid bij het verwijderen van vertrouwelijke gegevens.

9. *Worden medewerkers gescreend voordat deze aangenomen, op welke zaken?*
   Er is een controle bij het in diensttreden of bij een tijdelijke opdracht, op het kunnen overleggen van een VOG.
   Vanuit IBF rol geen zicht op welke checks HRM bij het in dienst treden uitvoert.

10. *Is er bij het beëindigen van een dienstverband controle op het retourneren van bedrijfsapparatuur, toegangspassen en het afsluiten van voorzieningen?*
    Ja, accounts worden gedisabled bij het uitdienst treden. Op het inleveren van bedrijfsmiddelen heb ik geen zicht.

11. *Hoe wordt omgegaan met een beveiligingsincident binnen uw afdeling/organisatie? Hoe worden incidenten afgewikkeld? Wordt er een incidentrapport opgemaakt na een beveiligingsinbreuk?*
    Een incident op de afdeling wordt in de regel rechtstreeks gemeld bij de afdeling Beveiliging. De afdeling Beveiliging maakt een incidentrapport.

12. *Wie is binnen uw organisatie en/of afdelingen verantwoordelijk voor het uitvoeren en controleren van het informatiebeveiligingsbeleid?*
    De afdeling Beveiliging is verantwoordelijk voor het opstellen en controleren van het beleid. De leidinggevende is verantwoordelijk voor het beleid op de afdeling, de uitvoering en het voldoen aan BIR maatregelen.

13. *In hoeverre is uw directe lijnverantwoordelijke van uw organisatie betrokken bij het informatiebeveiligingsbeleid?*
    De leidinggevende heeft nu zelf de IBF rol opgenomen, maar is ook verantwoordelijk voor het beleid op de afdeling, de uitvoering en het voldoen aan BIR maatregelen.

14. *Worden er risico analyses gemaakt op het informatiebeveiligingsbeleid? Wie is hier verantwoordelijk voor? Hoe vaak worden deze gemaakt?*
    Geen zicht op.

15. *Wordt het beveiligingsbeleid uitgedragen/verspreid binnen de afdeling en organisatie? Wordt op alle afdelingen het beleid op dezelfde manier uitgedragen?*
    Het uitdragen van het beleid op deze afdeling is erg beperkt, wordt weinig aan gedaan. Mijn beeld is dat het op andere afdelingen actiever plaats vindt.

16. *Is er het afgelopen jaar een controle/audit uitgevoerd op de beveiligingsbeleidspunten?*
    Niet dat ik weet.

Social engineering

17. *Wat verstaat u onder social engineering? Wat is de kern hiervan? Kunt u zich vinden in de volgende definities van social engineering?*
    Social engineering speelt op meerdere vlakken, maar het draait om de persoon/medewerker die verleid wordt, bewust of onbewust om een bepaalde handeling uit te laten voeren.

    Definitie 1 is echt gericht op het verkrijgen van informatie, wat ik versta onder social engineering. Definitie 2 is beperkter, alleen gericht op informatiesystemen.

18. *Kunt u beschrijven hoe een social engineeringaanval in zijn werk gaat?*

Het is heel divers, van phishing en het verleiden op een link te klikken via de mail, maar ook "blind" bellen en een gesprek aanknopen, alles met als doel het verkrijgen van informatie.

19. *Welke motieven zou een social engineer kunnen hebben?*
    Binnen deze organisatie zou het bijvoorbeeld kunnen gaan om journalisten die informatie willen verkrijgen. Breder kan het gaan om bedrijfsgeheimen, financiële motieven.

20. *Bent u in staat om een aantal verschillende social engineeringsaanvallen te beschrijven?*
    Voorbeeld van social engineering zoals direct benadering en vragen om iets te mogen printen, phishing mails, meelopen, telefonisch of via facebook benaderen, voordoen als iemand anders.

21. *Waar maakt een social engineer misbruik van?*
    Het misbruik van de goedheid van de mens, de welwillendheid.

22. *Ziet u vanuit uw eigen medewerkers en/of externe partijen bedreigingen binnen de organisatie?*
    Nee, maar kan het ook niet uitsluiten.

23. *Zijn er recent incidenten geweest rondom social engineeringsaanvallen? Via welk (communicatie)kanaal werd deze poging ondernomen?*
    Nee, niet dat ik weet

24. *Is naar uw mening uw organisatie voldoende op de hoogte/bewust van social engineering?*
    Medewerkers zijn zich steeds meer bewust. De recente phishing mailtest draagt in ieder geval bij aan het bewustzijn en mogelijke werkwijzen en verleidingen die zich kunnen voordoen.

25. *Is naar uw mening uw organisatie momenteel voldoende beschermd tegen social engineeringsaanvallen? Welke verbeteringen kunnen worden doorgevoerd?*
    De recente phishing mailtest laat die zien dat de organisatie wel op dat vlak voldoende beschermd is geweest. Maar het blijft lastig, het gaat immers om het individueel gedrag en de aanval kan de volgende keer weer anders zijn. Het blijft noodzakelijk om regelmatig aandacht te vragen op verschillende wijzen, in andere vormen, zodat de alertheid blijft.

26. *Wat zijn de mogelijke gevolgen voor de organisatie als vertrouwelijke informatie op straat komt te liggen?*
    Gevolgen liggen in mogelijke politieke verantwoording, het beschadigde vertrouwen en imagoschade voor de organisatie en de overheid als geheel.

27. *Hoe groot is de kans dat een medewerker in een phishing mailt trapt?*
    Acht de kans niet groot, er is voldoende alertheid op phishing.

28. *Hoe groot is de kans dat een persoon het gebouw binnenkomt als deze zelf geen toegang heeft?*
    De kans is reëel, meelopen zou kunnen. De organisatie is groot genoeg om niet iedereen te kunnen kennen.

29. *Hoe groot is de kans dat wanneer een medewerker een data medium (USB stick, cdrom) vindt, deze ook daadwerkelijk bekijkt?*
    Dit is minder aannemelijk, een losliggende USB stick is te verdacht. Maar in een andere vorm, het uitdelen van USB – gadgets, zou de verleiding wel kunnen vergroten.

30. *Weet je welke trends er spelen op het gebied van social engineering?*
    Technieken worden geavanceerder, mailings zijn professioneler opgezet, waardoor het lastiger wordt deze te herkennen.

31. *Reageert de organisatie snel genoeg op nieuwe ontwikkelingen, in dit geval social engineering. Is het een nieuwe ontwikkeling?*
    De organisatie kent veel IT-technische maatregelen, die de organisatie wel voor de meeste aanvallen beschermd. Wel is het nodig regelmatig aandacht te vragen voor het menselijke aspect, en ook andere vormen en/of methoden van social engineering te belichten.

Interview IBF 6 m.b.t. social engineering binnen de Rijksoverheid

Algemene vragen

1. *Wat is uw rol als IB functionaris (IBF) en kunt u deze in het kort omschrijven?*
   Ik zie mijn IBF rol breder dan strikt de gemiddelde IBF invulling, naast het bijdragen aan de BIR maatregelen op en voor de afdeling, vervul ik ook een beveiligingstechnisch adviserende rol in de diensten die we leveren.

2. *Hoeveel jaar bent u in dienst en hoeveel jaar vervult u de IBF rol voor uw afdeling?*
   7 jaar in dienst en 2 jaar als IBF voor de afdeling

3. *Hoeveel medewerkers telt uw afdeling?*
   Ca. 30 medewerkers

Informatiebeveiligingsbeleid

4. *Hoe wordt binnen uw Rijksdienst omgegaan met informatiebeveiliging. Hoe wordt dit vastgelegd?*
   De organisatie heeft haar eigen informatiebeveiligingsbeleid, dat aanhaakt op het bredere Rijksbeleid. Daarbinnen kent elke afdeling haar diensten waarvoor de status op het vlak van de BIR maatregelen wordt ingeregeld en bijgehouden. Sommige diensten of processen moeten tevens aan bepaalde specifiekere informatiebeveiligingscertificeringen voldoen, zoals bijvoorbeeld de ETSI normering.

5. *Hoe verhoudt het informatiebeveiligingsbeleid zich tot de BIR / ISO 27001 normering?*
   Het informatiebeveiligingsbeleid is een organisatie specifieke invulling, hierin staan veelal bepalingen / vertalingen van het Rijksbeleid. Het BIR tactisch normenkader komt overeen met de ISO normering, daarnaast zijn er aanvullend Rijks specifieke maatregelen die worden met een R aangeduid in het kader.

6. *Zijn er directe of indirecte informatiebeveiligingsmaatregelen tegen social engineering vastgelegd in het huidige informatiebeleid van uw organisatie? Kunt u hiervan een voorbeeld geven?*
   Niet in het informatiebeveiligingsbeleid van de organisatie, wel in het afdelingsspecifieke beleid rondom de gecertificeerde diensten, waarin specifieke maatregelen worden benoemd op het vlak van social engineering.

7. *Wat is waardevolle informatie voor uw organisatie? Weten uw manager en de medewerkers dat? Is er binnen de organisatie bekend welke informatie het belangrijkst is?*
   Dat verschilt per afdeling en de diensten, denk aan de in de informatiesystemen opgeslagen privacygevoelige gegevens, maar ook blauwdrukken van IT diensten, of kennis van processen en /of werkwijzen. Het werken met vertrouwelijke informatie binnen een Rijksdienst mag bij medewerkers en leidinggevenden als algemeen bekend worden beschouwd.

8. *Hoe gaat men binnen de organisatie om met het verwijderen van vertrouwelijke gegevens en/of documenten?*
   Documenten en andere vertrouwelijke papieren worden via aparte containers ingezameld en vernietigd. Procedures voor het vernietigen van digitale gegevens hangt samen met de dienstverlening rondom een specifiek informatiesysteem, en vindt meestal via geautoriseerde wijzigingsverzoeken plaats.

9. *Worden medewerkers gescreend voordat deze aangenomen, op welke zaken?*
   Bij het in diensttreden is het kunnen overleggen van een VOG noodzakelijk. Ik heb zelf geen zicht op eventuele controle van referenties en/of diploma's.

10. *Is er bij het beëindigen van een dienstverband controle op het retourneren van bedrijfsapparatuur, toegangspassen en het afsluiten van voorzieningen?*
    Dat weet ik niet, mij niet bekend of hierop een controle is.

11. *Hoe wordt omgegaan met een beveiligingsincident binnen uw afdeling/organisatie? Hoe worden incidenten afgewikkeld? Wordt er een incidentrapport opgemaakt na een beveiligingsinbreuk?*
    Van een beveiligingsincident wordt altijd melding gemaakt bij de afdeling Beveiliging. Daarnaast zijn er specifieke procedures voor het melden van datalekken aan verschillende instanties, zoals het Agentschap Telecom of de Autoriteit Persoonsgegevens. Het opstellen van een incidentrapport is in samenspraak met de afdeling Beveiliging.

12. *Wie is binnen uw organisatie en/of afdelingen verantwoordelijk voor het uitvoeren en controleren van het informatiebeveiligingsbeleid?*
    De leidinggevende is verantwoordelijk voor het beleid op de afdeling, de uitvoering en het voldoen aan BIR maatregelen.
    De afdeling Beveiliging richt op de controle van de beleidsmaatregelen, de IBF'er vervult hierbij een brug functie, door voor de afdeling de status van maatregelen bij te houden.

13. *In hoeverre is uw directe lijnverantwoordelijke van uw organisatie betrokken bij het informatiebeveiligingsbeleid?*
    De leidinggevende is verantwoordelijk voor de uitvoering van het beleid op de afdeling, maar binnen deze afdeling niet direct betrokken bij de invulling van maatregelen. Bij mij als IBF'er ligt de rol om te signaleren en zaken aan te kaarten binnen de afdeling, eventueel in afstemming met de leidinggevende. Twee maandelijks is er afstemming met de afdeling Beveiliging, de leidinggevende en de IBF'er om de voortgang en knelpunten in de uitvoering van het beleid te bespreken.

14. *Worden er risico analyses gemaakt op het informatiebeveiligingsbeleid? Wie is hier verantwoordelijk voor? Hoe vaak worden deze gemaakt?*
    Voor bepaalde gecertificeerde diensten vinden jaarlijks audits plaats, hierin zitten ook risicoafwegingen. Binnen het Rijk geldt er een driejaarlijkse cyclus met daarbinnen een risicoanalyse, het invullen van de maatregelen en het auditen op de BIR.

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

Het beveiligingsbeleid geldt organisatiebreed en is gepubliceerd op intranet, wel is deze gedateerd. Als afdeling hebben we tevens een eigen actueel informatiebeveiligingsbeleid, welke wordt gehanteerd om de gecertificeerde diensten te kunnen leveren. Ik heb geen zicht op wat andere afdeling doen en uitdragen.

16. *Is er het afgelopen jaar een controle/audit uitgevoerd op de beveiligingsbeleidspunten?*
    Ja, er heeft een audit plaats gevonden op het specifieke afdelingsinformatiebeveiligingsbeleid rondom de gecertificeerde diensten.

Social engineering

17. *Wat verstaat u onder social engineering? Wat is de kern hiervan? Kunt u zich vinden in de volgende definities van social engineering?*
    Social engineering draait om het gebruiken van de zwakheden van de mens, deze uit te buiten met als doel informatie te verkrijgen.

    Definitie 1 is breder omschreven, maar klinkt wat verouderd. Definitie 2 is moderner en gaat specifieker over informatie en de systemen. Beide definities laten in het midden wat nu interessante informatie is en wat het doel van het misbruik is.

18. *Kunt u beschrijven hoe een social engineeringaanval in zijn werk gaat?*
    Er zijn diverse methoden die passen binnen de term social engineering, van direct benadering, voordoen als iemand anders, meelopen, phishing mailing, ed.

19. *Welke motieven zou een social engineer kunnen hebben?*
    Binnen deze organisatie zal het voornamelijk zitten op het kunnen verkrijgen van vertrouwelijke informatie, zoals persoonsgegevens. Maar wellicht ook uit rancune.

20. *Bent u in staat om een aantal verschillende social engineeringsaanvallen te beschrijven?*
    Voorbeeld van social engineering zoals phishing mail, meelopen, telefonisch benaderen, voordoen als iemand anders, zie ook vraag 18.

21. *Waar maakt een social engineer misbruik van?*
    De goede wil van mensen, maar ook de gevoeligheid van de sociale druk/norm. Een mooi voorbeeld is het afspelen van een bandje van een huilende baby tijdens een gesprek met de helpdesk, de helpdeskmedewerker is onder deze druk eerder geneigd verificatiestappen te negeren en vertrouwelijke informatie zoals een account en wachtwoord vrij te geven.

22. *Ziet u vanuit uw eigen medewerkers en/of externe partijen bedreigingen binnen de organisatie?*
    Nee, geen redenen om aan te nemen dat interne of externe medewerkers een bedreiging vormen.

23. *Zijn er recent incidenten geweest rondom social engineeringsaanvallen? Via welk (communicatie)kanaal werd deze poging ondernomen?*
    Nee, alleen de gecontroleerde “incidenten” vanuit de phishing mail test.

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

Medewerkers zijn zich voldoende bewust van phishing mails en het niet zomaar klikken op linkjes. Vanuit het Rijk worden er nu regelmatig bewustzijnscampagnes en worden proeven met phishing mail uitgevoerd.
Maar social engineering is veel breder, benadruk ook andere minder bekende vormen. De organisatie is te groot om iedere collega te kennen, maak medewerkers daarom ook bewust van het risico op het niet aanspreken bij meelopen. Of maak medewerkers bewust op het direct of telefonisch benaderen met een plausibel verhaal en hoe misbruik te herkennen / voorkomen.

25. *Is naar uw mening uw organisatie momenteel voldoende beschermd tegen social engineeringsaanvallen? Welke verbeteringen kunnen worden doorgevoerd?*
    Technisch zijn er tal van maatregelen getroffen, waardoor bijvoorbeeld phishing of andere online scam niet zo makkelijk de organisatie zal binnen komen. Maar via andere meer persoonlijke kanalen is het afschermen een stuk lastiger, en zal vooral geïnvesteerd moeten worden in preventie door het voorlichten van medewerkers op het herkennen van andere vormen van social engineering.

26. *Wat zijn de mogelijke gevolgen voor de organisatie als vertrouwelijke informatie op straat komt te liggen?*
    De vertrouwelijkheid van informatie is groot en daarmee de gevolgen van het eventueel uitlekken ook. De gevolgen liggen in reputatieschade en mogelijke politieke consequenties op ministerieel niveau als het gaat om het functioneren van de organisatie.

27. *Hoe groot is de kans dat een medewerker in een phishing mailt trapt?*
    De kans is klein, recente phishing mail test liet weinig response zien.

28. *Hoe groot is de kans dat een persoon het gebouw binnenkomt als deze zelf geen toegang heeft?*
    De kans is reëel, meelopen is mogelijk. Ook het aantrekken van een hesje van een schoonmaker laat waarschijnlijk deuren openen.

29. *Hoe groot is de kans dat wanneer een medewerker een data medium (USB stick, cdrom) vindt, deze ook daadwerkelijk bekijkt?*
    Ik ben bang dat de nieuwsgierigheid het wint van het logisch nadenken en de kans reëel is dat een medewerkers dit gaat bekijken.

30. *Weet je welke trends er spelen op het gebied van social engineering?*
    Technieken worden geavanceerder, waardoor het lastiger wordt deze te herkennen. Het wordt steeds professioneler, er zit geld achter, waardoor het is een business geworden om bedrijven gericht te benaderen. Waterholing lijkt toe te nemen, het creëren van specifieke websites om zo specifieke doelgroepen aan te spreken/lokken.

31. *Reageert de organisatie snel genoeg op nieuwe ontwikkelingen, in dit geval social engineering. Is het een nieuwe ontwikkeling?*
    Social engineering is zeker geen nieuw fenomeen. De recente bewustheidscampagnes zijn een goede beweging, maar hadden mijn ziens al veel eerder plaatst moeten vinden.

Interview IBF 7 m.b.t. social engineering binnen de Rijksoverheid

Algemene vragen

1. *Wat is uw rol als IB functionaris (IBF) en kunt u deze in het kort omschrijven?*
   De IBF rol binnen deze afdeling vervul ik samen met een collega. We richten ons op het bijhouden en implementeren van de BIR maatregelen op de te ontwikkelen producten en diensten. Daarbij hoort ook het bijhouden en actualiseren van de BIR sheet met de IB maatregelen voor de afdeling en het afstemming met collega IBF'ers over organisatiebrede onderwerpen.

2. *Hoeveel jaar bent u in dienst en hoeveel jaar vervult u de IBF rol voor uw afdeling?*
   3 jaar in dienst en 1,5 jaar als IBF voor de afdeling

3. *Hoeveel medewerkers telt uw afdeling?*
   Ca. 40 medewerkers

Informatiebeveiligingsbeleid

4. *Hoe wordt binnen uw Rijksdienst omgegaan met informatiebeveiliging. Hoe wordt dit vastgelegd?*
   De organisatie heeft een cluster Beveiliging, van waaruit de kaders en normen komen die samen het informatiebeveiligingsbeleid van de organisatie vormen. Daarnaast zijn er tal van richtlijnen gepubliceerd, over hoe je op een afdeling praktisch invulling kunt geven aan bepaalde normen. Elke afdeling onderhoud de vorderingen en status op het vlak van de BIR maatregelen in een zogenaamde BIR sheet.

5. *Hoe verhoudt het informatiebeveiligingsbeleid zich tot de BIR / ISO 27001 normering?*
   Het informatiebeveiligingsbeleid is organisatie specifiek en wordt getoetst aan het Rijkskader welke de BIR / ISO 27001 normering voorschrijft.

6. *Zijn er directe of indirecte informatiebeveiligingsmaatregelen tegen social engineering vastgelegd in het huidige informatiebeleid van uw organisatie? Kunt u hiervan een voorbeeld geven?*
   De term social engineering zei mij op het eerste oog niets, met het invullen van de survey en de gegeven toelichting werd mij duidelijk wat hiermee werd bedoeld. Er is, voor zover ik weet, geen specifiek beleid op het vlak van social engineering. Wel wordt er praktisch invulling gegeven aan bewustzijn, als onderwerp binnen het IBF overleg of door de phishing campagne.

7. *Wat is waardevolle informatie voor uw organisatie? Weten uw manager en de medewerkers dat? Is er binnen de organisatie bekend welke informatie het belangrijkst is?*
   De informatie binnen de Rijksdienst, veelal besloten in informatiesystemen, kent verschillende gradaties van vertrouwelijkheid. Het merendeel van de informatie waarmee gewerkt wordt is minimaal departementaal vertrouwelijk. De medewerkers, inhuur,

managers kennen deze vertrouwelijkheid, en zijn zich bewust van het werken in deze vertrouwelijke setting.

8. *Hoe gaat men binnen de organisatie om met het verwijderen van vertrouwelijke gegevens en/of documenten?*
   Voor het vernietigen van papieren informatie is er een werkprocedure, waarbij deze informatie apart wordt ingezameld en vernietigd. Bij digitaal opgeslagen informatie is mij niet duidelijk of hiervoor een procedure is, wel worden de gegevens met rechten afgeschermd en kan informatie niet zomaar worden verwijderd.

9. *Worden medewerkers gescreend voordat deze aangenomen, op welke zaken?*
   Een nieuwe medewerker of inhuur moeten een VOG kunnen overleggen. Het controleren van referenties en/of diploma's is niet standaard.

10. *Is er bij het beëindigen van een dienstverband controle op het retourneren van bedrijfsapparatuur, toegangspassen en het afsluiten van voorzieningen?*
    Rondom het uitdiensttreden is er een werkproces met formulieren, waarbij de leidinggevende een verzoek inschiet om vanaf een bepaalde datum de autorisaties in te trekken en eventuele apparatuur en toegangspassen in te nemen.

11. *Hoe wordt omgegaan met een beveiligingsincident binnen uw afdeling/organisatie? Hoe worden incidenten afgewikkeld? Wordt er een incidentrapport opgemaakt na een beveiligingsinbreuk?*
    Op intranet staat beschreven op welke wijze beveiligingsincident gemeld moet worden. Als er een incident zich voordoet, dan weten medewerkers dat ze in overleg moet treden met de afdeling Beveiliging en wordt er een incidentrapport opgemaakt.

12. *Wie is binnen uw organisatie en/of afdelingen verantwoordelijk voor het uitvoeren en controleren van het informatiebeveiligingsbeleid?*
    Hiërarchisch is het cluster Beveiliging onder leiding van de directie, die verantwoordelijk is voor het opstellen en naleving van het beleid. De organisatie in z'n geheel zijn en leidinggevenden in het bijzonder zijn verantwoordelijk voor het invullen en toepassen van het beleid op de afdeling.

13. *In hoeverre is uw directe lijnverantwoordelijke van uw organisatie betrokken bij het informatiebeveiligingsbeleid?*
    De leidinggevende is verantwoordelijk voor de uitvoering van het beleid op de afdeling.

14. *Worden er risico analyses gemaakt op het informatiebeveiligingsbeleid? Wie is hier verantwoordelijk voor? Hoe vaak worden deze gemaakt?*
    Op onze afdeling speelt dit minder, de productgroepen waaraan wij onze diensten leveren maken veelal de afwegingen en bepalen de prioritering van maatregelen. Daarnaast heeft de afdeling Beveiliging een faciliterende en aanjagende rol, om de afdelingen te begeleiden met het uitvoeren van de risico analyses.

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

Ik denk dat het uitdragen van het beleid op de afdelingen niet overal in dezelfde mate en omvang plaats vindt. Het uitdragen van beleid vanuit de organisatie is mijn ziens te weinig en kan beter. Bewustwording en ook privacy-aspecten moeten gewoon jaarlijks terugkerende thema's zijn, zeker gezien de informatieverwerkende rol binnen het Rijk. Bij mijn vorige werkgever bijvoorbeeld, moest iedereen verplicht jaarlijks een online training volgen en het certificaat overleggen.

16. *Is er het afgelopen jaar een controle/audit uitgevoerd op de beveiligingsbeleidspunten?*
    Ik weet dat er audits plaats vinden binnen de organisatie, onze afdeling wordt daarin niet direct betrokken. Wel als onderdeel van het controleren van het bestaan van een BIR maatregelen, maar niet hoe deze nu in de praktijk werkt / wordt ingevuld in relatie met de producten die we ontwikkelen.

Social engineering

17. *Wat verstaat u onder social engineering? Wat is de kern hiervan? Kunt u zich vinden in de volgende definities van social engineering?*
    Voor dit onderzoek had ik geen beeld bij de term social engineering. Nu ik meer achtergrond heb gekregen, ook vanuit de online survey, zie ik het vooral als het argeloos, met goede bedoeling en zonder de negatieve gevolgen te overzien, ingaan op verzoeken om "hulp".

    Beide definities dekken volgens mij de lading. Definitie één spreekt meer over groepen en draait daarbij meer om de mens en het uitbuiten, definitie twee spreekt meer over het individu en de technieken informatie te verkrijgen uit informatiesystemen.
    Deze tweede definitie spreekt mij meer aan, omdat hierin de oorzaken waarom mensen ingaan op verzoeken, zoals nieuwsgierigheid, hebzucht, vertrouwen en de manipulatie duidelijker naar voren komen.

18. *Kunt u beschrijven hoe een social engineeringaanval in zijn werk gaat?*
    Het is heel breed, van een "collega" met een verzoek via mail, of de glazenwasser die iets is vergeten en wil ophalen, en die daarbij een beroep doen op je hulpvaardigheid.

19. *Welke motieven zou een social engineer kunnen hebben?*
    Voor deze organisatie kan het gaan om het achterhalen van persoonlijke en privacy gevoelige informatie die voor een netwerk van belang kan zijn, of het manipuleren / chanteren van een medewerker. Breder zullen ook financiele motieven een rol spelen.

20. *Bent u in staat om een aantal verschillende social engineeringsaanvallen te beschrijven?*
    Voorbeeld van social engineering zoals het voordoen als iemand anders, phishing mail, meelopen, telefonisch benaderen, infiltreren door op een (tijdelijke) functie te solliciteren.

21. *Waar maakt een social engineer misbruik van?*
    De behoefte van mensen om hulpvaardig te zijn.

22. *Ziet u vanuit uw eigen medewerkers en/of externe partijen bedreigingen binnen de organisatie?*

Nee, geen redenen om aan te nemen dat interne of externe medewerkers meer een bedreiging vormen.

23. *Zijn er recent incidenten geweest rondom social engineeringsaanvallen? Via welk (communicatie)kanaal werd deze poging ondernomen?*
    Nee.

24. *Is naar uw mening uw organisatie voldoende op de hoogte/bewust van social engineering?*
    Ik denk van niet, als mensen al bekend zijn met vormen van sociale engineering, dan is dat vooral met de term phishing door de recente phishingcampagne en aandacht in de media. Maar dat informatiebeveiliging ook een zachte kant heeft en draait om het gedrag van de mens en dus ook over het manipuleren van mensen, dat is minder of niet bekend is. Dat speelt overigens niet alle binnen deze organisatie, maar ook een gemiddelde persoon op straat die zich van geen kwaad bewust is als deze wordt aangesproken.

25. *Is naar uw mening uw organisatie momenteel voldoende beschermd tegen social engineeringsaanvallen? Welke verbeteringen kunnen worden doorgevoerd?*
    Ik denk ten delen, het melden van voorvallen of het bewustzijn hier binnen een vertrouwelijke omgeving te werken is zeker aanwezig. Maar ondanks deze alertheid is het niet uitsluiten dat in een onachtzaam moment een medewerker op een link klikt.

    Ik denk dat meer op bewustzijn kan worden ingezet, blijf de boodschap herhalen. Maar benadruk ook die andere vormen van manipulatie, zodat deze tijdig worden herkend.

26. *Wat zijn de mogelijke gevolgen voor de organisatie als vertrouwelijke informatie op straat komt te liggen?*
    Met name de reputatie van de organisatie die geschaad wordt en mogelijk op spel staat bij ernstige inbreuken.

27. *Hoe groot is de kans dat een medewerker in een phishing mailt trapt?*
    Die kans is er zeker, de laatste phishingcampagne liet zien dat er wel medewerkers zijn geweest die verleid of onachtzaam waren en op een link hadden geklikt.

28. *Hoe groot is de kans dat een persoon het gebouw binnenkomt als deze zelf geen toegang heeft?*
    De gebouwen zijn alleen met toegangspassen toegangelijk, dus de kans is niet zo heel groot. Maar het meelopen met groepen medewerkers is niet uit te sluiten.

29. *Hoe groot is de kans dat wanneer een medewerker een data medium (USB stick, cdrom) vindt, deze ook daadwerkelijk bekijkt?*
    Dit is minder aannemelijk, er zijn technische maatregelen getroffen die het niet mogelijk maken om een usb-stick of cd-rom af te kunnen spelen. Daarnaast heb ik ook gemerkt dat medewerkers al snel met zaken die ze niet vertrouwen naar mij toekomen, om het te melden of om gevonden zaken af te komen geven.

30. *Weet je welke trends er spelen op het gebied van social engineering?*
    Nee, geen afdoende beeld bij. Wel zie ik meer media aandacht voor ransomware, of phishing, die op grotere schaal plaats lijken te vinden.

31. *Reageert de organisatie snel genoeg op nieuwe ontwikkelingen, in dit geval social engineering. Is het een nieuwe ontwikkeling?*
    Geen nieuwe ontwikkeling, maar wel steeds meer in samenhang met andere hack methoden wordt toegepast. Rondom de recente ransomware uitbraak reageerder de IT organisatie zeer snel en adequaat, ik denk dat we op dergelijke aanvallen goed beschermd zijn. Wel blijft het noodzakelijk om, zoveel mogelijk actief met medewerkers, te blijven werken aan bewustwording.

Interview IBF 8 m.b.t. social engineering binnen de Rijksoverheid

Algemene vragen

1. *Wat is uw rol als IB functionaris (IBF) en kunt u deze in het kort omschrijven?*
   De IBF rol richt zich voornamelijk ondersteunen van de manager op a; het implementeren van de BIR maatregelen op de afdeling en b; het adviseren rondom beveiligingsonderwerpen en incidenten.

2. *Hoeveel jaar bent u in dienst en hoeveel jaar vervult u de IBF rol voor uw afdeling?*
   4 jaar in dienst en 2 jaar als IBF voor de afdeling

3. *Hoeveel medewerkers telt uw afdeling?*
   45 medewerkers

Informatiebeveiligingsbeleid

4. *Hoe wordt binnen uw Rijksdienst omgegaan met informatiebeveiliging. Hoe wordt dit vastgelegd?*
   Voor mij is het informatiebeveiligingsbeleid het hanteren en vertalen van de BIR maatregelen binnen de organisatie.

5. *Hoe verhoudt het informatiebeveiligingsbeleid zich tot de BIR / ISO 27001 normering?*
   Dat weet ik zo niet, kan ik geen antwoord op geven.

6. *Zijn er directe of indirecte informatiebeveiligingsmaatregelen tegen social engineering vastgelegd in het huidige informatiebeleid van uw organisatie? Kunt u hiervan een voorbeeld geven?*
   Er worden geen specifieke maatregelen genoemd op het vlak van social engineering in de BIR. Het is geen term die daarbinnen wordt gehanteerd. Wel onderkennen we in risicoanalyses de mens als kwetsbare factor en zijn er tal van gerelateerd maatregelen genomen, zoals bijvoorbeeld functiescheiding en autorisatieprocedures.

7. *Wat is waardevolle informatie voor uw organisatie? Weten uw manager en de medewerkers dat? Is er binnen de organisatie bekend welke informatie het belangrijkst is?*
   Op deze afdeling is dat bewustzijn er zeker, medewerkers weten heel goed wat waardevolle informatie is. Het werken met vertrouwelijke informatie ligt besloten in de aard van de dienstverlening, hierbij is geen onderscheid in leidinggevende en medewerkers.

8. *Hoe gaat men binnen de organisatie om met het verwijderen van vertrouwelijke gegevens en/of documenten?*
   Alle wijzigingen binnen het informatiesysteem wordt gelogd en zijn te herleiden naar een medewerker. Het verwijderen van gegevens is een specifieke procedure waarvoor een geautoriseerd verzoek noodzakelijk is. Papieren en andere informatiedragers worden apart ingezameld en vernietigd.

9. *Worden medewerkers gescreend voordat deze aangenomen, op welke zaken?*
   Er is een controle bij het in diensttreden op het kunnen overleggen van een VOG.

10. *Is er bij het beëindigen van een dienstverband controle op het retourneren van bedrijfsapparatuur, toegangspassen en het afsluiten van voorzieningen?*
    Er is een werkproces ingericht met stappen die doorlopen moeten worden, waaronder het inleveren van bedrijfsmiddelen, intrekken van accounts, toegangspas ed. Het komt wel voor dat het intrekken van de toegang tot een specifieke applicatie wordt vergeten, deze komen dan bij een generieke opschoning naar boven.

11. *Hoe wordt omgegaan met een beveiligingsincident binnen uw afdeling/organisatie? Hoe worden incidenten afgewikkeld? Wordt er een incidentrapport opgemaakt na een beveiligingsinbreuk?*
    Op deze afdeling wordt door de medewerker zelf de leidinggevende ingelicht en wordt het incident gemeld bij de afdeling Beveiliging. Deze meldingen worden daar centraal verzameld en eventueel verder doorgezet, tevens maakt de afdeling Beveiliging een rapportage op.

12. *Wie is binnen uw organisatie en/of afdelingen verantwoordelijk voor het uitvoeren en controleren van het informatiebeveiligingsbeleid?*
    De leidinggevende is verantwoordelijk voor het beleid op de afdeling, de uitvoering en het voldoen aan BIR maatregelen. De IBF'er ondersteunt daar bij.

13. *In hoeverre is uw directe lijnverantwoordelijke van uw organisatie betrokken bij het informatiebeveiligingsbeleid?*
    De leidinggevende is niet betrokken bij het opstellen van het beleid, dit ligt bij de afdeling Beveiliging. Er is twee-maandelijks afstemming tussen de afdeling Beveiliging, de leidinggevende en de IBF'er over de voortgang van beveiliging op de afdeling en lopende zaken.

14. *Worden er risico analyses gemaakt op het informatiebeveiligingsbeleid? Wie is hier verantwoordelijk voor? Hoe vaak worden deze gemaakt?*
    Volgens een driejarig cyclus, vindt er een risicoanalyse op de informatiesystemen en haar omgeving plaats. Hierin worden de dreigingen en kwetsbaarheden geanalyseerd, en volgen daaruit eventuele aanvullende maatregelen voor de afdeling. De leidinggevende is verantwoordelijk voor het initiëren van de risico-analyses, de afdeling Beveiliging faciliteert.

15. *Wordt het beveiligingsbeleid uitgedragen/verspreid binnen de afdeling en organisatie? Wordt op alle afdelingen het beleid op dezelfde manier uitgedragen?*
    De medewerker op de afdeling is zich vanuit zijn/haar functie bewust van de beveiligingsaspecten en hoe te handelen met vertrouwelijke informatie. Echter is dit niet een onderwerp dat regelmatig besproken wordt en waar actief aandacht voor wordt gevraagd.

    Het oppakken, uitdragen hangt af van de relevantie, prioritering binnen de afdelingen. Daarnaast verschilt per afdeling ook de kennis / achtergrond van de IBF'er en de leidinggevende, om dit op te zetten en uit te dragen. Ik zou dit daarom liever organisatie-breed willen oppakken.

16. *Is er het afgelopen jaar een controle/audit uitgevoerd op de beveiligingsbeleidspunten?*
    Ja, er heeft het afgelopen jaar een audit plaats gevonden naar een specifiek werkproces op de afdeling.

Social engineering

17. *Wat verstaat u onder social engineering? Wat is de kern hiervan? Kunt u zich vinden in de volgende definities van social engineering?*
    De term social engineering zei mij voor dit onderzoek niets.

    Beide definities hebben in de kern de menselijke factor als zwakste schakel, definitie twee is voor mij concreter over de menselijke eigenschappen en sluit meer aan naar hoe ik er naar kijk.
    Ik mis dat ook het onbewuste een factor kan zijn in social engineering. Als ik op verjaardagen vertel waar ik werk, lokt dat ook potentieel ongewenste interesse uit. Ik zelf ben daar terughoudend in, dit heeft volgens mij een preventieve werking.

18. *Kunt u beschrijven hoe een social engineeringaanval in zijn werk gaat?*
    Nee, geen beeld bij of ervaring mee.

19. *Welke motieven zou een social engineer kunnen hebben?*
    Het bemachtigen en kennis vergaren over vertrouwelijke persoonsgegevens van burgers.

20. *Bent u in staat om een aantal verschillende social engineeringsaanvallen te beschrijven?*
    Voorbeelden van social engineering zoals phishing mail, meelopen en persoonlijk benaderen.

21. *Waar maakt een social engineer misbruik van?*
    Het misbruiken van persoonlijke situaties van mensen, maar ook de goedheid van de persoon om te helpen en daarmee ongewild bepaalde informatie prijs geeft.

22. *Ziet u vanuit uw eigen medewerkers en/of externe partijen bedreigingen binnen de organisatie?*
    Nee, die bedreigingen zijn er volgens mij niet. Ik heb geen redenen om aan te nemen dat interne of externe medewerkers een bedreiging vormen. Wel maak ik me zorgen over het gemak waarmee externe partijen hier kunnen rondlopen, in potentie kan dit een bedreiging zijn.

23. *Zijn er recent incidenten geweest rondom social engineeringsaanvallen? Via welk (communicatie)kanaal werd deze poging ondernomen?*
    Nee.

24. *Is naar uw mening uw organisatie voldoende op de hoogte/bewust van social engineering?*
    Medewerkers zijn zich zeker bewust op “ongewone” verzoeken, alleen zullen ze dat niet direct social engineering noemen. Vanuit het Rijk zijn er bewustzijnscampagnes met phishing mail uitgevoerd, ik vind wel dat er vanuit de organisatie zelf ook meer aan bewustzijn kan worden gedaan.

25. *Is naar uw mening uw organisatie momenteel voldoende beschermd tegen social engineeringsaanvallen? Welke verbeteringen kunnen worden doorgevoerd?*
    Ik denk op technisch gebied wel, al heb ik zelf geen zicht op de maatregelen.
    Of het voldoende beschermd is vind ik lastig, het gaat immers om persoonlijke afwegingen. Doordat het zo persoonlijk kan zijn, moet je gezamenlijk werken aan het creëren van een vertrouwde omgeving, waarin je met elkaar open durft te spreken over gedragingen en mogelijke risico's.

26. *Wat zijn de mogelijke gevolgen voor de organisatie als vertrouwelijke informatie op straat komt te liggen?*
    De privacy gevoeligheid van de informatie binnen de afdeling is groot en daarmee de gevolgen van het eventueel uitlekken ook. Er zal een onderzoek plaats vinden naar de oorzaken van het lek, om zo aanvullende maatregelen te kunnen treffen die herhaling moeten voorkomen. Daarnaast betreft het een datalek die volgens de wet direct moet worden gemeld.

27. *Hoe groot is de kans dat een medewerker in een phishing mailt trapt?*
    De kans acht ik niet zo groot meer, althans de afdeling reageerde zeer alert op de recente phishing mailtest.

28. *Hoe groot is de kans dat een persoon het gebouw binnenkomt als deze zelf geen toegang heeft?*
    De kans is aanwezig, het is mijn ziens mogelijk om binnen te komen. Het meelopen met groepen of je zelf legitimiteit verzorgen via een jasje met logo is niet ondenkbaar en is iets waar we alerter op moeten zijn.

29. *Hoe groot is de kans dat wanneer een medewerker een data medium (USB stick, cdrom) vindt, deze ook daadwerkelijk bekijkt?*
    Het gebruik van een usb-stick of cd-rom om data te verplaatsen is niet gebruikelijk binnen deze organisatie. Ik verwacht dat een losse stick daarom niet snel bekeken zal worden, maar als gevonden voorwerp wordt afgegeven aan de receptie.

30. *Weet je welke trends er spelen op het gebied van social engineering?*
    Nee, geen beeld bij. Wel is er meer aandacht voor het onderwerp, via de media over bijvoorbeeld phishing fraude.

31. *Reageert de organisatie snel genoeg op nieuwe ontwikkelingen, in dit geval social engineering. Is het een nieuwe ontwikkeling?*
    Kan ik niet beoordelen, weet ik niet. Wel lijkt het me een goed om na aanleiding van dit onderzoek, het bewustzijn op social engineering onder medewerkers te gaan vergroten.