'Veilig' gedrag tegen Social Engineering

in Industriële Automatisering (IA) omgeving van Rijkswaterstaat

Open Universiteit
www.ou.nl

Master thesis

Versie: 1.5
Datum: 30 augustus 2017
Status: Definitief

Studentnummer: 851063040

ing. Mustafa Nizami

Afstudeercommissie

Open Universiteit
Eerste begeleider: Dr. ir. Hugo Jonker
Tweede begeleider: Prof. dr. Rob Kusters
Examinator: Prof. dr. Rob Kusters

Rijkswaterstaat
Begeleider: dr. ir. ing. John Steenbruggen

Vakgebied

T9232B Master Business Process Management and IT
Faculteit Management, Science and Technology, Open Universiteit

Voorwoord

Allereerst wil ik graag alle mensen bedanken, die het mogelijk hebben gemaakt om aan deze masterscriptie bij te dragen.

In het bijzonder wil ik mijn eerste afstudeerbegeleider dr. ir. Hugo Jonker bedanken voor zijn tijd en ondersteuning tijdens de feedback momenten en de begeleiding tijdens mijn masterscriptie en wil mijn tweede begeleider Prof. dr. Rob Kusters, wil ik bedanken voor zijn feedback tijdens de laatste fase van mijn onderzoek.

Daarnaast wil ik alle medeweerkers van Rijkswaterstaat bedanken, die tijd beschikbaar hebben gesteld om mijn interview en enquête vragen te beantwoorden met als doel een belangrijke bijdrage te leveren aan mijn onderzoek.

In het bijzonder wil ik mijn begeleider vanuit Rijkswaterstaat dr. ir. Ing John Steenbruggen bedanken voor zijn ondersteuning tijdens mijn onderzoek.
Speciale dank gaat uit naar mijn vrouw Naziefa, mijn ouders en mijn broers. Graag wil ik jullie bedanken voor de steun, het geduld en de aanmoediging gedurende mijn studie.

Afkortingenlijst

Afkorting	Uitleg
A&O	Aanleg en Onderhoud
AS	Assetmanagement
APA	American Psychological **Association**
BIR	Baseline Informatiebeveiliging Rijksdienst
BIR RWS	Baseline Informatiebeveiliging Rijkswaterstaat
CIV	Centrale Informatie Voorziening
CLC	Corporate Learning Center
CS	Cybersecurity
CSBN	Cybersecuritybeeld Nederland
CSIR	Cybersecurity Implementatierichtlijn Rijkswaterstaat
DBFM	Design, Build, Finance and Maintain contract
D&C	Design & Construct
EAR	Ènterprise Architectuur
FB	Fysiek Beveiliging
FV	Functioneel Veiligheid
GPO	Grote Projecten Onderhoud
GWW	Grand- Weg- en Waterbouw
HR	Human Resource
HVWN	Hoofdvaarwegennet
HWN	Hoofdwegennet
HWS	Hoofdwatersysteem
IA	Industriële Automatisering
ICS	Industrial Control Systems
IMPAKT	Impuls Programma Aanpak Kritische Technische infrastructuur
IPM	Integraal Project Management
IV	Informatievoorziening
NCSC	National Cyber Security Centrum
NLP	Neuro linguïstische programmering
NSS	Nuclear Security Summit
OG	Opdrachtgever
ON	Opdrachtnemer
P&C	Prestatie Contracten
PPO	Programma's Projecten en Onderhoud
RWS	Rijkswaterstaat
SCADA	Supervisory Control And Data Acquisition
SE	Social Engineering
SOC	Security Operation Center
SLU	Samenwerking Landelijke Uitvoering
VWM	Verkeer- en Watermanagement
WWAO	Werk Wijzer Aanleg Onderhoud

Tabel 1: Afkortingenlijst

Inhoudsopgave

Management samenvatting

De *situatie* is dat het digitaliseren van het Nederlandse weg- en waterinfrastructuur waarvoor Rijkswaterstaat verantwoordelijk is toeneemt en daarmee ook het aantal cyberdreigingen en het gevaar dat het netwerk door kwaadwillenden wordt overgenomen. Deze digitalisering wordt ook wel Industriële Automatisering genoemd en behelst momenteel meer dan 460 fysieke objecten (tunnels, sluizen, gemalen, bruggen, etc..) lokaal verspreid over Nederland, die via het RWS-netwerk aangesloten zijn op meer dan 32 centrales van waaruit de lokale objecten bediend, bewaakt en bestuurd worden. In het jaar 2016 alleen al werden 8.982 dreigingen in het RWS-netwerk gedetecteerd.

Het *probleem* is dat huidige awareness programma's om RWS-medewerkers weerbaar te maken tegen cyberdreigingen niet lijken te helpen. Het gaat vooral om een specifiek vorm van cyberdreigingen, waarbij medewerkers worden gemanipuleerd om informatie vrij te geven, ook wel social engineering genoemd. Op een specifieke social engineering aanval phishing-mail, door RWS zelf begin 2017 opgezet, gingen (trapten) nog altijd meer dan 2000 medewerkers in.

De *vraag* is dan ook hoe meer grip te krijgen op 'veilig' cybergedrag van medewerkers van Rijkswaterstaat in de Industriële Automatisering (IA) omgeving. De medewerkers zijn de bedienaars, objectbeheerders en projectleden.

Het *antwoord* hierop is vanuit psychologisch perspectief gegeven: Voor gedragsverandering is meer nodig dan alleen informatie verstrekking. Ten eerste dienen de medewerkers het advies te kunnen plaatsen in hun normenkader van waaruit ze opereren: Medewerkers volgen andere collega's, dus voorbeeldgedrag helpt, veilig gedrag moet als groepsnorm aangeduid worden en met maatregelen aansluiten op de kernwaarden van een individu. Ten tweede, dienen medewerkers gemotiveerd te worden. Laat zien wat de ernst is van dreigingen gerelateerd aan hun werk en laat zien dat de voorgeschreven maatregelen ook helpen. Ten derde, stel de medewerkers in de gelegenheid en maak het aantrekkelijk voor ze om voor zich doelen te stellen waardoor ze zichzelf instaat vinden om zelfstandig de voorgeschreven beveiligingsmaatregelen succesvol uit te voeren.

Dit *rapport* is als volgt opgebouwd: allereerst wordt uitgebreid ingegaan op de problematiek, vervolgens wordt de onderzoeksopzet besproken en de te nemen stappen. Daarna worden de resultaten van het onderzoek toegelicht, waarbij eerst het referentiemodel gedestilleerd op basis van literatuurstudie wordt uitgelegd en vervolgens toetsing van dit referentiemodel aan de hand van het interview van 11 medewerkers van Rijkswaterstaat. Tenslotte volgt de enquête, welke door 102 medewerkers zijn beantwoord.

Ik wens u veel leesplezier.

Introductie

We leven in een tijd van digitalisering en de afgelopen decennia zijn niet alleen onze dagelijkse activiteiten bijna volledig gedigitaliseerd, maar ook de koppeling van onze fysieke wereld aan de digitale wereld. Onze kritieke infrastructuursystemen zoals treinnetwerken, elektriciteit, gas, telecommunicatiesystemen, vitale objecten (waterkeringen, sluizen, stuwen, gemalen, bruggen, tunnels en verkeerscentrales) zijn uitgebreid gedigitaliseerd en onderling verbonden over de hele wereld. Waar voorheen beveiliging niet meer inhield dan het beveiligen van de toegangspoorten van een zakelijk pand, zijn er tegenwoordig meer toegangspoorten te beschermen dan alleen de fysieke toegangen. Iedere medewerker heeft op afstand een verbinding met het bedrijfsnetwerk van een organisatie door het gebruik van een laptop, smartphone of tablet, en hiermee is dit dus zo ook in feite een toegangspoort.

De menselijke fout:

Kwaadwillenden richten zich steeds meer op de medewerkers om via hen ongewenste toegang te verkrijgen tot informatiesystemen van een organisatie. Door te focussen op de menselijke factor, omzeilen kwaadwillenden hierdoor zwaar-technisch beveiligingssystemen, zoals firewalls, detectie systemen en publiek belangrijke infrastructuur. Peltier (2006) licht de menselijke factor toe: het feit dat de kwaadwillende het slachtoffer beïnvloedt door een beroep te doen op zijn/haar menselijke eigenschappen (psychologische zwaktes) als behulpzaamheid, onwetendheid, luiheid en vertrouwen. Het gebruik van bijbehorende methoden en technieken om mensen te manipuleren om zo beveiligingssystemen binnen te komen wordt ook wel social engineering (SE) genoemd, direct of indirect via bijvoorbeeld email contract (Applegate, 2009; Krombholz et al., 2015).

De reden dat ongewenste personen toch toegang krijgen tot systemen is te wijten aan psychologische zwaktes in de mens waarop social engineer aanvallers inspelen met onvoldoende verdediging hiertegen vanuit informatiebeveiliging (Manske 2000; Aloul, 2012; Workman, 2008, Maan, 2012). Daarom is het in toenemende mate belangrijk om te werken aan de weerbaarheid van de medewerkers. Dit wordt ook bevestigd door steeds meer onderzoeken. Hieruit komt naar voren dat de ‘menselijke fout’ de grootste barrière is voor het bereiken van een cyberveilige organisatie (PWC, 2016; NCSC, 2016; Ponemon Institute, 2016; McAfee, 2014).

Bewustwording:

Om hun medewerkers weerbaar te maken, hebben 53% van de Nederlandse organisaties een awareness programma (PWC, 2016). Deze programma’s hebben als doel de medewerker kennis te geven over de aanvalsmanieren en ze daarmee weerbaar maken. Echter, resultaten uit een onderzoek op basis van een vragenlijst in 2016 onder de werkzame bevolking in Nederland laat zien dat we met de huidige awareness programma’s niet het gewenste resultaat bereiken; het percentage van de daadwerkelijke slachtoffers zijn fors te noemen (phishing mail: 52%; malware: 25%) (TNS, 2016). Het is waar dat mensen kennis moeten hebben van de dreigingen om ze te herkennen, maar in talloze gevallen blijkt dat deze kennis niet leidt tot gewenste gedragsverandering en dus niet het probleem is.

TNS (2016) constateert bv. dat zelfs een kwart van de algemene bevolking en 17% van de werkzame bevolking ondanks dat we allemaal weten wanneer een wachtwoord veilig is, we nog regelmatig wachtwoorden op een (verstopt) briefje schrijven. Een ander voorbeeld is dat het draaien van automatische updates algemeen bekend is, terwijl minder dan de helft deze heeft aanstaan. Er is dus meer nodig dan het bijspijkeren van kennis. Verschillende studies geven aan dat awareness niet altijd leidt tot de gewenste gedragsverandering (Wetze, 2016).

Gedragsverandering:

De vraag is of gedrag überhaupt te beïnvloeden is en zo ja welke factoren daarbij een rol spelen. Meerdere studies hebben verschillende aanknopingspunten gevonden in de gedragsliteratuur, namelijk de gedachte dat intenties van mensen en daarmee gedrag van mensen is te beïnvloeden om daarmee meer grip te krijgen op cyberveilig gedrag (Wetze, 2016; Koers & Nuijten, 2016). In de gedragsliteratuur komen we verschillende opvattingen, theorieën en modellen tegen die dit

onderbouwen. Op basis hiervan is een referentiemodel uitgewerkt in het hoofdstuk literatuurstudie gedrag.

Veilig gedrag:
Om van 'onveilig' gedrag naar 'veilig' gedrag te komen, leert de psychologie ons dat gedrag, om veranderd te kunnen worden, heel specifiek gedefinieerd moet worden. Met andere woorden wat is het gewenste gedrag dat een organisatie wil zien van zijn of haar medewerker? In het domein van cybersecurity zien we dat een groot aantal gewenste gedragingen haast voor elke organisatie van toepassing is. Neem bv. het nooit delen van je wachtwoord met anderen en het veranderen hiervan om de zoveel tijd. Echter, afhankelijk van de omgeving waarin iemand werkt kunnen deze gedragingen ook heel specifiek zijn. Bijvoorbeeld, een bedienaar van een tunnel die een melding naar de beheerder van de tunnel moet maken als hij onbekenden in de tunnelruimtes ziet. Wanneer de norm binnen een organisatie duidelijk is, kan worden onderzocht hoe het staat met de kennis, risicoperceptie, attitude en de subjectieve norm om het gewenste gedrag te vertonen.

Huidige programma's zetten vooral in op het geven van trainingen en informatie over het gewenste gedrag, met de aanname dat gedrag niet optreedt vanwege een gebrek aan kennis erover. Het kan net zo goed ontbreken aan risicoperceptie zijn bij informatieverlies of –schade, of het ontbreken van een positieve waardering van het gewenste gedrag, of het ontbreken van een duidelijke regel in de directe omgeving van de medewerker van wat wel/niet toelaatbaar is.

Wanneer eenmaal bekend is wat ontbreekt voor de gewenste gedragsverandering, kan de stap gemaakt worden naar het treffen van passende maatregelen. B.v. als het probleem is dat iemand niet gelooft in de beveiligingszaken, dan helpt het niet om nog meer training te geven maar eerder het uitdragen van positieve ervaringen en het opnemen van de norm in de cultuur (rituelen, helden, symbolen).

1.1 Aanleiding van het onderzoek

Zowel vanuit de wetenschap als de praktijk is er behoefte aan onderzoek om beter grip te krijgen op SE bij overheden. Krijn (2016) heeft weliswaar onderzoek gedaan naar het kennisniveau van de medewerkers van bij rijksoverheid over SE met als aanbeveling voor een vervolgonderzoek op het verkennen van variabelen die invloed hebben op de awareness van de medewerkers, zoals de tijd door bv. het onderzoek zelf te herhalen. Maar dit onderzoek zou gebaseerd kunnen zijn op een verkeerde aanname, namelijk dat het gewenste gedrag bij medewerkers niet optreedt vanwege een gebrek aan kennis over SE.

Het gaat erom dat het onderwerp moet 'leven' bij de medewerker om over te gaan tot het gewenste gedrag en daarbij is kennis èèn van de factoren. In de wetenschap is de vraag of er en zo ja welke andere factoren er zijn die het gedrag beïnvloeden. Wel zal in dit onderzoek de wijze waarop Krijn (2016) de kennis van de medewerker over SE heeft gemeten, gebruikt worden.

Dit kunnen we doen als het gaat over algemene kennis over SE, maar de gedragingen zijn in mijn onderzoek heel specifiek. Het is een IA omgeving, waar andere eisen gelden dan in een kantooromgeving. En bij algemene kennis over SE gaat het vooral om de hoeveelheid kennis die nodig is om over te gaan tot veilig gedrag. Dat is dus niet zozeer tot het op de puntjes kennen van alle aanvalsvormen en techniek van SE, maar eerder het onderkennen en herkennen van het mechanisme van SE. Het detecteren van de verschillende soorten technieken is beter weggelegd door inzet van technische middelen.

Vanuit de praktijk is voor Rijkswaterstaat (RWS) er alles aan gelegen dat haar medewerkers op een 'veilige' manier hun werkzaamheden doen voor of in een object (waterkeringen, sluizen, stuwen, gemalen, bruggen, tunnels en verkeerscentrales). Deze objecten staan in toenemende mate in verbinding met het digitaal netwerk. Denk bijvoorbeeld aan het op afstand bedienen van een tunnel.

Dit is een softwarematig aansturing door Supervisory Control And Data Acquisition systemen (SCADA-systemen) (Nicholson, 2012). Het voert functies uit als verzamelen, doorsturen, verwerken en visualiseren van meet- en regelsignalen van verschillende machines in objecten zoals tunnels. Het

aansturen van deze SCADA-systemen gebeurt via het internet. Iedere medewerker die informatie heeft waarmee indirect of direct toegang tot dat netwerk verkregen kan worden, kan in feit gezien worden als een toegangspoort.

Uit een parlementaire enquête 2014 bleek dat RWS een potentieel doelwit is van cybercrime: “Een hacker zou bijvoorbeeld een overstroming kunnen veroorzaken of een brug kunnen openen en daarmee wegverkeer het water in kunnen leiden.

Dergelijk incidenten zouden het gevoel van veiligheid in Nederland ernstig ondermijnen alsmede het vertrouwen beschamen dat de organisatie voldoende grip heeft op de eigen processen”.[1]

Ook in de productieopgave van 2018-2023 van RWS staat cybersecurity van infrastructurele objecten in de top 5 van risico’s (Speerpuntenbrief RWS 2018). Inbreuk op de veiligheid door cyber criminaliteit maakt dat deze objecten kwetsbaar zijn waarmee er in potentie grote risico’s bestaan voor de kerntaken van het ministerie van Infrastructuur en Milieu. Het gaat hierbij zowel om droge voeten, water kwaliteit en veilige doorstroming van het verkeer op zowel de vaarwegen als de snelwegen. Dit heeft direct een impact op de veiligheid en leefbaarheid van de samenleving.

Daarnaast vormden meerdere ontwikkelingen van buiten (cybersecurityincident gemeente Veere in 2012 [2] resultaten Algemene Rekenkamer[3], cybercrime bende opgerold in 2015[4]) de aanleiding voor Rijkswaterstaat om de weerstand van haar infrastructuur te toetsen tegen cybersecurity dreigingen.

Het Programma IMPAKT (Impuls Programma Aanpak Kritieke Technische Infrastructuur) heeft op basis van haar inventarisatie een set aan Cybersecurity Implementatie Richtlijnen (CSIR) opgesteld. Hierin staat onder andere wat het gewenste gedrag is en wat de organisatie verwacht van een medewerker (veilig gedrag).

Als volgende stap heeft RWS meerdere ‘awareness’-activiteiten in gang gezet om de medewerker bewust te maken van risico’s in IA objecten, de te nemen eigen verantwoordelijkheid, noodzaak van goede procedures, leren herkennen van verdachte situaties en bewust maken van nieuwe dreigingen. Het is slechts een kwestie van tijd om de kennis van de medewerkers op het juiste niveau te brengen teneinde zich te kunnen weren tegen cyberaanvallen.

Echter, kunnen we ons voorstellen dat de set aan maatregelen uit CSIR door de medewerkers als ‘te overdreven’ wordt ervaren. Immers, de medewerkers werken al vele jaren op hun eigen manier, en is het (tot nu toe!) nog nooit mis gegaan.

1.2 Doelstelling

De doelstelling van dit afstudeeronderzoek is tweeledig.

1.2.1 Wetenschappelijke relevantie

Enerzijds heeft dit onderzoek een wetenschappelijke relevantie. Dat is om kennis te verkrijgen op welke wijze gedrag van mensen is te beïnvloeden om weerbaar te zijn tegen technieken van social engineering aanvallen. Daarbij wordt inzicht verkregen in:

- De wijze waarop een social engineer inspeelt op de psychologische zwaktes in de mens;
- Of gedrag is te beïnvloeden en welke factoren daarbij een rol spelen;

[1] Response-Ability RWS-Strategie 2014 Digitale Beveiliging voor RWS infrastructuur

[2] Eenvandaag bericht 14 feb 2014: onbekenden stonden aan de voordeur om binnen te komen in het systeem waarmee de pomp voor waterhuishouding in de gemeente Veere bediend kon worden.

[3] RWS kreeg een rode kaart van de Algemene Rekenkamer dat de informatiebeveiliging van RWS niet voldeed aan de Baseline Informatiebeveiliging Rijksdienst (BIR).

[4] In juni 2015 verschenen er een bericht op nu.nl dat Europol een banktrojan-bende uit Oekraïne had opgerold, die via het internet Zeus- en Spyeye malware verspreidde om zo bankrekeningen te plunderen

1.2.2 Praktische relevantie

Anderzijds heeft dit onderzoek een praktische relevantie. Dat is om RWS meer grip te bieden op het 'veilig gedrag' van haar medewerkers. Daarbij wordt inzicht verkregen in:

- Wat voor een beleid/norm RWS stelt aan het gedrag van medewerkers in IA objecten van Rijkswaterstaat;
- Wat voor een beeld de medewerkers van RWS hebben om veilig gedrag in IA objecten te vertonen;

1.2.3 Leeswijzer

In hoofdstuk 1 wordt de introductie, aanleiding en de doelstelling van dit onderzoek beschreven. Hoofdstuk 2 gaat in op de methodiek die gebruikt is bij de uitvoering van het onderzoek. Hoofdstuk 3 bevat de resultaten van de literatuurstudie, de beantwoording van de theoretische deelvragen (T1 t/m T5). In hoofdstuk 4 worden de resultaten van het empirische onderzoek beschreven, de beantwoording van de Empirische deelvragen (E1 t/m E5).In hoofdstuk 5 worden de conclusies, aanbevelingen voor vervolgonderzoek beschreven en wordt er gereflecteerd op het onderzoek. Hoofdstuk 6 bevat tot slot een overzicht van gebruikte bronnen (wetenschappelijk en niet wetenschappelijk) die bij het uitvoeren van dit onderzoek zijn gebruikt.

1.3 Onderzoeksvragen

1.3.1 Vraagstelling

Welke factoren hebben invloed op het 'veilig' gedrag gedrag van RWS medewerkers tegen social engineering (SE) in industriële automatisering (IA) objecten van Rijkswaterstaat.
De hypothese in dit onderzoek luidt als volgt:
Kennis is niet de enige factor waardoor medewerkers niet overgaan tot veilig gedrag!!

1.3.2 Theoretisch deel

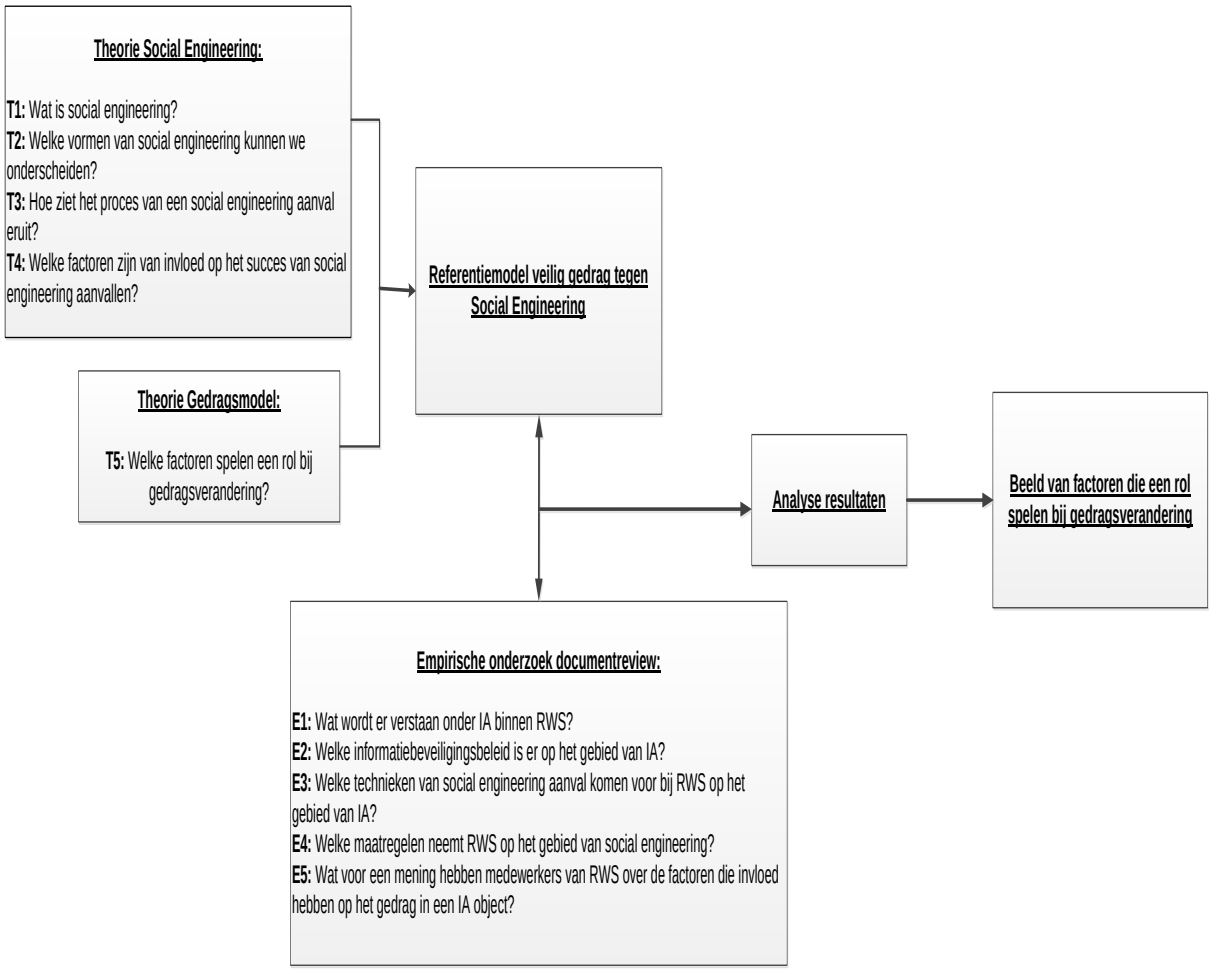
Wat is social engineering? (T1)
Welke vormen van social engineering kunnen we onderscheiden? (T2)
Hoe ziet het proces van social engineering aanval eruit? (T3)
Welke factoren zijn van invloed op het succes van social engineering aanval? (T4)
Welke factoren spelen een rol bij gedragsverandering? (T5)

1.3.3 Empirische deel

Wat wordt onder industriële automatisering (IA) verstaan? (E1)
Welk informatiebeveiligingsbeleid is er op het gebied van IA? (E2)
Welke technieken van social engineering aanval komen voor bij RWS op het gebied van IA? (E3)
Welke maatregelen neemt RWS op het gebied van social engineering? (E4)
Wat voor een mening hebben medewerkers van RWS over de factoren die invloed hebben op het gedrag in een IA object? (E5)

1.3.4 Onderzoeksmodel

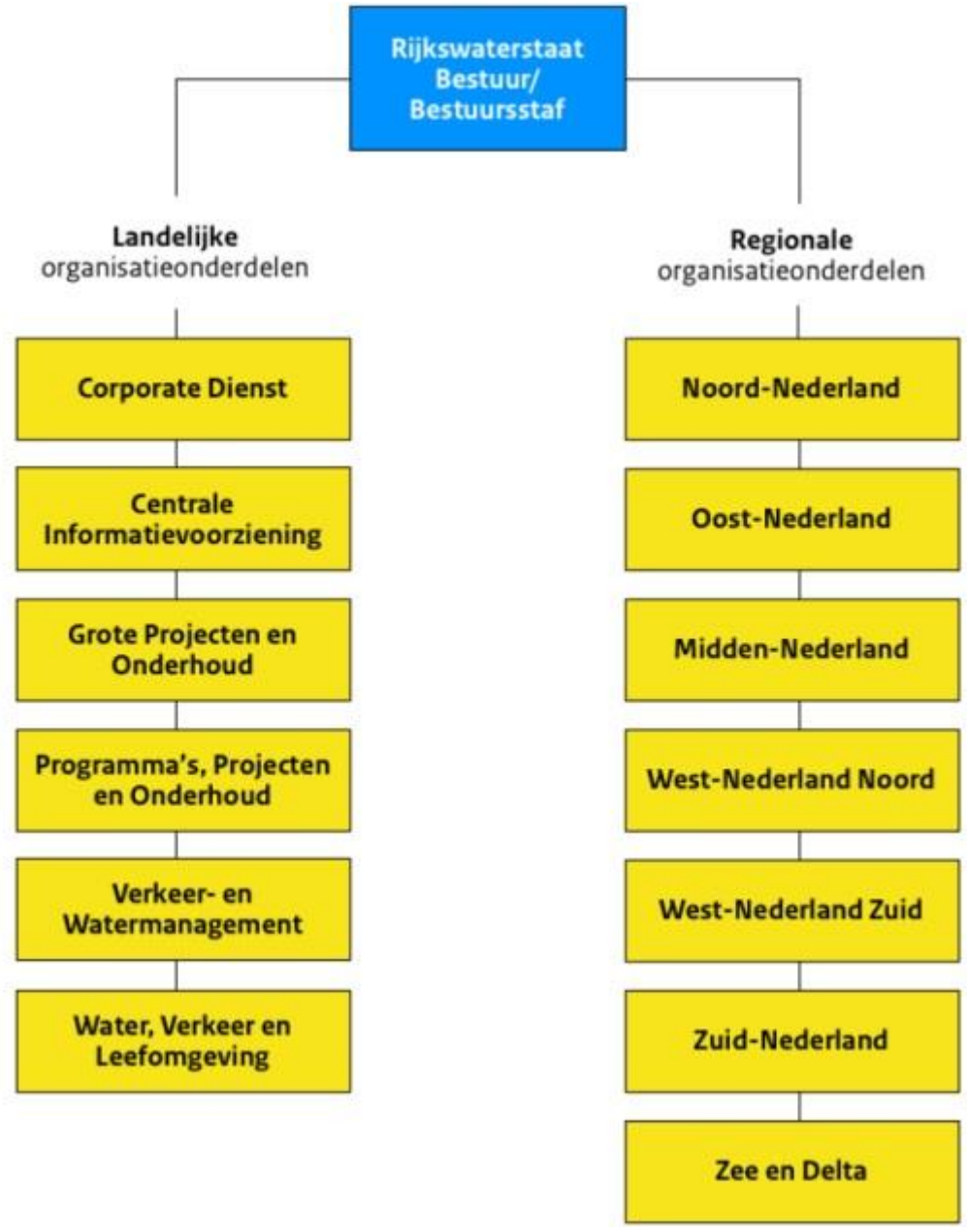
Hieronder in figuur 1 worden de opzet van dit onderzoek visueel weergegeven. Tijdens de literatuurstudie zijn eerst de theorieën over SE en het gedragsmodel bestudeerd, wat leidt tot een referentiemodel. Daarnaast heeft er een archiefonderzoek(documentreview) plaatsgevonden. Het referentiemodel is als toets kader gebruikt bij de invulling van de interviews en enquête voor het empirische onderzoek.



Figuur 1: Onderzoeksmodel

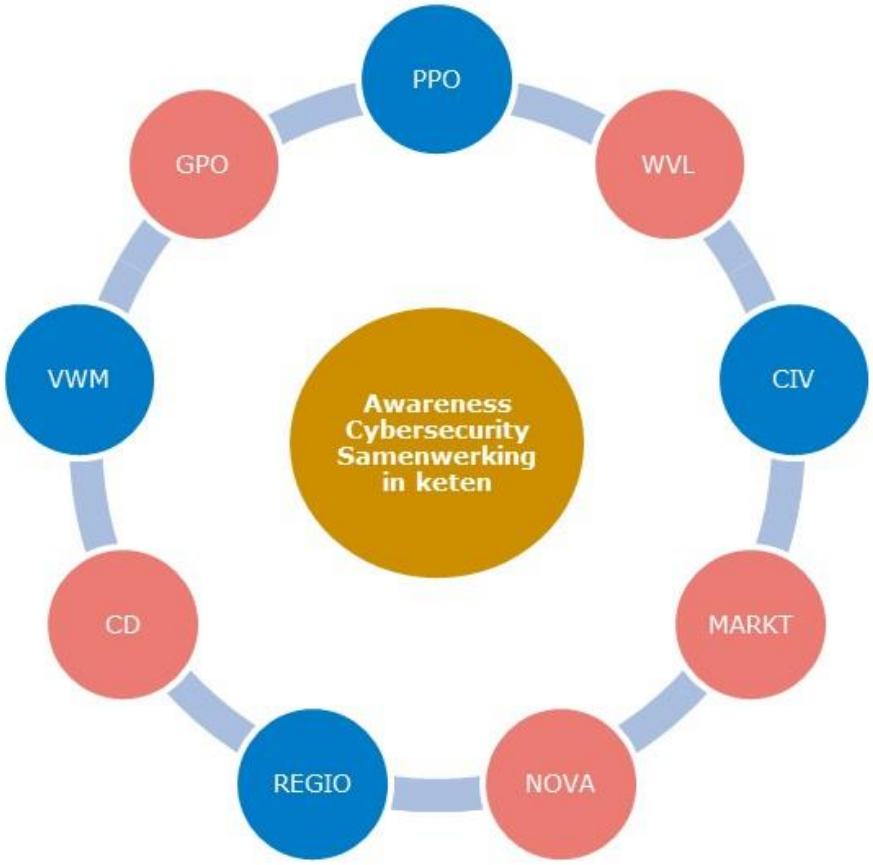
1.4 Scope

Dit onderzoek zal uitgevoerd worden binnen RWS. RWS heeft een complex en divers ICT landschap dat bestaat uit Industriële automatisering (IA) tot kantoorautomatisering. De scope van het onderzoek zal zich beperken tot de op IA van RWS.
RWS onderkent de volgende organisatieonderdelen zie figuur 2. RWS is onderverdeeld in landelijke organisatie onderdelen en regionale organisatieonderdelen.



Figuur 2: Organogram

In figuur 3 is aangegeven welke organisatieonderdelen binnen en buiten scope van dit onderzoek vallen. De blauw gearceerde bolletjes (organisatieonderdelen) vallen binnen de scope van dit onderzoek en de rode gekleurde bolletjes vallen buiten de scope.



Figuur 3: Scope onderzoek

Korte beschrijving van de organisatieonderdelen, die tot de scope behoren:

PPO: Verantwoordelijk voor allocatie van de productie, voorbereiding en uitvoering van onderhoud en oplevering van overdrachtsdossiers en toestandsrapportages (via de prestatiecontracten).

CIV: Verantwoordelijk voor de levering van netwerkdata (IGA), ondersteunende systemen t.b.v. datalevering (nu: Ultimo/Kerngis/DISK, straks AIR), VODK-contract (beheer DVM assets) en IA (IMPAKT/IA-bouwstenen). CIV heeft een afdeling die Security Center heet deze voert regie over de beveiliging van de IV- ketens van RWS en daarnaast is er SOC, het Security Operations Center deze bewaakt de informatievoorziening en Industriële automatisering van RWS tegen cyberdreigingen en reageert daar direct op als daar aanleiding toe is.

REGIO:

SLU: Is verantwoordelijk voor de verbinding tussen de RWS Regio en de landelijke uitvoeringseenheden van RWS bij het realiseren van de productie op en aan de netwerken van de regio. De Regisseur Assetmanagement is de verbinder van de Regio en de uitvoerende diensten (PPO, GPO, CIV) in de OG-ON-relatie.

District: Is ten alle tijden namens RWS aanspreekbaar op de toestand en het presteren van het areaal. Om deze rol in te kunnen vullen, werkt het district samen met de andere afdelingen in de keten.

VWM: Verantwoordelijk voor het waarborgen van de doorstroming op het areaal d.m.v. verkeersmanagement, stelt veilig bij verstoringen/storingen en levert aan de voorkant functionele eisen t.b.v. het presteren van het netwerk in de gebruiksfase.

In tabel 2 hieronder wordt aangegeven binnen welke organisatie onderdeel de onderzoeksgroepen vallen, die een belangrijke bijdrage hebben geleverd voor het tot stand komen van dit onderzoek.

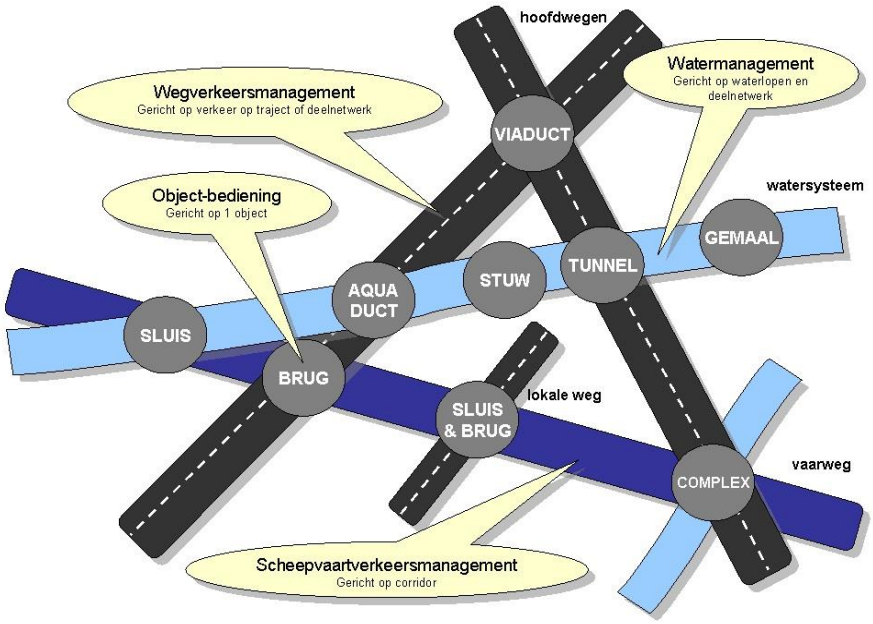
Organisatieonderdeel	Onderzoeksgroep	Definitie
PPO	Projectleden (IPM team)	Dit zijn mensen die de tunnelprojecten realiseren zonder direct betrokken te zijn met Cybersecurity.
CIV	Experts (Security)	Dit zijn mensen die de CSIR en Cybersecurity eisen hebben opgesteld voor contracten.
Regio	Objectbeheerders	Dit zijn de objectdeskundige en installatieverantwoordelijke.
VWM	Bedienaars	Bediening, bewaken van bijvoorbeeld tunnels en verkeerssignalering.

Tabel 2: Scope

IA in relatie met de processen van RWS

IA valt onder de volgende processen van RWS Aanleg & Onderhoud (AO) en Informatievoorziening (IV). De IA binnen RWS is onderverdeeld over de volgende organisatieonderdelen GPO, PPO,CIV. De benoemde organisatie onderdelen hebben tijdens de aanleg & onderhoud van infrastructurele projecten te maken met IA.

De drie netwerken Hoofdvaarwegennet (HVWN), Hoofdwegennet (HWN) en (Hoofdwaterstysteem) HWS staan met elkaar in verbinding door verschillende objecten. Dit is schematisch weergegeven in figuur 4. Deze objecten worden op afstand vanuit de verkeercentrale of lokaal bij het object bediend.



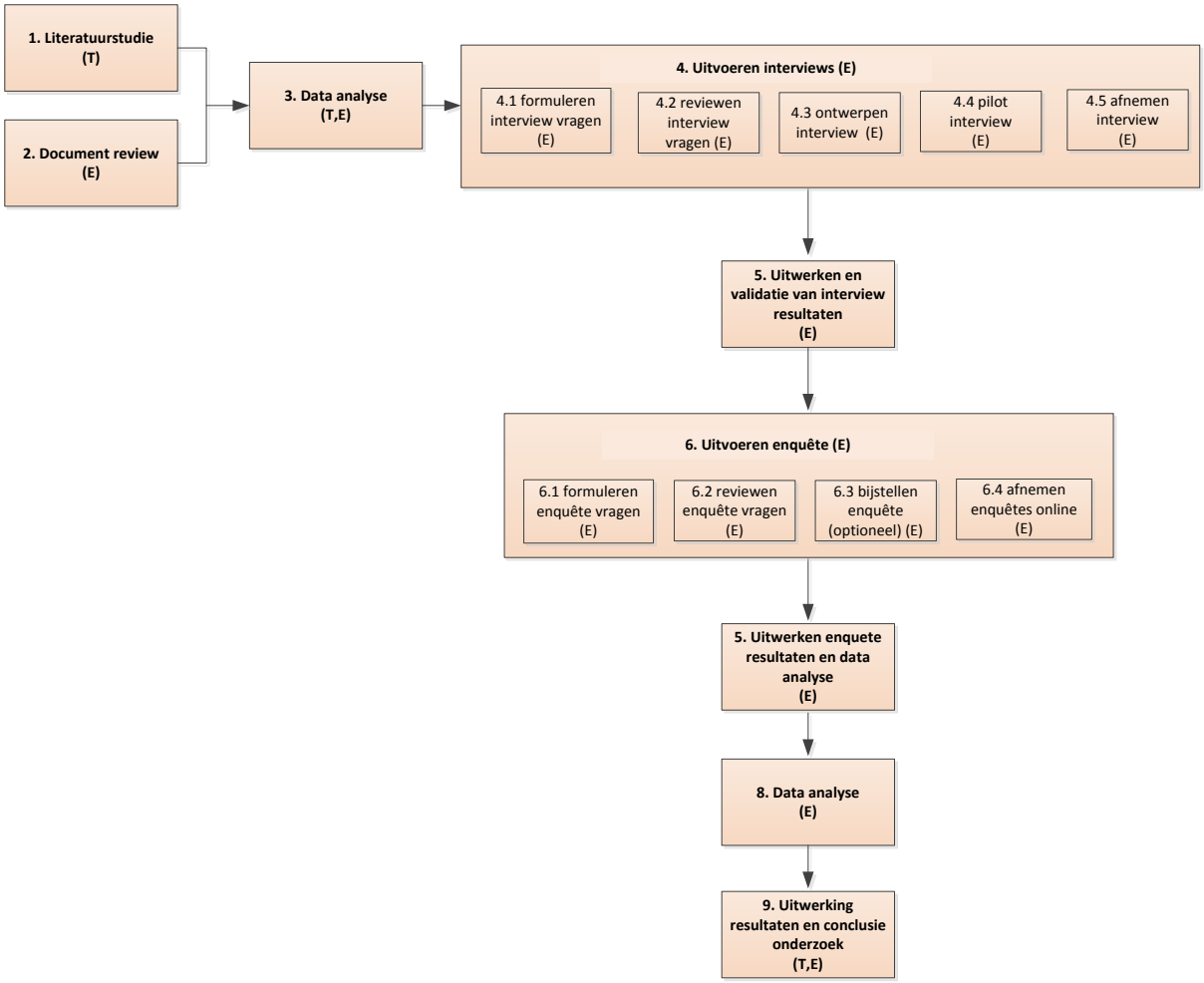
Figuur 4: Netwerken RWS (HVWN, HWN,HWS)
Bron: Inleiding EAR Architectuur Industriële Automatisering RWS 0.1

2. Methode van onderzoek

Voor het uitvoeren van een onderzoek moeten er bepaalde keuzes gemaakt worden zo ook over de te volgen aanpak van het onderzoek. In dit hoofdstuk wordt de onderzoeksmethode voor de uitvoering van dit onderzoek beschreven. Als eerste zal de onderzoekstrategie beschreven worden gevolgd door de gebruikte methoden van onderzoek. Hierna wordt de dataverzameling, betrouwbaarheid, validiteit en de ethiek van het onderzoek toegelicht.

2.1 Onderzoeksstrategie

Om het onderzoek op een gestructureerde wijze uit te kunnen voeren is een onderzoekstrategie bepaald. De onderzoeksstrategie beschrijft de opeenvolgende stappen, die doorlopen zullen worden bij het uitvoeren van het theoretische deel (T) en empirische deel (E) van het onderzoek (Saunders et al., 2011). De stappen zijn schematisch weergegeven in figuur 5.



Figuur 5: Stappenplan onderzoek

Hieronder worden de stappen beknopt beschreven:

Stap 1. Literatuurstudie
De literatuurstudie is bedoeld om meer informatie over het onderzoeksonderwerp te verzamelen. De resultaten van de literatuurstudie zullen als input worden gebruikt bij het opstellen van de interview/enquête vragen. Verder zal de literatuurstudie dienen om de theoretische deelvragen (T) te beantwoorden.

Stap 2. Document review
In de document review zal interne documentatie worden bekeken en geanalyseerd. De document review zal inzicht geven in wat RWS op het gebied van SE doet. De uitkomsten van de document review zullen vergeleken worden met de resultaat van de literatuurstudie en daarnaast worden deze resultaten gebruikt voor het opstellen van interview/enquête vragen. De document review levert informatie op voor de geformuleerde empirische vragen (E).

Stap 3. Data analyse
Na de literatuurstudie en de document review te hebben uitgevoerd zal een analyse uitgevoerd worden om het probleem beter te begrijpen. De resultaten van de data analyse worden gebruikt bij het verder formuleren van de interview/enquête vragen. Data analyse levert informatie op voor het theoretische deel (T) en het empirische deel (E) van het onderzoek.

Stap 4. Uitvoeren interviews
Voor wat betreft dit onderzoek was vooraf weinig inzicht in welke mate er kennis en aandacht is voor SE binnen IA van RWS. Om een beter beeld te krijgen hoe dit leeft is er voor gekozen om dit onderzoek op te splitsen in twee delen. Er is voor gekozen om de enquêtes validatie van de interviews te zijn. De interview vragen zullen worden geformuleerd op basis van de resultaten uit de literatuurstudie en data analyse.

In het eerste deel van dit onderzoek zijn er doormiddel van interviews open vragen gesteld. Hiermee wordt inzichtelijk gemaakt hoe dit onderwerp leeft bij de belangrijkste spelers (medewerkers) van RWS. Dit kan worden beschouwd als een exploratief (verkennend) onderzoek waarbij op basis van een uitgebreide literatuur studie de belangrijkste aspecten van SE worden bevraagd. Het gaat hierbij om kennis, risico's, houding en de subjectieve norm. Dit geeft een globaal beeld waar binnen RWS de belangrijkste issues en uitdagingen zitten voor SE.

De interview vragen zullen ter review aangeboden worden aan selecte groep personen en de experts. Na de review te hebben uitgevoerd kunnen eventueel de vragen worden aangepast (Saunders et al., 2011). Er wordt vervolgens een pilot interview gehouden om te bepalen of de interviews de gewenste resultaten opleveren en om de benodigde tijd te bepalen. Na het pilot interview kan de opzet van de interviews en de interview vragen eventueel bijgesteld worden. Hierna kunnen de echte interviews worden afgenomen. De interview vragen hebben betrekking op het empirische deel(E) van het onderzoek.

Stap 5. Uitwerken en validatie van interview resultaten
In deze stap worden de interview resultaten uitgewerkt en voorgelegd aan de geïnterviewde voor validatie. Om er zeker van te zijn dat er geen fouten zijn gemaakt tijdens het uitwerken van de interviews. Deze vragen hebben betrekking op het empirische deel van het onderzoek(E).

Stap 6. Uitvoeren enquête
In de tweede stap is er gekozen voor het uitzetten van een enquête waarbij de resultaten uit de interviews (eerste stap) de richting (zwaartepunt) bepalen. Hiermee krijgen we een nog scherper beeld en meer diepgang op de hiervoor genoemde 4 aspecten. Deels 'zoomen' deze vragen verder in op aspecten die ook in de interviews aan bod zijn gekomen.

Enerzijds wordt hiermee getoetst of de beelden die uit de interviews zijn opgehaald ook kloppen, een soort herbevestiging van de opgehaalde beelden.

Anderzijds wordt op sommige aspecten nog meer diepgang gezocht om nog een scherper beeld te krijgen van de meest belangrijke aspecten van SE. Enerzijds worden de resultaten van de interview gevalideerd bij de respondenten anderzijds worden verdiepings vragen gesteld.

De enquête vragen zullen ter review aangeboden worden aan een selecte groep personen en de experts (Saunders et al., 2011). Na de review te hebben uitgevoerd kunnen eventueel de vragen worden aangepast en vervolgens kan de enquête uitgevoerd worden.

Stap 7. Uitwerken enquête resultaten en data analyse
Met deze opzet kan een scherpe analyse worden gemaakt van de belangrijkste nalatigheden van SE binnen het bredere domein van IA binnen objecten van RWS. Dit vormt de basis voor het trekken van de juiste conclusies met bij behorende aanbevelingen voor het management van RWS. Deze vragen hebben betrekking op het empirische deel van het onderzoek (E).

Stap 8. Data analyse
Na de interview/enquête te hebben uitgevoerd zal een analyse uitgevoerd worden om interessante concepten en bevindingen te verzamelen. Data analyse levert informatie op voor het theoretische deel (T) en het empirische deel (E) van het onderzoek.

Stap 9. Resultaten theoretisch en empirisch
In deze stap worden de resultaten van theoretische deel (T) en empirische deel (E) van het onderzoek verder uitgewerkt. Verder wordt de hoofdvraag met bijbehorende deelvragen beantwoord. Hieruit volgende de conclusies en aanbevelingen van het onderzoek.

2.2 Onderzoeksmethoden

Voor het uitvoeren van het onderzoek wordt het boek ‘Methoden en technieken van onderzoek’ (Saunders et al., 2011) gehanteerd. Vanuit dit boek zijn de meest geschikte onderzoeksmethoden voor de uitvoering van dit onderzoek geselecteerd. Voor het bepalen van de onderzoeksmethoden zijn onderzoeksvragen en de beschikbare tijd als uitgangspunt genomen. In deze paragraaf worden de gekozen onderzoeksmethodes voor de uitvoering van dit onderzoek beschreven.

<u>Enquête/ vragenlijst</u>
Een enquête is een populaire methode waarbij een vragenlijst gebruikt wordt om gegevens te verzamelen voor een onderzoek. De vragenlijst wordt doorgaans onder meerdere respondenten verspreid. De enquête wordt met name gebruikt om antwoorden te krijgen op “wie, wat, waar en hoeveel” vragen en is een deductieve methode. (Saunders et al., 2011, pg 121). Vragenlijsten worden voornamelijk ingezet om kwantitatieve gegevens te verzamelen.

Verder kan door gebruik te maken van een enquête in een korte tijd een grote hoeveelheid gegevens verzameld worden uit een grote onderzoekspopulatie. De gegevens worden met behulp van een gestructureerde vragenlijst verzameld en gestandaardiseerd waardoor deze gemakkelijk met elkaar vergeleken kunnen worden.

De beperkte tijd die er is voor het uitvoeren van dit onderzoek maakt deze methode zeer geschikt om in korte tijd relevante gegevens te verzamelen. De gegevens zullen verzameld worden door gebruik te maken van zowel vragenlijsten als het afnemen van (semi) gestructureerde interviews.

<u>Case-study</u>
De case-study methode wordt vooral gebruikt in een verklarend of verkennend onderzoek. Deze methode is met name interessant al men een goed begrip wil krijgen van de context en de processen van een onderzoek. Een case-study wordt meestal gebruikt om de “waarom” vraag te beantwoorden. Er zijn vier soorten case-study methodes verdeeld over twee dimensies:”
Enkelvoudige case (één organisatie) of meervoudige case (meerdere organisaties).
Holistische case (een bedrijf wordt al geheel onderzocht) of ingebedde case (een aantal logische eenheden bijv. afdelingen of werkgroepen binnen een bedrijf worden onderzocht.)

Voor dit onderzoek zal een case-study gebruikt worden om de hoofdvraag te kunnen beantwoorden. Om de resultaten van dit onderzoek te kunnen vergelijken met andere onderzoeken zal de onderzoeker uitgaan van een meervoudige case-study. Aangezien dit onderzoek uitgaat van het onderzoeken van meerder afdelingen binnen één organisatie zal er uitgegaan worden van een ingebedde case.

Archiefonderzoek
Een archiefonderzoek (document review)is een methode waarbij documenten en administratieve gegevens als bron gebruikt worden. De gegevens en documenten kunnen uit het verleden en/ of recente documenten zijn. Een archiefonderzoek is geschikt om gegevens te verkrijgen om de huidige situatie in kaart te brengen. De methode wordt vaak toegepast om onderzoeksvragen die gericht zijn op het verleden en de verandering in de loop van de tijd te beantwoorden.

Een archief onderzoek is een kwantitatieve methode met een inductieve benadering. Bij een archiefonderzoek kan het voorkomen dat de onderzoeker niet altijd de informatie kan vinden waar deze naar op zoek is. Dit kan komen doordat sommige documentatie en informatie vertrouwelijk is en dus niet altijd toegankelijk voor de onderzoeker.

Voor dit onderzoek zal een archiefonderzoek uitgevoerd worden om informatie te verzamelen over het huidige informatiebeveiligingsbeleid binnen RWS. Niet alle informatie rondom informatiebeveiliging zal beschikbaar zijn. Met de informatie die beschikbaar is zal getracht worden een zo compleet mogelijk beeld te krijgen.

Om de hoofdvraag met bijbehorende deelvragen te kunnen beantwoorden zal dus een combinatie gebruikt worden van een enquête, casestudy en een archiefonderzoek (documentreview).

2.2.1 Dataverzameling

Zoals in voorgaande paragraaf beschreven wordt er een combinatie van 3 onderzoeksmethoden gebruik in dit onderzoek. In deze paragraaf worden de dataverzamelingstechnieken beschreven die gebruikt zullen worden.

Documentreview
Voor het onderzoek is een documentreview uitgevoerd. Tijdens de documentreview zijn verschillende documenten uitgebreid geanalyseerd om relevante gegevens te verzamelen zie tabel 3 voor gebruikte documenten. De documenten zijn geselecteerd op basis van de volgende kernwoorden:

- Informatiebeveiliging
- Cyber Security
- Industriële automatisering
- System Engineering
- Leidraad SE

Documentnaam	Beschrijving	Versie/Jaar	Documenttype/ Overig
Baseline Informatiebeveiliging Rijksdienst (BIR)	De Baseline Informatiebeveiliging Rijksdienst (BIR) schrijft het basisniveau voor informatiebeveiliging bij de Rijksoverheid voor.	1.0 / 01 december 2012	PDF
Baseline Informatiebeveiliging Rijkswaterstaat (BIR RWS)	De Baseline Informatiebeveiliging Rijkswaterstaat (BIR RWS) is een vertaalslag en invulling van de BIR voor de	1.1/ 11 november 2013	PDF

	beveiliging van de Informatievoorziening (IV) van RWS.		
Cybersecurity Implementatierichtlijn Objecten RWS (CSIR)	De CSIR beschrijft de maatregelen die specifiek van toepassing zijn op de Industriële Automatisering van Rijkswaterstaat.	1.01 / 02 december 2013	PDF
Handreiking industriële automatisering	Aanwezigheid van goede assetmanagement- en cybersecurityprocessen voor beheersing van Industriële automatisering	Juni 2016	PDF
Inleiding Architectuur Industriële automatisering	Identificeren van de kernelementen uit de bestaande architectuurproducten	0.1 / 7 juli 2011	PDF
Architectuur voor industriële automatisering bij Rijkswaterstaat	Architectuur van de IA	0.99 / 10 februari 2011	PDF
Security by Design IA	security by design in V model		PowerPointpresentatie
Speerpuntenbrief RWS	Bestuur	2018	WORD
Response-Ability RWS-Strategie 2014 Digitale Beveiliging voor RWS infrastructuur	Beveiligde Werken, Beveiligde Infrastructuur	2014	WORD
Bestuurbesluit	Beveiligde Werken, Beveiligde Infrastructuur	2013	WORD
Procesbeschrijving SE	System Engineering	versie 2.1.2 (25 januari 2017)	PDF
Inleiding EAR Leidraad SE	System Engineering	versie 3.0 (19 november 2013)	PDF

Tabel 3: documentreview

Semigestructureerde interviews

Aan de hand van de bestudeerde literatuur en de hoofdvraag en deelvragen zijn interviewvragen geformuleerd. Alvorens de interviews af te nemen zijn de interviewvragen ter review aangeboden aan de afstudeerbegeleider van de Open Universiteit voor een check en begeleider vanuit RWS. Na deze review zijn de interviewvragen verder aangescherpt en aangepast.

Hierna is een pilot-interview uitgevoerd om te bepalen hoeveel tijd er nodig zal zijn voor het afnemen van een interview en om te bepalen of het interview de gewenste data oplevert. Na het pilot-interview zijn nog een aantal wijzigingen doorgevoerd. Na het pilot-interview zijn deelnemers benaderd om de interviews in te plannen. Dit is gebeurd door het opstellen en versturen van een mail zie bijlage 1. In deze mail heeft de onderzoeker zich kort geïntroduceerd en daarnaast is het doel van het onderzoek

nader toegelicht en de vraag gesteld om deel te nemen aan het onderzoek. Na een bevestiging te hebben ontvangen van deelname zijn in overleg de afspraken ingepland. Bij het inplannen van de afspraken zijn ook de interviewvragen van te voren toegestuurd, zodat de deelnemers zich konden voorbereiden en de onderzoeker zo de juiste informatie kon krijgen.

Na het afnemen van het interview zijn de uitwerkingen naar de deelnemers gestuurd voor een controle. Zie bijlage 2 voor de interview vragen.

Enquête
Voor het uitzetten van de enquête is een andere aanpak gehanteerd dan bij de interviews. Bij het uitzetten van een enquête moet de onderzoeker expliciet goedkeuring van een afdelingsmanager of manager vragen. Dit is nodig omdat het om capaciteit en dus geld gaat. Bij een enquête kan het ook gaan om vertrouwelijke informatie waar ook de goedkeuring voor nodig is.

De enquête vragen zijn opgesteld aan de hand van de interview resultaten en de documentanalyse. In de enquête zijn alleen gesloten vragen gesteld en daarmee dus kwantitatief van aard. Er zijn verschillende soorten vragen in de enquête opgenomen waaronder meerkeuze en schaal vragen. De enquête vragen zijn voorgelegd aan de afstudeerbegeleider en begeleider vanuit RWS voor een review. Na het verwerken van het reviewcommentaar is de enquête afgestemd met de begeleider vanuit RWS, na goed keuring is de enquête rond gestuurd naar de medewerkers om de gegevens te verzamelen. Zie bijlage 3 voor de ingevulde enquête resultaten.

2.2.2 Betrouwbaarheid

Er dient voldoende aandacht besteed te worden aan de betrouwbaarheid van het onderzoek. Om de betrouwbaarheid te beoordelen is rekening gehouden met de volgende zaken:

- Deelnemersvertekening
  Bij het afnemen van de interviews en de enquête is het belangrijk dat de respondenten zonder sociale wenselijkheid kunnen antwoorden. Om te voorkomen dat er deelnemersvertekening optreedt is er voor anonimiteit gezorgd en zijn de respondenten hier vooraf over geïnformeerd. De verwerkte interview resultaten zijn ook in geanonimiseerde vorm aan de respondenten aangeboden, zodat deze zelf kunnen zien dat hun antwoorden anoniem worden gebruikt in het onderzoek. Ook is er gecommuniceerd naar de respondenten, dat deze bij vragen en onduidelijkheden contact kunnen opnemen met de onderzoeker.
- Robuustheid van de vragenlijst

2.2.3 Validiteit

Een ander belangrijk punt waar aandacht aan besteed moet worden tijdens het onderzoek is validiteit. De onderzoeker wil er zeker van zijn dat hij meet wat hij wil weten. Verder is het belangrijk dat er geen systematische fouten worden gemaakt in het onderzoek.

Interne validiteit
De interne validiteit gaat er over dat de onderzoeker meet wat hij wil meten. Hierbij is de vragenlijst een belangrijk onderdeel. Er moet voor gezorgd worden dat het gene wat met de vragenlijst wordt ontdekt ook daadwerkelijk het gene is wat men wil meten. De vragenlijst moet dus valide zijn. Om ervoor te zorgen dat de vragenlijst een valide instrument is welke in het onderzoek wordt gebruikt is de constructvaliditeit onderzocht.

De vragenlijst is aan een aantal expert waaronder de afstudeerbegeleider en begeleider vanuit RWS voorgelegd om te beoordelen of de vragen die in de vragenlijst zijn opgenomen ook daadwerkelijk bijdragen aan de onderzoeksvragen. Dit is gedaan om inzichtelijk te krijgen welke vragen essentieel zijn, nuttig zijn maar niet essentieel of niet noodzakelijk. Op deze wijze is er naar een vragenlijst toegewerkt die voldoende essentiële vragen bevat. Aan het empirische onderzoek ligt ook een uitgebreid literatuuronderzoek te grondslag.

Externe validiteit
Om externe validiteit te bereiken moeten de resultaten van het onderzoek gegeneraliseerd kunnen worden. Dit betekent dat de uitkomsten van het onderzoek ook zouden moeten gelden in vergelijkbare situaties. Het onderzoek is uitgevoerd binnen RWS gericht op SE en het informatiebeveiligingsbeleid binnen IA. Het informatiebeveiligingsbeleid is van toepassing op de gehele IA van RWS. De uitkomsten zouden ook van toepassing kunnen zijn binnen andere vergelijkbare organisaties maar dit is niet onderzocht. De uitkomsten van de bekendheid van de medewerkers rondom SE zijn niet generaliseer baar binnen andere organisaties daar er maar een kleine populatie is gebruikt in dit onderzoek..

2.2.4 Ethiek

Bij een mens gebonden onderzoek heeft men te maken met ethiek. Het is hierbij belangrijk dat de onderzoeker op de hoogte is van de kaders en hiernaar handelt. Het is belangrijk om rekening te houden met de volgende zaken:

- Deelnemers worden vooraf geïnformeerd over het doel van het onderzoek.
- Deelname op vrijwillige basis gebeurt en hierbij de instemming van de deelnemers gevraagd wordt.
- Er zorgvuldig wordt omgegaan met de persoonsgegevens van de deelnemers en verzamelde gegevens voor het onderzoek.
- Het onderzoek controleerbaar en onafhankelijk is.

Voor dit onderzoek:

- Zijn alle deelnemers vooraf geïnformeerd over het doel van het onderzoek. De deelname aan de enquête en interviews gebeurd op vrijwillige basis. De enquête wordt volledig anoniem afgenomen en de namen van de geïnterviewde worden geanonimiseerd. De namen zijn alleen bekend bij de onderzoeker en zal vertrouwelijk mee omgegaan worden. Verder worden de deelnemers in staat gesteld om de uitwerking van hun interview te controleren om eventuele onjuistheden aan te passen of aan te gegeven dat bepaalde gegevens niet gebruikt mogen worden.
- Zal de deelname aan het onderzoek op vrijwillige basis geschieden, hierbij zal expliciet de instemming van de deelnemers gevraagd worden. Er wordt een geïnformeerde toestemming gevraagd van de deelnemers.
- Worden de verzamelde (persoons)gegevens ten behoeve van dit onderzoek als vertrouwelijk beschouwd en behandeld. Zoals eerder aangegeven zal er vertrouwelijk omgegaan worden met de gegevens van de deelnemers.
- Wordt ernaar gestreefd om het onderzoek controleerbaar te houden en zo onafhankelijk mogelijk uit te voeren. De onderzoeker voert het onderzoek zelfstandig uit. De begeleiders zijn geraadpleegd en gevraagd advies te geven over de aanpak en de herhaalbaarheid van het onderzoek te borgen.

3. Literatuurstudie

Dit hoofdstuk bevat de literatuurstudie welke is uitgevoerd ten behoeve van het onderzoek. De literatuurstudie is gebaseerd op de theoretische deelvragen met betrekking tot SE. Als eerst zullen de zoekstrategie en selectiecriteria toegelicht worden. Daarna worden de theoretische deelvragen beantwoord.

3.1 Zoekstrategie

ZOEKSTRATEGIE & SELECTIECRITERIA
Om de theoretische deelvragen te beantwoorden is een literatuuronderzoek uitgevoerd. Voor dit doel wordt het proces van literatuurstudie (Saunders et al., 2011) gevolgd om literatuur te vinden die op iedere onderzoeksvraag een onderbouwd en kritisch antwoord kan geven. Dit proces zorgt voor verfijning en filtering van de bruikbare literatuur bij iedere iteratie: zoektermen definiëren, zoeken, literatuur vastleggen, literatuur beoordelen en notities maken, en conceptoverzicht uitwerken.

Deze zoekmethode is aangevuld met de sneeuwbalmethode. Deze methoden zijn gebonden aan voorwaarden zoals hieronder beschreven in de zoekstrategie. Er is gezocht binnen Engels- en Nederlandstalige publicaties. Verder is gefilterd op “scholarly and peer reviewed” publicaties en is gezocht binnen het veld business, engineering en computer science.

De volgende databases werden voor deze studie gebruikt: De Digitale bibliotheek van de Open Universiteit en Scholar google. De Digitale Bibliotheek van de Open Universiteit is, te vinden via de link http://bibliotheek.ou.nl/.

De volgende zoektermen gecombineerd met de Boolean operator AND zijn gebruikt om relevante publicaties te vinden via de Digitale bibliotheek van de Open Universiteit:

- social engineering AND attacks: 19801 resultaten
- social engineering AND attacks AND wetware: 20 resultaten
- social engineering AND attacks AND phishing : 873 resultaten
- social engineering AND attacks AND phishing AND security awareness: 300 resultaten
- social engineering AND attacks AND phishing AND security awareness AND information security: 300 resultaten
- social engineering AND attacks AND phishing AND security awareness AND information security AND business: 254 resultaten
- social engineering AND attacks AND phishing AND security awareness AND information security AND business AND costs: 188 resultaten

De volgende zoektermen zijn gebruikt om relevantie publicaties te vinden via scholar.google.com:

- behavior AND principle
- behavior AND principle AND theory
- behavior AND principle AND theory AND model
- gedrag AND principe
- gedrag AND principe AND theorie
- gedrag AND principe AND theorie AND model
- gedrag AND informatiebeveiliging
- behavior AND informationsecurity

De gevonden publicaties met de zoekstrategie met minder dan 200 resultaten zijn toegevoegd aan de Endnote Library. Duplicaten zijn hiermee verwijderd. Relevante publicaties zijn in eerste instantie bepaald op basis van titel en abstract. Niet al de gevonden (wetenschappelijke) artikelen en boeken waren relevant voor dit onderzoek.

Het doorlezen van deze relevante publicaties leidde tot het vinden van referenties naar andere artikelen, die weer leidde tot nieuwe relevante artikelen. De door de sneeuwbalmethode gevonden artikelen zijn ook gebruikt voor dit onderzoek.

Resultaten literatuur	
Gevonden artikelen	208
Relevante artikelen na lezen titel en abstract	15
Relevante artikelen gevonden door sneeuwbaleffect	14
Relevante artikelen gevonden via Google	8

Tabel 4: Resultaten literatuur

Op basis van deze zoekstrategie en selectiecriteria kwamen er enkele tientallen peer-reviewed wetenschappelijke artikelen en boeken uit. Hierboven in tabel 4 zijn de resultaten weergegeven. De relevante artikelen en boeken zijn vervolgens bestudeerd en op basis daarvan zijn de theoretische deelvragen beantwoord. In paragraaf 3.2 staan de resultaten van de literatuurstudie uiteengezet. De betreffende wetenschappelijke artikelen zijn opgenomen in de literatuurlijst. De gebruikte referentiestijl is APA versie 6.

3.2 Wat is Social Engineering (T1)?

We leven in een tijd van digitalisering en een vergaande dataficatie van de samenleving. Dit vormt een grote uitdaging bij het beschermen van deze kritieke infrastructuren tegen computer gedragen aanvallen. Deze bedreigingen kunnen variëren van computerfouten (Madani en Novosel, 2005; Van Eeten *et al.*, 2006) tot aanvallen door hackers en terroristen (Cieslewicz, 2004; Li *et al.*, 2005; Luiijf en Klaver, 2004; Wilson, 2006).

Overheden en industrieën hebben hun beveiligingssystemen onderzocht om hun kritieke informatie te beschermen. Daar*en*tegen zijn cyberaanvallen tegenwoordig erg complex en kunnen niet worden opgelost met behulp van de klassieke beveiligingsmethoden.
Met andere woorden, de technische beveiliging van de meeste kritieke infrastructuursystemen *staat op een hoog niveau*, maar deze systemen blijken erg kwetsbaar voor aanvallen door social engineers. (intern, extern of beide)

Sociale engineering is de moeilijkste vorm van aanval om een organisatie *tegen te* verdedigen, omdat het niet alleen kan worden *beveiligd door* hardware en software. Het vereist een effectieve informatiebeveiliging, die alle aspecten van dit fenomeen kan weerstaan.

Social engineering (SE) komt in de literatuur neer op verschillende definities en interpretaties van dit fenomeen, maar de gemeenschappelijke factor bij al deze definities en interpretaties is dat social engineers zich op mensen, systemen of beide richten om persoonlijke of kritieke werk gerelateerde informatie te verkrijgen. De aanvaller probeert meestal een geloofwaardig verhaal te vertellen om het vertrouwen van zijn slachtoffer te winnen. De verhalen kunnen inhoudelijk bestaan uit basis menselijke instincten, zoals: hebzucht, sympathie of angst (Townsend, 2010).

3.2.1. Definities Social enginering

In tabel 5 is een verzameling gemaakt van een aantal definities van SE wat je terug vindt in de literatuur.

Definitie	Bron
“Met betrekking tot het gebied van informatiesystemen is het uiteindelijke doel van een social engineer zich directe toegang te verschaffen tot de informatie van een bedrijf, zowel fysiek als digitaal, door middel van zijn informatiesystemen.”	Thornburg (2004)
“In tegenstelling tot traditionele hacking methodes, waar de aanvaller technisch uitgerust moet zijn om een aanval uit te voeren, moet een social engineer zich richten op zijn sociale vaardigheden om een succesvolle aanval uit te voeren”	Ivaturi., et al(2011)
“Sociale engineering is de kunst om gebruikers te verleiden tot informatie over informatiesystemen. In plaats van technische aanvallen op systemen richten social engineers zich op mensen met toegang tot informatie, manipuleren ze om vertrouwelijke informatie uit te geven of zelfs hun kwaadaardige aanvallen door invloed en overreding uit te voeren.”	Krombholz et al., (2015)
“Sociale techniek is de kunst om de zwakste schakel in informatiebeveiligingssystemen te exploiteren: de mensen die ze gebruiken.”	Chitrey., et al (2012)

Een vorm van hacken die vooral toegepast wordt door manipulatieve hackers. Met behulp van flink wat mensenkennis proberen zij personen zo gek te krijgen om gevoelige (computer)informatie prijs te geven.	http://www.encyclo.nl/lokaal/10273
Een term waarbij een persoon word verleid om informatie door te geven, die normaal toegankelijk is door vreemden. Vaak wordt gebruikt gemaakt van een of andere verhaal of smoes om het slachtoffer zo ver te krijgen dat hij behulpzaam alle veiligheidsprocedures aan zijn laars lapt.	http://www.encyclo.nl/lokaal/10433

Tabel 5: Definities uit de literatuur van het begrip “Social engineering”

Bovenstaande definities zijn uit de literatuur verzameld en gecombineerd tot een eigen definitie:
SE is het verkrijgen van informatie door personen te beïnvloeden met als doel toegang te krijgen tot bedrijf vertrouwelijke informatie. De social engineer zet hierbij social vaardigheden en mensen kennis in om de mens als zwakste schakel zodanig te manipuleren om gevoelige informatie prijs te geven.

SE is onderverdeeld in drie categorieën, namelijk; Soorten aanval, kanalen en operatoren uitvoerders (exploitanten) (Krombholz et al., 2015).

Gezien het groeiende aantal literatuurstukken en verschillende definities over dit fenomeen, gebeurt SE eerst op de mens, de software of een combinatie van beide. Vervolgens moeten verschillende soorten aanvallen worden gecategoriseerd volgens de bovengenoemde factoren.

Het doel van social engineer is het verkrijgen van directe toegang tot informatie of informatiebronnen van organisaties, zoals bedrijven en overheden (Thornburg, 2004). Dit kan zowel fysieke als digitale toegang zijn. Het middel waarmee social engineers deze informatie proberen te bemachtigen is niet in eerste instantie van technische aard, zoals het bij hackers wel het geval is. Social engineers bereiken namelijk hun doel, de informatie, via de mensen die deze informatie(bronnen) gebruiken of beveiligen.

De social engineer overtuigt mensen om vertrouwelijke informatie prijs te geven, zodat die bij de informatie(bron) kan komen. Social engineers doen dit door gebruik te maken van hun sociale vaardigheden (Brody et al., 2012; Krombholz et al., 2015). Verschillende auteurs geven aan dat manipulatie en emoties belangrijke factoren zijn in het verkrijgen van deze informatie binnen informatiesystemen (Applegate, 2009; Greiner, 2008; Krombholz et al., 2015; Mitnick & Simon, 2011; Peltier, 2006; Thornburgh, 2004). Een belangrijke emotie die veelvuldig wordt gebruikt in SE is het scheppen van vertrouwen bij de mensen waarvan ze informatie willen verkrijgen.

3.3 Welke vormen van Social Engineering kunnen we onderscheiden (T2)?

In deze paragraaf worden als eerst de type aanvallen van SE nader toegelicht. Vervolgens worden de technieken van social engineering beschreven. Tot slot worden de kanalen waarlangs een SE zijn informatie verzameld beschreven.

3.3.1 Type Social engineering aanvallen

SE aanvallen kunnen eenvoudig of zeer ingewikkeld zijn: hieronder leg ik de verschillende vormen uit met een korte omschrijving.

Physical
De aanvaller in deze vorm probeert zijn/haar slachtoffers te overtuigen om een gegeven actie uit te voeren. De aanvaller in deze vorm voert gewoonlijk eerder onderzoek uit en gebruikt bekende informatie zoals: geboortedatum, postadres, enz. Een vaak gebruikte methode bij dit soort aanvallen wordt ‘dumpster diving’ genoemd, waarbij de aanvaller door de afvalbakken van een persoon of organisatie zoekt (Granger, 2010).

Social
Dit type SE aanval is de meest succesvolle. De aanvaller in deze vorm vertrouwt op principes die door Cialdini (2001) zijn aangewezen, en gebruikt de (beweerde) autoriteit. Krombholz et al., (2015) identificeerde de ‘speer phishing’ aanvallen, waar de aanvaller zijn/haar sociale vaardigheden gebruikt om een relatie met zijn toekomstig slachtoffer te ontwikkelen. De manipulatie van het slachtoffer via telefoon wordt vaak als een succesvolle methode gemeld in dit type aanval (Granger, 2010).

Reverse sociale engineering
Dit is een indirect type aanval, waarbij de aanvaller het slachtoffer wil beïnvloeden en dwingt om namens hem acties uit te voeren. Gemeenschappelijke voorbeelden van dit soort aanvallen zijn e-mail ‘phishing’ en ‘spear phishing’ (Irani et al., 2011). Volgens Nelson (2008) bevat dit soort aanvallen drie belangrijke onderdelen: sabotage, reclame en hulpverlening. Bijvoorbeeld: De aanvaller vertrouwt eerst op een of andere vorm van ‘Baiting’ om de nieuwsgierigheid van zijn/haar slachtoffer op te wekken en wacht vervolgens op zijn/haar slachtoffer om de eerste aanpak te maken en vervolgens contact te maken.

Deze vorm van SE aanvallen is zeer gebruikelijk voor online sociale netwerken (Irani et al., 2011). Net als via sociale netwerken kan de aanvaller een groot aantal geregistreerde gebruikersaccount en informatie bereiken, en kan ook filter gebaseerde detectietechnieken omzeilen.

Technical
Dit soort aanvallen op het gebied van SE vindt voornamelijk online plaats (Krombholz et al., 2015). Tegenwoordig hebben de meeste van ons dagelijkse activiteiten een internetverbinding nodig. Sociale engineers leggen hun focus daarom op de wachtwoorden van online gebruikers, gebruikersnamen en kritieke persoonlijke en werk gerelateerde informatie.

Social technical
De sociaal-technische vorm van sociale engineering aanvallen kan een of alle vormen van bovengenoemde vormen van aanvallen inhouden. De meest voorkomende type aanval is ‘Bating’ (Stasiukonis, 2006) door malware- geïnfecteerde usb in een kantoor te laten liggen, ‘phishing’ door e-mails te sturen waar het zich richt op een grote groep mensen en ‘spearphishing’ (Jagatic et al., 2007) waar aanvallen eerst zijn

3.3.2 Technieken van social engineering

SE aanvallen kunnen in verschillende vormen plaats vinden, En zoals ik hierboven noemde, streven de social engineers altijd naar de zwakste link in een netwerk waar overal mensen betrokken zijn. De volgende technieken zijn de meest voorkomende vormen van sociale techniek.

Phishing
Deze techniek is de meest voorkomende vorm van aanval in e-mails en sms'jes, waar een social engineer een gevoel van angst, urgentie of nieuwsgierigheid creëert bij zijn/haar slachtoffers. Deze techniek kan gebruikt worden in verschillende vormen van web-browsen naar webdiensten (Krombholz et al., 2015; Irani et al., 2011; Granger, 2010).

Spear phishing
Deze techniek is een meer gerichte versie van de 'phishing', waar een sociale engineer een specifiek individu of bedrijf kiest. Deze techniek is veel moeilijker te detecteren in een systeem en kent een hoger succespercentage (Krombholz et al., 2015; Irani et al., 2011).

Ransomware
Deze techniek wordt meestal gecombineerd met phishing-email. Social engineers versturen meestal een bijlage met een bestandsextensie van ". PDF, .zip, .rar, etc. "die het nietsvermoedende slachtoffer passeert en de lading aflevert. Deze techniek kan de harde schijf van een computer coderen en vereist een bitcoin-betaling om het te ontgrendelen (Irani et al., 2011).

Baiting
Deze techniek maakt gebruik van een valse belofte om een slachtoffer te begroeten. Social engineers lokken gebruikers in de val en stelen hun slachtoffer persoonlijke en werk gerelateerde informatie. Deze techniek infecteert ook het slachtofferbesturingssysteem met een malware. 'Baiting' kan fysiek gebeuren door een virus bevattende USB in een kantoor of online te brengen (Granger, 2010).

Dumpster diving
Dit is de techniek om door de papieren/afval van een individu of bedrijf te zoeken. Soms bevatten deze papieren gevoelige informatie en het lekken hiervan naar social engineers kan aanzienlijke schade veroorzaken (Irani et al., 2011).

Shoulder surfing
Deze techniek omvat de fysieke aanwezigheid van een social engineer, omdat de social engineer de benodigde informatie proberen te krijgen door te observeren en te kijken naar zijn/haar slachtoffer (Granger, 2010).

Waterholing
Alvorens deze techniek op zijn/haar slachtoffer toe te passen, neemt een social engineer wat tijd om het gedrag van zijn slachtoffer te observeren. Vervolgens stuurt hij de malware en vangt de benodigde informatie op. (Krombholz et al., 2015; Irani et al., 2011).

Pretexting
Hier verkrijgt een social engineer informatie door een reeks zorgvuldig opgestelde leugens. De oplichting wordt vaak geïnitieerd door een social engineer, die voordoet alsof hij persoonlijke of werk gerelateerde informatie van zijn/haar slachtoffer nodig heeft om een kritieke taak uit te voeren (Henry, 2014; Workman, 2008).

Advanced persistent threat
Deze techniek heeft een langdurige tijdsinvestering nodig van een social engineer. Social engineers die deze techniek gebruiken, zijn in staat om continue/onafgebroken in een computersysteem te interveniëren. (Krombholz et al., 2015)

3.3.3 Kanalen

De kanalen waarlangs een sociale engineer informatie probeert te verzamelen, zijn belangrijk om te begrijpen en het is ook belangrijk om de zwakheid en de sterkte van elke kanaal binnen een organisatie te testen.

Onze dagelijkse activiteiten zijn sterk afhankelijk van computers, mobiele telefoons, tablets, enz., en we hebben ook een internetaansluiting nodig om toegang te krijgen tot verschillende soorten informatie. Daarom bestaan er veel verschillende kanalen voor een social engineer om informatie te verzamelen.

De volgende lijst dekt niet alle kanalen die een social engineer probeert te gebruiken, maar het geeft wel de belangrijkste aan.

E-mail
E-mail is het meest voorkomende kanaal om een malware aanval te lanceren. Reardon (2009) geeft aan dat ongeveer 1,9 miljard mensen in 2013 e-mails gebruiken als hun primaire communicatievorm. De meest voorkomende vormen van aanvallen in e-mails zijn ‘phishing’ en ‘reverse social engineering’ (Krombholz et al., 2015).

Sociale Netwerken
Sociale netwerken worden steeds populairder. Zo meldde Facebook in 2011 dat het aantal gebruikers 500 miljoen bedroeg, dat is ongeveer 8,5% van de totale bevolking van de wereld (Ivaturi and Janczewski, 2011). Sociale engineers gebruiken dit kanaal meestal en creëren nep identiteiten om hun eigen identiteit te verbergen en om gevoelige persoonlijke en werk gerelateerde informatie te verzamelen. De meest voorkomende aanvallen zijn ‘phishing’ en ‘reverse social engineering’ (Boshmaf et al., 2011).

Zoekmachines
Tegenwoordig zoeken wij verschillende soorten informatie in zoekmachines zoals Google, Yahoo en enz.. Sociale engineers bouwen meestal nepwebsites die ze vullen met malware en blootstellen aan internet voor hun mogelijke slachtoffers (Townsend, 2010). De algemene aanvallen in dit kanaal zijn ‘phishing’, ‘waterholing’ en ‘advance persistent threats’.

Cloud en Websites
In deze kanalen worden door de social engineer bestanden of software geüpload, die malware of computervirussen bevatten. Deze kanalen worden ook gewoonlijk samen met ‘phishing’ via e-mail gebruikt.

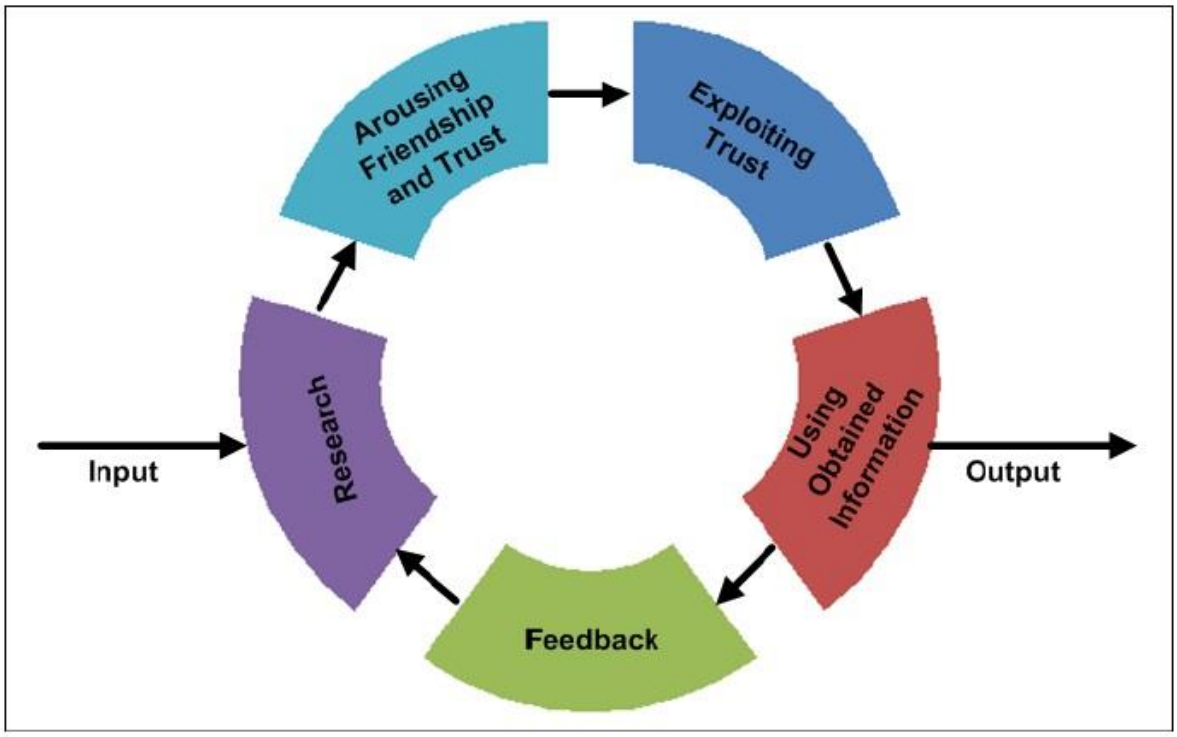
Popups
Popups is online reclame die gewoonlijk in een webbrowser verschijnt. Social engineers gebruiken dit kanaal om hun slachtoffers te bedreigen of te groeten en ze te bewegen om de beoogde actie uit te voeren. De algemene aanvallen zijn ‘phishing’, ‘waterholing’ en voortdurende bedreigingen (Ivaturi en Janczewski, 2011).

Instant messaging
Het aantal applicaties voor instant messaging neemt toe. Sociale engineers gebruiken deze kanalen voor phishing en reverse social engineering aanvallen (Krombholz et al., 2015).

3.4 Hoe ziet het proces van een Social Engineer aanval eruit (T3)?

Een social engineerings aanval verloopt in fases (Mataracioglu en Ozkan, 2013). De eerste fase is het onderzoeksproces. In dit stadium vergaart de social engineer zoveel mogelijk informatie over de persoon of organisatie die hij of zij wil aanvallen. In de tweede fase kweekt de sociaal engineer een vriendschappelijke en/of vertrouwelijke band met de betreffende persoon. De vriendschap of het vertrouwen wordt misbruikt om vertrouwelijke informatie te verkrijgen.

Deze informatie wordt geëvalueerd en indien deze bevredigend is wordt de aanval gestopt. Indien de informatie niet toereikend is begint de social engineer bij het onderzoeksproces en volgt de cylus tot de verkregen informatie toereikend is zie figuur 6.



Figuur 6 – Social Engineering Cycle (Mataracioglu, Ozkan & Hackney, 2013)

Social engineer heeft dus als doel om onder valse voorwendsels geheime of vertrouwelijke informatie te verkrijgen om deze voor eigen gewin te misbruiken (De Boer, 2011). Het feit dat social engineers het lukt om aan deze informatie te komen komt, zoals al hier boven vermeld, door de mens, de zwakste schakel. In beginsel wil de mens namelijk aardig gevonden worden, en heeft hij ontzag voor autoriteit (De Boer, 2011).

Bovendien is hij gevoelig voor complimenten en weet niet altijd welke informatie vertrouwelijk is. Hij kent vaak de procedures niet, en weet niet waarom bepaalde procedures er soms zijn (De Boer, 2011). De social engineer maakt handig gebruik van deze gebreken en gebruikt een of meer van de zes onderstaande benoemde basis methodes om mensen te overtuigen en te beïnvloeden (Cialdini, 2009):

Mensen die deze technische controles proberen te omzeilen, gebruiken methoden om zich anders voor te stellen in combinatie met emoties van hun slachtoffer om zo uiteindelijk toegang te krijgen tot informatie. Cialdini beschrijft dat er zes basis methodes zijn om mensen te overtuigen en te beïnvloeden (Cialdini, 2009):

1. Wederkerigheid: mensen zijn geneigd een wederdienst te verlenen wanneer je ze een dienst bewijst door bijvoorbeeld giften of informatie verschaffing.

2. Inzet en consistentie: indien men heeft toegezegd tot hulp of dienst zijn mensen geneigd door te gaan totdat de hulp of dienst is gehonoreerd, zelfs als de oorspronkelijke reden of motivering hiervoor niet meer aanwezig is.

3. Sociale bewijskracht: mensen zijn geneigd te geloven of iets correct is of iemand betrouwbaar is als andere mensen (kennissen / collega's / vrienden) dat vinden.

4. Autoriteit: mensen zijn geneigd gezag dragende personen te gehoorzamen ook al gaat het om hulp of diensten die laakbaar zijn.

5. Sympathie: mensen zijn makkelijk te overtuigen door mensen die voor hen sympathiek over komen.

6. Schaarste: het schaarste principe is een manier om mensen te overtuigen een dienst of hulp te bieden. Een veel voorkomende schaarste dat gecreëerd wordt is tijdsdruk. Mensen zijn geneigd snel hulp of diensten te bieden zonder het beleid of regels van hun werkgever te volgen, omdat er haast geboden is.

3.5 Welke factoren zijn van invloed op het succes van Social Engineering aanvallen (T4)?

Social engineering vanuit het operator perspectief is verdeeld in twee secties, namelijk; Mens en software (Krombholz et al., 2015). Aanvallen via software zijn zeer gecompliceerd en geautomatiseerd door software. Dit type aanvallen heeft meestal een hoger succespercentage en de identiteit van aanvaller blijft meestal anoniem.

In een organisatie is het verhogen van het beveiligingsniveau van hardware, software en firmware relatief makkelijk, maar de 'wetware' - de mens die verbonden is met een computer - is het moeilijkst. Daarom probeert een vakkundige social engineer vaak de zwakste koppeling in een systeem te exploiteren. (Holz and Bos, 2011).

De zwakke punten door de slechte training van het systeem of de werknemers (dit kan betrekking hebben op slechte opleiding van werknemers voor het slechte beleidskennis van bestaande systemen of werknemers) maakt een organisatie een gemakkelijk doelwit. Hasle et al. (2005) hebben een experiment uitgevoerd om de weerstandsgraad van een bedrijf tegen SE te tonen en ze hebben geconstateerd dat SE een goedkope en makkelijke methode is om succesvol toegang te krijgen tot kritieke informatie.

Een buitenstaander die interesse heeft in het verkrijgen van informatie voert meestal SE aanvallen uit en gebruikt een aantal psychologische trucs (persoonlijk of via computer) om de benodigde informatie te krijgen. Sociale ingenieurs *azen* op zwakke kwaliteiten van de mens, zoals:

1. De angst om in problemen te komen: tegenwoordig zetten de aanvallers (social engineer) mensen onder druk om bepaalde handelingen te verrichten met als doel het verkrijgen van bepaalde informatie.

2. Behulpzaamheid: social engineer doet zich voor als klant op basis van het principe 'klant de koning' worden medewerkers getraind om klanten te helpen met hun klantbehoefte. Dit kan soms leiden tot het vrijgeven van meer informatie aan klanten (social engineer) dan nodig is.

3. De neiging om mensen te vertrouwen: het zit in de menselijke natuur om mensen te vertrouwen tot het tegendeel bewezen is en hier maakt de social engineer gebruik van.

4. Nalatigheid: dit treed op als we onze wachtwoorden op het bureau achterlaten of materialen achterlaten welke vertrouwelijke informatie bevatten, hierdoor kan de social engineer eenvoudig aan vertrouwelijk informatie komen.

3.6 Welke factoren spelen een rol bij gedragsverandering (T5)?

3.6.1 Basisopvattingen/principes van gedrag

Er zijn meerdere opvattingen over de werking van gedrag. Volgens Fishbein & Ajzen (1977) is *intentie* van een individu een van de belangrijkste voorspeller of een individu ook echt overgaat tot het uitvoeren van een bepaald gedrag. Ajzen (1985) heeft voor specifieke domeinen onderzocht dat als iemand van plan is iets te doen (intentie) dan is de kans tussen de 75% en 96% dat iemand ook echt overgaat tot handelen.

Aan hetgeen wat iemand van plan is te doen, liggen verschillende overtuigingen ten grondslag. Hoe sterk die overtuigingen zijn, is de basis voor gedrag:

- **Normatieve overtuiging (Stimulus-Respons);** Deze opvatting gaat ervan uit dat gedrag (respons) optreedt als gevolg van een prikkel (stimulus) die voortvloeit uit een bepaalde context c.q. situatie. Oftewel het is de normatieve overtuiging, afgeleid van de situatie waarin een individu zich bevindt, over welk gedrag goed of fout is en daarnaar handelt. John Watson wordt gezien als de grondlegger van deze opvatting. In zijn manifest legde Watson (1913) de nadruk op het uiterlijk, observeer baar gedrag en reacties van mensen op gegeven situaties, in plaats van op de innerlijke, mentale staat waarin die mensen verkeren.

  Onderzoekers volgens deze opvatting gingen op basis van experimenteel onderzoek op zoek naar hoe observeerbare situaties waarin een individu zich bevindt en het gedrag wat een individu vertoon aan elkaar zijn gerelateerd.

- **Persoonlijke overtuiging (Stimulus-Organism-Respons);** Deze opvatting gaat ervan uit dat een organisme op een aantal verschillende manieren op een prikkel (stimulus) reageert (respons). Ieder persoon ervaart een situatie op een ander manier. Het verschil tussen wat iemand ervaart en de behoeftes die hij heeft, leidt tot een zekere motivatie om een bepaald gedrag te gaan vertonen. Clark Hull ging als een van de eerste aan de slag met deze opvatting en zette de werking van deze opvatting om in mathematische formules.

  Hull (1943) beschrijft de werking van de opvatting, waarmee hij aan de slag ging, als volgt: organismen lijden aan beroving (stimulus), beroving leidt tot behoefte, behoefte creëert motieven, motieven beweegt een reactie, de reactie is doel georiënteerd (respons). Het bereiken van het doel heeft overlevingswaarde.

Niet in alle gevallen leidt hetgeen wat iemand van plan is te doen (intentie) tot werkelijke gedrag. Sheeran (2002) vond zelfs gevallen, waarin gemiddeld maar 28% van het gemeten gedrag kon worden verklaard aan de hand van iemands intentie. Met andere woorden, 72 van de 100 gedragingen van een persoon had andere (onbekende) aanleidingen. Sutton (1998) geeft aan dat een deel van de discrepantie aan meetfouten is te wijten zoals bv. het tijdsverschil waarin je meet: intenties kunnen in de tijd veranderen, of vanwege een zekere mate van onbewust gedrag. Haal je dit soort meetfouten eruit dan blijkt volgens de Vries *et al.* (1988) of iemand overgaat tot gedrag af te hangen van een derde factor: het vermogen en de overtuiging om adequaat en efficiënt te handelen;

- **Zelf-doeltreffendheid (Stimulus-Respons-Consequences);** Deze opvatting gaat ervan uit dat als men ziet dat er met het eigen gedrag succes wordt geboekt, zal men overtuigd zijn de volgende keer weer in staat te zijn dit succes te behalen en dus het gedrag vaker laten zien. Thorndike (1927) ging met zijn ‘Law of effect’ ervan uit dat een individu verschillende gedragingen vertoont en als een gedrag een positief effect veroorzaakt, het gedrag vaker zal vertonen en in het geval van een negatief effect minder vaak c.q. sancties of beloningen.

3.7 Gedragstheorieën

3.7.1 Normatieve theorie

Straathof en van Dijk (2003) onderscheidt drie niveau's van waaruit prikkels ontstaan waarop een individu reageert zie figuur 7. Cialdini et al. (1991) beschrijft hoe dit gaat: een individu leidt op basis van prikkels een set van normen en regels af die bepalen welk gedrag goed of fout is;

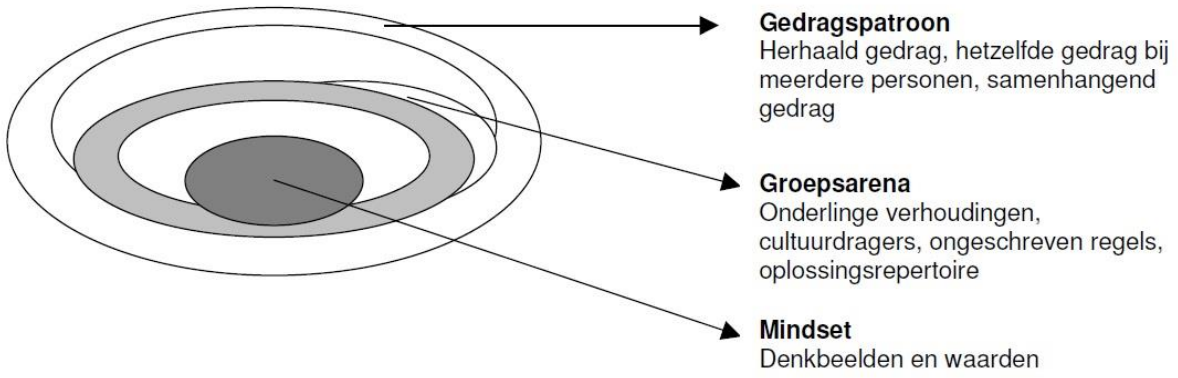
- het '**gedragspatroon**' van de groep beschrijft de norm (beschrijvende norm), bv. je kijkt naar een concert en als de muziekspeler stopt met spelen, staat iedereen op en klapt. Je zal dan ook opstaan en beginnen te klappen. Hier wordt de norm afgeleid, op basis van het herkennen van hetzelfde gedrag bij meerdere personen, een samenhangend gedrag. Onderzoekers beperken zich hier daarom ook tot het bestuderen van de acties;

- in de '**groepsarena'** hangt een bepaald atmosfeer die de norm bepaalt, bv. je stapt in een bibliotheek en je begint automatisch te fluisteren met een medewerker en legt uit naar wat je zoekt. De atmosfeer maakt dat je denkt wat voor een gedrag de omgeving wel/niet waardeert. Het gaat hier niet om wat andere doen of niet doen, maar wat jij denkt dat anderen denken.

  Daarbij gaat het er niet om of die anderen dat ook daadwerkelijk denken. In de 'groepsarena' wordt op basis van de onderlinge verhoudingen een ongeschreven regel tot norm verheven binnen de groep, wat zich vervolgens uit in samenhangend gedrag aan de buitenkant. Groepsnorm is een ongeschreven regel, waaraan de groepsleden zich dienen te houden.

- de **'mindset'** van een medewerker bepaalt hoe iemand zijn eigen gedrag wel/niet waardeert, de persoonlijke norm. Wat voor een norm een individu hanteert om zijn handelen te waarderen heeft te maken met de innerlijke gedachten van een persoon, zijn of haar persoonlijkheid. Wetenschappelijke literatuur hierover beoogt op een analytische wijze de onbegrepen denkwijzes van mensen te begrijpen. Zo identificeert bv. Caluwe & Vermaak (2000) vijf verschillende denkwijzes. Hiermee wordt een verklaring gegeven, tot wat voor een gedrag een bepaalde gedachtegang leidt onder dezelfde omstandigheden. Of andersom geredeneerd, de een zal eerder tot gedragsverandering overgaan als je bv. van tevoren een duidelijk resultaat en doel formuleert en een stappenplan maakt (blauwdruk), terwijl een ander pas iets doet als je hem ook iets teruggeeft voor wat hij jou geeft (rooddruk).

  Een ander veelgebruikte test is the 'Big Five" assessment van Goldberg (1990), ook wel OCEAN genoemd: Openness, Conscientiousness, Extraversion, Agreeableness, Neuroticism. McBride (2012) concludeert dat extroverte individuen niet gemotiveerd worden zich aan cybersecurity regels te houden bij sancties, terwijl dezelfde sancties wel werkt bij iemand die dienstbaar is ingesteld om anderen te helpen.



Figuur 7 Straathof en van Dijk (2003) onderscheidt de culturele context in drie niveau

Meerdere wetenschappers geven aan dat de atmosfeer waarin mensen zich begeven, in hoe mensen denken welk gedrag wel/niet wordt gewaardeerd, vaak bepalend is wat voor gedrag ze vertonen. Ook al is dit gedrag tegenstrijdig met de persoonlijke normen en waarden (Straathof en van Dijk 2003; Cialdini et al. 1991; Ghoshal et al. 1997). Ghoshal et al. (1997) formuleert de groepsarena ook wel met het begrip '*the smell of the place*'.

Hij beweert dat het probleem vaak niet het hebben van de juiste mindset is bij een individu: gewenste denkbeelden als ondernemerschap, creativiteit, initiatief en motivatie is er allemaal in organisaties, maar dat alles wordt vaak gedood door de atmosfeer in de organisatie. Als voorbeeld haalt hij aan dat de reden waarom organisaties niet over kunnen naar individueel ondernemerschap komt doordat we gevangen zitten in de na de oorlog succesvolle kenmerken als meegaandheid, gehoorzaamheid, controle, voorschriften en contracten.

3.7.2 Motivatie theorie

Thierry (1998) omschrijft motivatie "als een proces dat zowel datgene betreft waarop een individu zich oriënteert (behoefte) als het specifiek handelen om het doel te bereiken."[5] Vroom (1964) onderkent twee soorten 'motieven': een individu raakt gemotiveerd om een bepaald behoefte te bevredigen waar een tekort aan ontstaat ('need' theorie) en een individu vindt bepaalde doelen of opbrengsten aantrekkelijk en zet zich in om deze te bereiken ('goal' theorie).

3.7.3 'Need'-theorieën

Een van de meest bekende 'need-theorie' is die van Abraham Maslow. Maslow (1943) schrijft de motivatie van een mens toe aan een hiërarchische ordening van universele behoeftes van de mens. Volgens zijn theorie zou de mens pas streven naar het voldoen aan een hoger in de hiërarchie geplaatste behoefte, nadat de lager geplaatste behoeften bevredigd zijn. Deze behoeftes zijn; (1) lichamelijke behoefte, (2) veiligheid en zekerheid, (3) behoefte aan sociaal contact, (4) erkenning en waardering en (5) zelfrealisatie.

Informatie beveiligen kunnen we volgens de theorie van Maslow relateren aan de behoefte aan veiligheid en zekerheid. Een individu gaat over tot het treffen van beveiligingsmaatregelen om zijn behoefte aan veiligheid en zekerheid te bevredigen. Rogers (1975) legt met zijn Protection Motivation Theorie (PMT) uit hoe een individu dit doet. Volgens deze theorie beschermt een individu zich door het gevaar onder controle te krijgen en gaat daarbij als volgt te werk;

- **Risico-perceptie**: een individu schat de ernst van de situatie in door enerzijds een inschatting te maken van de kans van optreden van een gevaar en anderzijds een inschatting van de gevolgschade. Dit is een inschatting van de eigen kwetsbaarheid ten opzichte van het gevaar dat getoond wordt. Meer toegespitst op informatiebeveiliging, dan zien we dat vooral de manier waarop individuen beveiligingsrisico's waarderen, bepalend is voor het gedrag wat ze vertonen (Vance et al., 2014; Ogbanufe & Kim, 2005);

- **Attitude**; een individu schat in hoe om te gaan met het gevaar door enerzijds een inschatting te maken van de effectiviteit van het aanbevolen gedrag (maatregel) en anderzijds de mate waarin een individu denkt het aanbevolen gedrag uit te kunnen voeren met zo min mogelijk fouten.

[5] Koers & Nuijten (2006)

3.7.4 ‘Goal’-theorieën

Een van de ‘goal-theorie’ is de benadering zoals ontwikkeld door Edwin A. Locke. Locke (1968) stelt in dat specifieke doelen tot meer prestatie leiden in vergelijking tot algemene doelen. Vanuit de educatieve psychologie zijn twee soorten doelen opgemerkt; (1) een soort student die als doel heeft om nieuwe vaardigheden en kennis op te doen en (2) een soort student die als doel heeft om hoge cijfers te behalen.

Op basis hiervan onderscheidt Dweck (1986) bij een individu twee verschillende type goal-oriëntaties;

- **Learning-goals (kennis);** een individu op zoek naar hoe zijn competenties verder kan ontwikkelen, om nieuwe situaties te overmeesteren. De focus hier ligt op het leren van nieuwe vaardigheden en kennis;

- **Performance-goals;** een individu op zoek naar hoe zijn taak zo eenvoudig mogelijk zonder fouten kan uitvoeren. De focus hier ligt op het verkrijgen van gewenste feedback en negeren van negatieve feedback. Dit ligt in het verlengde van de attitude parameter, waarin een individu beoordeelt of hij een gedrag met zo min mogelijk fouten kan uitvoeren.

Onderzoekers vinden dat een individu zich beide oriëntaties als doel kan stellen; een persoon kan tegelijkertijd hoge leerdoelen en hoge taak-oriëntatie hebben, of laag in zowel leer en taak-oriëntatie, of hoog in het ene en laag in het andere type.

Deze goal-theorie in combinatie met de basisopvatting van gedrag: ‘Law of Effect’ brengt ons op het volgende: Een hoge oriëntatie op zowel het leren van nieuwe vaardigheden om nieuwe situaties te overmeesteren als een hoge oriëntatie op het succesvol uitvoeren van een taak, geeft een individu een positief gevoel dat met het eigen gedrag successen kan worden geboekt.

Dit gevoel stimuleert tot het vaker vertonen van gedrag. Andersom leidt een lage oriëntatie van een individu op zowel het aanleren van benodigde nieuwe informatie en lage oriëntatie om een taak zonder fouten uit te voeren tot een negatief gevoel dat met het eigen gedrag successen kan worden geboekt.

3.8 Gedragsmodellen

Op basis van bovengenoemde basisprincipes van gedrag en bijbehorende theorieën, zijn onderstaande referentie modellen te onderscheiden;

3.8.1 Bestaande gedragsmodellen

In het Model van gepland gedrag geeft Azjen (1991) aan dat intentie de grootste voorspeller is van gedrag en intentie op haar beurt weer wordt bepaald door (1) de attitude ten aanzien van het voorgeschreven gedrag, (2) de subjectieve norm met betrekking tot het gedrag en (3) de waargenomen controle over het gedrag.

Over het algemeen geldt hoe sterker de intentie om een bepaald gedrag te vertonen hoe waarschijnlijker het beoogd gedrag zal worden vertoond. Men voelt een sterke intentie indien een individu op drie vlakken overtuigd is; heeft een positieve houding ten opzichte van de effectiviteit van voorgeschreven gedrag, het voldoet aan de groepsnorm en de individu is zelf in staat maatregel succesvol uit te voeren.

In het *Triade* model geeft Bogaerts & Poiesz (2007) nader inzicht onder welke omstandigheden uiteindelijk een individu wel of niet overgaat van intentie tot het daadwerkelijk gedrag. Volgens het model vindt een bepaald gedrag plaats indien er sprake is van motivatie, capaciteit en gelegenheid. Met andere woorden respectievelijk, een individu wil het gedrag vertonen, moet zelf in staat zijn om het gedrag te vertonen en moet door de omstandigheden in de gelegenheid gesteld worden het gedrag te vertonen.

Norm Activation model: is een nadere uitwerking van de werking van de ‘mindset’/ persoonlijke norm van een individu. Het basisprincipe van het Norm Activation Model van Schwartz (1977) richt zich op het feit dat gedrag voortkomt uit een persoonlijke norm (mindset), die gevoelens van morele verplichtingen oproepen: Men voelt een sterke mate van morele verplichting indien het probleem wordt onderkend (probleembesef) en wordt onderkend dat men zelf bijdraagt aan het probleem (besef van verantwoordelijkheid).

Het volgen van de gevoelens van morele verplichting leidt tot morele baten zoals trots en verhoogde eigenwaarde. Het niet volgen van de morele gevoelens leidt tot morele kosten zoals schuldgevoelens en verlies van eigenwaarde.

3.8.2 Referentie-model

Het referentiemodel dient toepasbaar te zijn voor informatiebeveiliging. Met andere woorden met het model zou de mate waarin medewerkers zich aan informatiebeveiligingsmaatregelen (veilig of onveilig gedrag) houdt moeten kunnen worden voorspeld en vervolgens beïnvloed. Het is daarbij van belang die factoren te onderzoeken, waarop invloed kan worden uitgeoefend en die meetbaar zijn.

Het model van Fishbein & Ajzen(1977) is toepasbaar voor informatiebeveiliging. Dit model gaat ervan uit dat de intentie van medewerkers, en daarmee gedrag, is te beïnvloeden. Attitude en subjectieve norm. Ook Koers & Nuijten (2006) hebben dit model als basis gebruikt om organisaties te auditen op informatiebeveiliging. Het model van Schwartz (1977) vult het normen kader van waaruit een individu opereert aan door ook naar de persoonlijke norm te kijken.

Dit model beperkt zich echter alleen tot de persoonlijke norm met de morele verplichting een ander te helpen. Wij hanteren vanuit de theorie een breed palet aan normen gekoppeld aan persoonlijkheid van een individu, waarbij ‘dienstbaar’ zijn (de ander willen helpen) er een van is. Een nog gemiste onderdeel waar in de modellen niet naar wordt gekeken, is het gedragspatroon uit het gedragstheorie van Straathof en van Dijk (2003). Het gaat hierbij om de mate waarin een medewerker anderen volgt

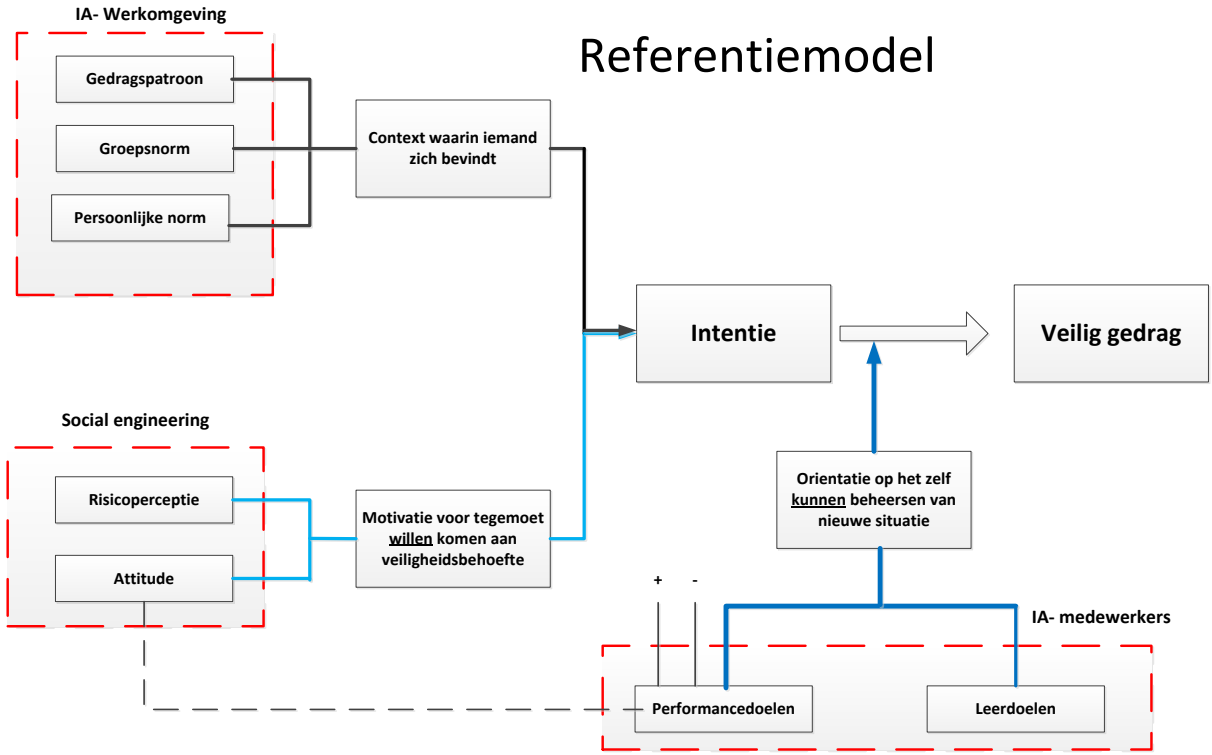
in een bepaald gedrag. Dit is te meten en achteraf ook te beïnvloeden, door bijvoorbeeld het aanmoedigen van voorbeeldgedrag.

De motivatietheorie biedt meer aanknopingspunten: de risicoperceptie & de motivatie om bepaalde doelen te bereiken. Op dat laatste gaat het model van Bogaerts & Poiesz (2007) weliswaar wel in, maar zijn zodanig geformuleerd dat de te meten factoren niet zijn te beïnvloeden: capaciteit; de medewerker is wel of niet in staat om een gedrag te vertonen en gelegenheid: de medewerker vindt zich wel of niet in de gelegenheid gesteld om een gedrag te vertonen.

Daarentegen biedt de motivatietheorie van Dweck (1986) wel aanknopingspunten. Hij definieert het vermogen van een individu om van intentie over te gaan naar beoogd gedrag, als de mate waarin een individu het aantrekkelijk vindt om leerdoelen te bereiken en de taak succesvol uit te voeren. Het bereiken van de leerdoelen haakt aan op het verhogen van kennis waarop vele awareness programma's vanuit het vakgebied van informatiebeveiliging de afgelopen jaren is ingezet. Dit zijn wel te beïnvloeden factoren.

Ook Rogers (1975) biedt vanuit de motivatietheorie een aanvullend aanknopingspunt. Hij beweert dat een individu gemotiveerd raakt wanneer hij de ernst van het tekort (in ons geval het gevaar) aan behoefte hoog inschat en laag gemotiveerd wanneer dit niet het geval is. Dit heeft te maken met hoe een individu de kans van optreden en gevolgschade van een gevaar beleeft: risicoperceptie.

Het referentiemodel in figuur 8 heeft de onderzoeker vervolgens toegepast tijdens zijn empirische onderzoek.



Figuur 8 Referentiemodel

4. Resultaten van het Empirische onderzoek

In dit hoofdstuk worden de resultaten van het empirische onderzoek gepresenteerd. De resultaten worden per empirische deelvraag beschreven.

4.1 Wat wordt onder industriële automatisering (IA) verstaan? (E1)

In dit hoofdstuk worden de resultaten van het empirische onderzoek beschreven. De sub paragrafen geven elk antwoordt op een empirische deelvraag.

4.1.1 Definitie IA

Om beter te begrijpen wat binnen RWS onder IA wordt verstaan wordt nu de definitie van IA nader verkend. Binnen RWS worden de volgende verschillende definities gehanteerd:
“Industriële Automatisering is de Informatievoorziening die functioneel verbonden is met infra”.
De term ‘infra’ staat voor de fysieke netwerkinfrastructuur (areaal). Met ‘functioneel verbonden’ wordt bedoeld dat de industriële automatisering niet per sé fysiek op het beton en staal gemonteerd hoeft te zijn. Tot de industriële automatisering behoort ook de centrale waar vandaan bewaakt en bediend wordt.

Daarnaast is er ook een meer uitgebreide definitie van industriële automatisering namelijk:
“Industriële Automatisering omvat de ICT gerelateerde systemen en onderdelen (hardware en software, zowel functioneel als technisch), waarbij functioneel interactie plaats vindt met de fysieke omgeving of gebruikers (bijvoorbeeld een brug, onderstation, DRIP, etc.). Dit omvat het verkrijgen van informatie over de fysieke omgeving (inwinnen) en het beïnvloeden van de fysieke omgeving (bedienen en besturen).”
Bron: Inleiding EAR Architectuur Industriële automatisering RWS 0.1 / 7 juli 2011

Naast bovenstaande definities wordt de volgende definitie genoemd in CSIR.
Industriële Automatisering omvat de ICS/SCADA systemen en de ICT gerelateerde systemen en onderdelen (hardware en software), waarbij functioneel interactie plaats vindt met de fysieke omgeving of gebruikers (bijvoorbeeld een brug, onderstation, DRIP, etc.). Dit omvat mede het verkrijgen van informatie over de fysieke omgeving (inwinnen) en het beïnvloeden van de fysieke omgeving (bedienen en besturen).
Bron: Cybersecurity Implementatierichtlijn Objecten RWS (CSIR) 1.01 / 02 december 2013

Het besturingsdeel zorg voor de aansturing van de installaties. De besturing wordt via het bedieningssysteem gedaan. Deze bediening kan zowel lokaal als centraal plaats vinden. Het bedieningsdeel van IA is het deel waarmee bijvoorbeeld de weg of tunnel door een verkeersleider/operator wordt bewaakt en zondig wordt bediend.

4.1.2 Rol IA binnen RWS

In het onderstaande tabel 6 is beschreven welke rol IA binnen RWS speelt.

Industriële automatisering binnen Rijkswaterstaat…	
…zorgt voor:	inwinning van informatie over de actuele toestand van de fysieke omgeving (bijv. lus), en/of wijziging toestand fysieke omgeving (bijv. brugdek, sluisdeur), en/of presentatie informatie naar fysieke omgeving (bijv. matrixbord, sein)
…functioneert:	doormiddel van sturing van de mens (bediening), en/of autonoom via regelsystemen/automaten
…bestaat uit:	sensoren en actuatoren verbonden met de civiele infrastructuur en/of besturing en regelsystemen installaties (bijv. motorregeling)

	en/of vaste en mobiele communicatienetwerken (data, video, audio) en/of bedieningssystemen (bijv. uniforme operator MMI, ICT in centrale)

Tabel 6: Rol IA binnen RWS
Bron: Inleiding EAR Architectuur Industriële automatisering RWS 0.1 / 7 juli 2011

We kunnen de IA zien als de ICT onder de motorkap van een auto. Hierbij is de auto zelf de fysieke infrastructuur van RWS en de automobilist de operator, die de auto bestuurt. Onder de motorkap bevinden zich verschillende onderdelen en die worden aangestuurd en bediend vanaf het dashboard door de automobilist. Verder zijn er ook systemen in de auto aanwezig die zonder tussenkomst van de automobilist functioneren. De ICT onder de motorkap dient veilig, betrouwbaar en beschikbaar te zijn.

4.1.3 Beveiliging IA

In de vorige paragraaf is duidelijk geworden dat veiligheid een belangrijke aspect is binnen de IA van RWS. Om te zorgen dat de systemen veilig met elkaar functioneren is het van belang dat er ook voldoende aandacht wordt besteed aan de beveiliging van IA systemen.
Beveiliging in de SCADA/ICS omgeving is hedendaags een veel besproken onderwerp. In het verleden waren deze systemen strikt gescheiden. De verbinding met gemeenschappelijke computernetwerken heeft nieuwe kansen voor hackers geopend. Omdat RWS veel systemen (ICS/SCADA) en IA omgevingen (objecten) heeft die los staan van de centrale kantooromgeving kan je al veronderstellen dat de dreigings- profiel van deze systemen een andere niveau heeft dan de IV in de kantooromgeving. Bron: Cybersecurity Implementatierichtlijn Objecten RWS (CSIR) 1.01 / 02 december 2013

4.1.4 Objecten

Binnen RWS zijn verschillende objecten die raakvlakken hebben met IA: tunnels, bruggen, sluizen, stuwen, gemalen, waterkeringen, centrales, meetnetten, rijbanen en spitsstroken. Deze objecten worden ook door RWS zelf of de gecontracteerde opdrachtnemers beheerd. De genoemde objecten vallen uiteen in de volgende netwerken die RWS beheert: het hoofdvaarwegennet (HVWN), hoofdwegennet (HWN) en hoofdwatersystemen (HWS), en delen daarvan.
In de onderstaande tabel 7 zijn de objecten met IA gecategoriseerd per netwerk.

IA-object, deelsysteem of civiele kunstwerk	Netwerk
Centrale (droog)	HWN
Centrale (nat)	HVWN, (HWS)
Testcentrum (TORO)	HVWN, (HVWN / HWS)
Brug (beweegbare.) (droog/nat)	HWN/ HVWN/ (HWS)
Tunnel (droog)	HWN, (/HVWN/HWS)
Sluis (nat)	HVWN / HWS
Stuw (nat)	HVWN/HWS
Kering (nat)	HWS (/HVWN)
Gemaal (nat)	HWS (/HVWN)
Spitsstrook (droog)	HWN
Gladheidsmeldsysteem (droog)	HWN
Weigh in Motion (droog)	HWN
Schip	HVWN/ HWS
Camera(droog/nat)	HWN/HWS (/HVWN)
Hydro/meteo sensor	HWS / (HWN /HVWN)
DRIP	HWS (/HVWN)
Informatieborden	HWN
Signaalgever	HWN
WKS	HWN
Lus	HWN

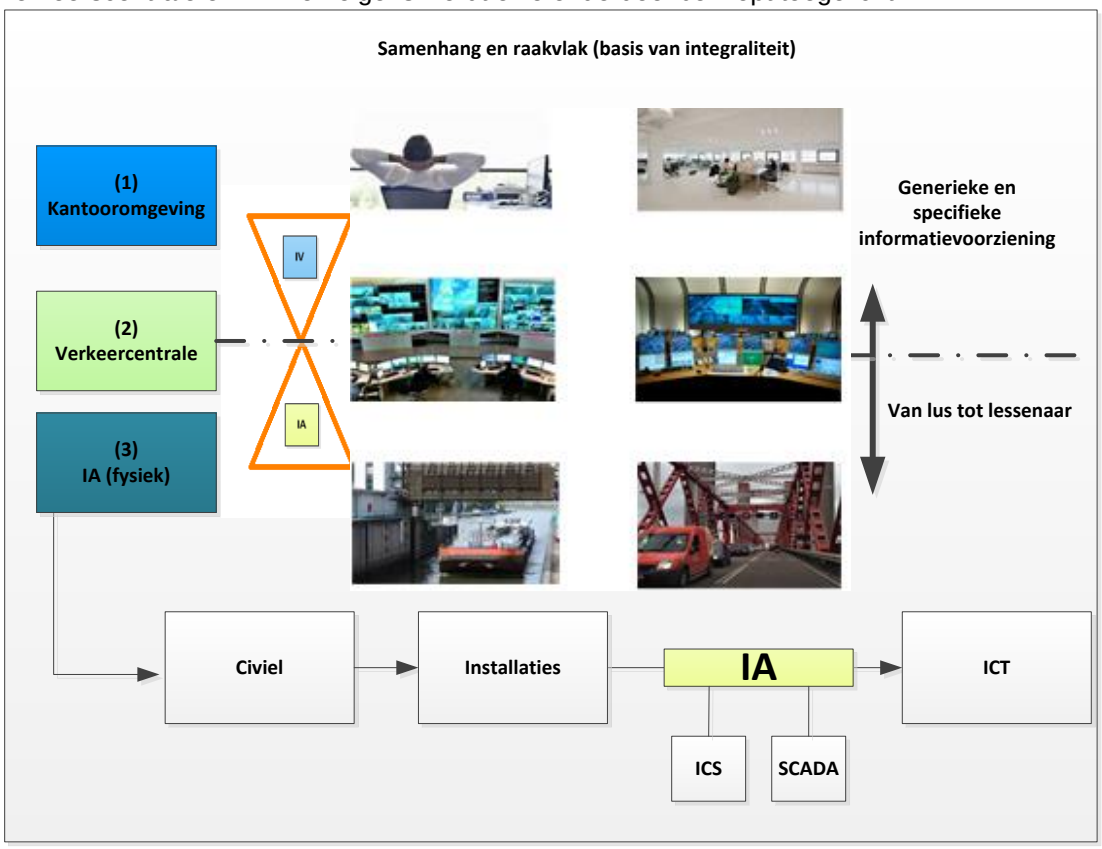
Toeritdosering	HWN
Verkeersregelinstallatie	HWN

Tabel 7: Object indeling per netwerk

RWS heeft per object een infraclassificatie toegekend op basis van het belang van het object. Dit wordt nader beschreven in paragraaf 4.2.6.

4.1.5 Samenhang en raakvlak

In het onderstaande figuur 9 worden de raakvlakken inzichtelijk gemaakt tussen de kantooromgeving, verkeerscentrale en IA. Vervolgens wordt elke onderdeel beknopt toegelicht.



Figuur 9: Samenhang en raakvlak

1. Kantoor
Binnen kantooromgeving van RWS wordt er gebruik gemaakt van de generieke en specifieke informatievoorziening zoals: Kerngis, autocad, MSoffice, Visio etc.

2. Verkeercentrale
Bepaalde objecten (bruggen, sluizen, tunnels,..) van RWS zijn verbonden met de verkeercentrales. Deze objecten kunnen ook een lokale bediening hebben vanuit bijv. een brugwachtershuisje. IA bevindt zich zowel in het object als langs de wegkant en vaarweg en in de centrale voor bewaken en bedienen op afstand. In de centrale vindt veel informatie-uitwisseling plaats en bevindt zich het raakvlak met de generieke ICT en applicaties/informatiesystemen.

3. IA
De IA loopt fysiek vanaf de objecten tot in de verkeercentrale. In de objecten langs de wegkant en de vaarweg zorgt de IA voor het uitlezen van de toestand van het object of verandert deze. In het object raakt de IA andere technologie zoals: civiel en installatietechniek elkaar.

4.2 Hoe ziet het informatiebeveiligingsbeleid van RWS eruit (E2)?

4.2.1 Baseline Informatiebeveiliging Rijksdienst

De Baseline Informatiebeveiliging Rijksdienst (BIR) schrijft het basisniveau voor informatiebeveiliging bij de Rijksoverheid voor en de volgende standaarden ISO 27001/ISO27992 zijn opgenomen in de BIR.

4.2.2 Baseline Informatiebeveiliging Rijkswaterstaat

De Baseline Informatiebeveiliging Rijkswaterstaat (BIR RWS) is een vertaalslag en invulling van de BIR voor de beveiliging van de Informatievoorziening (IV) van RWS.
De beheers doelen en beheersmaatregelen die in de BIR RWS worden beschreven zijn voor de Industriële Automatisering (IA) niet volledig dekkend en op onderdelen te algemeen van aard waardoor er bedrijfsrisico's blijven bestaan voor RWS.

4.2.3 Cybersecurity risico's RWS

In onderstaande tabel 8 worden de top 10 risico's t.a.v. van cybersecurity benoemd, die binnen RWS van toepassing zijn.

Risico's Cybersecurity	
1.	**Vertrouwelijke informatie indien behoefte kan deze opgevraagd worden bij de auteur.**
2.	
3.	
4.	
5.	
6.	
7.	
8.	
9.	
10.	

Tabel 8: Top 10 risico' s cybersecurity
Bron:

In het RWS beleid zijn maatregelen onderkent om SE tegen te gaan zie hiervoor in de bijlage 4 opgenomen risicoreductie.

4.2.4 Cybersecurity Implementatie Richtlijn Objecten RWS

Rijkswaterstaat heeft veel systemen en omgevingen die los staan van de centrale kantooromgeving. Dit zijn veelal operationele systemen voor het bedienen van objecten, het communiceren met vaarweggebruikers of het modelleren van waterkwaliteit en -kwantiteit in verschillende stroomgebieden.

Deze systemen hebben vaak een ander dreigingsprofiel dan de IV in de kantooromgeving en staan daar vaak ook los van zoals de Industriële Automatisering (IA) met veel ICS/SCADA-toepassingen. Kwaadwillenden en securiteitonderzoekers tonen interesse in de (on)veiligheid van industriële controlesystemen (ICS/SCADA-systemen). Systemen die direct vanaf het internet bereikbaar zijn liggen in het bijzonder onder vuur.
Bron: Cybersecurity Implementatierichtlijn Objecten RWS (CSIR) 1.01 / 02 december 2013

Cybersecurity wordt als volgt gedefinieerd binnen RWS:
Cybersecurity is het voorkomen van gevaar of schade veroorzaakt door verstoring, uitval of misbruik van ICT en Industriële Automatisering.
Bron: Nationaal Cyber Security Centrum (NCSC).Nationale Cybersecurity Strategie

Tegen de top tien Cybersecurity risico's heeft RWS specifieke beheersmaatregelen getroffen in de CSIR, die zijn in de tabel 9 hieronder zijn benoemd.

Specifieke maatregelenpakketten uit (CSIR)	
Maatregelen Fysieke toegangsbeveiliging IA-gerelateerde ruimten	Maatregelen Logging en Monitoring
Maatregelen Logische toegang	Maatregelen Bewustwording en Training
Maatregelen Beveiligingsincidenten en incident Response Plan	Maatregelen gecontroleerd wijzigen
Maatregelen Netwerkoppelingen	Maatregelen beheer en onderhoud
Maatregelen bescherming tegen malware, hardening en patching	Maatregelen Back-ups

Tabel 9: Specifieke maatregelen uit CSIR
Bron: Cybersecurity Implementatierichtlijn Objecten RWS (CSIR) 1.01 / 02 december 2013

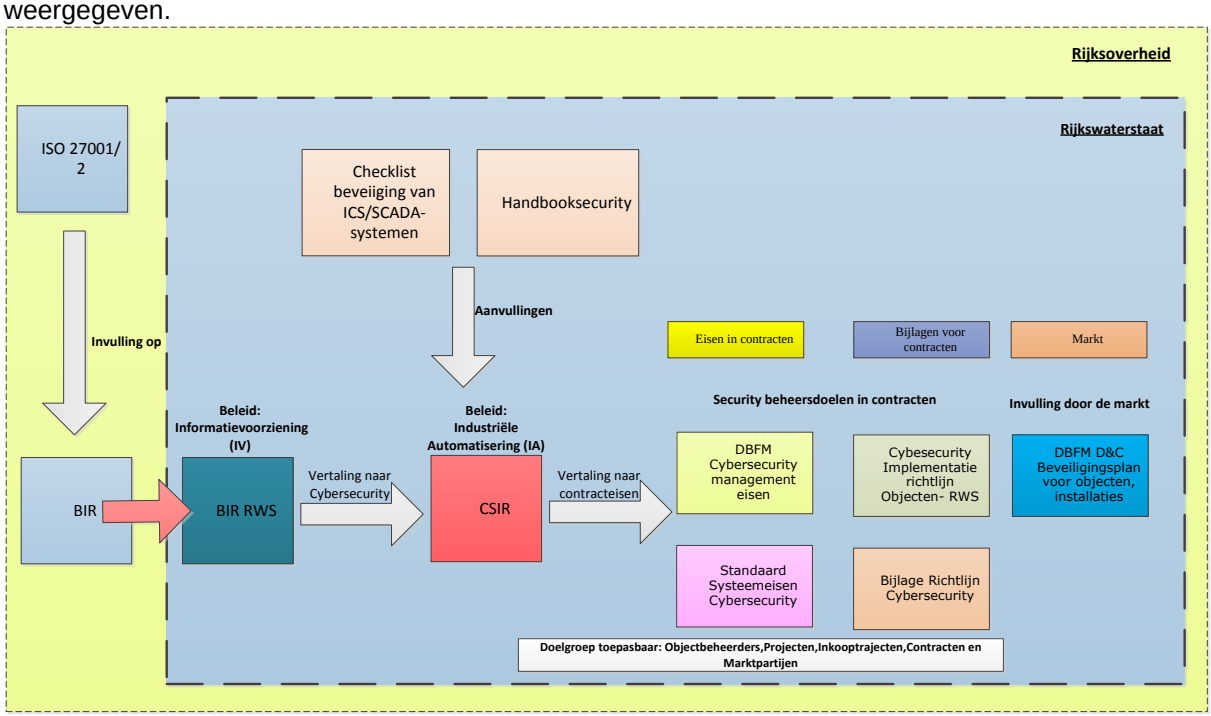
De CSIR is bedoeld voor RWS interne mensen, die in projecten werken, de objectenbeheerders en tijdens de uitvoering van de werkzaamheden, dienen de marktpartijen zich te houden aan de CSIR. Gezien de maatschappelijke taakstelling van RWS voor beheer van vitale infrastructuur is het zaak om cybersecurity te beheersen door implementatie en onderhoud van de beheersmaatregelen zoals beschreven in de CSIR.

Een van de maatregelen uit de CSIR is bestemd voor veilig gedrag voor de mens. Dat is in de maatregel bewustwording en training uit paragraaf 3.7 uit de CSIR. RWS gaat er vanuit dat de medewerkers van RWS hier naar handelen. In bijlage 5 zijn de gedragsregels opgenomen.

4.2.5 Relatie informatiebeveiligingsbeleid RWS

RWS heeft in het kader van beveiliging van de objecten het CSIR ontwikkeld. De CSIR is de vertaalslag van de specifieke beheer doelen en beheersmaatregelen uit de BIR, BIR RWS en de NCSC Checklist beveiliging ICS/SCADA systemen naar beheer doelen en beheersmaatregelen voor de beveiliging van de objecten van Rijkswaterstaat waarbinnen veel gebruik wordt gemaakt van ICS/SCADA-systemen.
Bron: Cybersecurity Implementatierichtlijn Objecten RWS (CSIR) 1.01 / 02 december 2013

De maatregelen die benoemd worden in de CSIR zijn door vertaald naar contract eisen die meegaan in contracten. In figuur 10 is de onderlinge relatie informatiebeveiligingsbeleid documenten weergegeven.



Figuur 10: Relatie informatiebeleid RWS

Tevens is in de CSIR rekening gehouden met de risico mitigatiestrategie van Rijkswaterstaat. Primair hebben in tabel 9 top 10 beheers doelen met bijbehorende beheersmaatregelen uit de CSIR het doel om verstoring, misbruik en uitval binnen de IV en IA te voorkomen.

4.2.6 Gedragsmodel voor informatiebeveiliging

De tien maatregelen die benoemd worden in de CSIR zijn gerelateerd aan de risico´s. Doordat RWS veel objecten in beheer en onderhoud heeft hebben ze per object de infraclassificatie van het object en de beveiliging ervan bepaald. Hiermee streeft RWS voor een passend niveau van beveiliging per object en proberen ze de risico´s te beheersen. Bijv. voor een object van weerstandniveau klasse 4 zie onderstaande tabel 10 cyber classificatie wordt een zwaardere maatregelen pakket geïmplementeerd dan voor een object met een weerstandsniveau 3.

Classificatie object in Infraclassificatie	**Cybersecurity weerstandsniveau**
A	4
B	3
C	2
D	1
E	1

Tabel 10: Cyber classificatie
Bron: Cybersecurity Implementatierichtlijn Objecten RWS (CSIR) 1.01 / 02 december 2013

Op basis van weerstandsniveau waar een object onderverdeeld is, wordt bepaald welke maatregelen voor dat niveau van toepassing is deze is gewoon vastgelegd in het beleid zie tabel 11. In de CSIR wordt voor de specifieke benoemde maatregelen, aandacht besteed aan de volgende aspecten: Mens, Procedure & Organisatie en Techniek.

3.3 Maatregelen Beveiligingsincidenten en incident Response Plan

Niveau	Mens	Procedures & Organisatie	Techniek
4	BIRM1	BIRPO1 t/m 8	BIRPT1
3	BIRM1	BIRPO1 t/m 8	BIRPT1
2	BIRM1	BIRPO1 t/m 3, 5, 6 en 7	BIRPT1
1	BIRM1	BIRPO1 t/m 3, 5 en 6	BIRPT1

Tabel 11: Maatregelen beveiligingsincidenten en incident response plan
Bron: Cybersecurity Implementatierichtlijn Objecten RWS (CSIR) 1.01 / 02 december 2013

4.2.7 Beleid versus Social Engineering Technieken van aanval

In het onderzoek social engineering binnen de Nederlandse Rijksoverheid (Krijn, 2016) is het referentie raamwerk voor SE ingevuld (paragraaf 3.3 Referentieraamwerk social engineering) met maatregelen uit de literatuur. In dit onderzoek is hier bewust van afgeweken door de maatregelen te gebruiken, die in het huidige informatiebeveiligingsbeleid van RWS zijn opgenomen. De maatregelen zijn door middel van empirische onderzoek verzameld.

Hieronder omschrijft de onderzoeker in tabel 12: het verschil en de onderbouwing ten op zichtte van de referentieraamwerk in het onderzoek van (Krijn, 2016).

Krijn van der laan (Krijn, 2016)	***Mijn onderzoek***	***Motivatie***
Referentie raamwerk voor SE is ingevuld uit de literatuur.	Wijk daarvan af en benoem daar maatregelen, die in de informatiebeveiligingsbeleid zijn opgenomen. Maak een onderverdeling voor de maatregelen, die gelden voor de kantooromgeving en specifieke maatregelen die van toepassing zijn op de IA omgeving.	Er is onderzocht in hoeverre de informatiebeveiligingsbeleid invulling geeft aan de verschillende technieken en vormen van SE aanval.
In paragraaf 3.3. Referentieraamwerk social engineering. Omschrijft Krijn in de tabel “Aanvallen van Social Engineering”	Wijk daar van af en benoem het Technieken van social engineering.	Het zijn geen aanvallen van social engineering, maar technieken van aanval. (dat is wel iets anders)
Krijn heeft manipulaties als techniek van social engineering aanval benoemt.	Wijk daar vanaf doordat een social engineer kan het rationele denken van een slachtoffer beïnvloeden door te spelen op de emoties van de mens.	Het zijn menselijke eigenschappen zoals: emoties, behulpzaam zijn, gemogen mogen worden.
In het referentiemodel heeft Krijn technieken van social engineering benoemd.	Wijk af van de technieken benoemd in het referentiemodel. Doordat je een aantal van die technieken kunnen onderbrengen onder een soort van technieken van	Dit lijkt allemaal hetzelfde je komt op zich de zelfde informatie tegen (doel). (zie hieronder om welke technieken het betreft)

	social engineering aanval.	

Tabel 12: Verschil referentieraamwerk

In de tabel 13: hieronder omschrijft Krijn van der Laan (Krijn, 2016) een aantal technieken van social engineering aanvallen, heb aangegeven welke invulling de onderzoeker heeft gegeven in zijn onderzoek en de onderbouwing ervan.

Onderzoek Krijn: De benoemde aanvallen van Social Engineering (Krijn, 2016)	***Mijn onderzoek: Technieken van social engineering aanval***	***Argument***
Dumpster diving	Letterlijk dumpsterdiving betekent wat anders dan office snooping. De twee benoemde technieken van SE aanval is in dit onderzoek als een soort beschouwd	Je komt op zich de zelfde informatie tegen alleen de technieken zijn anders.
Office snooping		
Spearphishing	De benoemde technieken zijn feitelijk zelfde technieken.	
Mailouts		
Impersonatie	De benoemde technieken zijn als een soort beschouwd.	Je komt op zich dezelfde informatie tegen.
Fake profiles		

Tabel 13: Technieken van SE

Er is door de onderzoeker onderzocht in hoeverre de informatiebeveiligingsbeleid BIR en CSIR invulling geeft aan de verschillen technieken van SE aanval. In de tabel 14 Beleid versus technieken van SE worden de resultaten weergegeven. Doormiddel van “x” wordt aangegeven of de maatregelen de technieken van SE aanval afdekken. In het overzicht is ook aangegeven welke maatregelen specifiek voor de IA gelden in vergelijking met de kantooromgeving.

Hiermee wordt inzichtelijk of de maatregelen voldoende bescherming bieden tegen de verschillen type aanvallen: physical, social, social technical en technical of dat er nog aanvullende maatregelen genomen moeten worden voor de IA objecten.

	Maatregelen Kantoor- en IA omgeving															Maatregelen specifiek voor IA									
Technieken van social engineering	Classificatie van informatie (BIR 7.2)	Retournering van bedrijfsmiddelen (8.3.2)	Fysiek toegang (BIR 9.1.2)	Controle van systeemgebruik (BIR RWS 10.10.2)	Registratie van gebruikers (systeem) (BIR RWS 11.2.1)	Beheer van (speciale) bevoegdheden (BIR RWS 11.2.2)	Beheer van gebruikerswachtwoorden (BIR RWS 11.2.3)	Beoordeling van toegang rechten van gebruikers (BIR RWS 11.2.4)	Gebruik van wachtwoorden (BIR RWS 11.3.1)	Onbeheerde gebruikersapparatuur (BIR RWS 11.3.2)	Clear desk en clear screen (BIR RWS 11.3.3)	Beveiligde inlogprocedures (BIR RWS 11.5.1)	Gebruikersidentificatie en authenticatie (BIR RWS 11.5.2)	Systemen voor wachtwoordenbeheer (BIR RWS 11.5.3)	Sleutel beheer (BIR 12.3.2)	Fysieke toegang IA- ruimte (CSIR 3.1)	Logische toegang(CSIR 3.2)	Beveiligingsincidenten Responseplan (CSIR 3.3)	Netwerkkoppelingen (CSIR 3.4)	Bescherming malware, hardening, patching (CSIR 3.5)	Logging en monitoring (CSIR 3.5)	Bewustwording en training (CSIR 3.7)	Gecontroleerd wijzigen (CSIR 3.8)	Beheer en onderhoud CSIR (3.9)	Back-up (CSIR 3.10)
Dumpster diving **(P)**	x	x	x							x	x	x	x		x	x	x	x			x	x	x	x	x
Shoulder surving **(P)**	x	x	x							x	x	x	x		x	x	x	x			x	x	x	x	x
Baiting **(P) (ST)**	x	x	x			x			x	x	x	x	x	x	x	x	x	x		x	x	x		x	x
Reverse social engineering **(S)**									x				x					x			x	x			
Ransomware **(ST)**	x					x			x				x	x			x	x		x	x	x			x
Waterholling **(ST)**	x					x			x				x	x			x	x		x	x	x			x
Pre-texting **(ST)**	x					x			x				x	x			x	x		x	x	x			x
Phishing **(ST)**	x					x			x				x	x			x	x			x	x			x
Advance persistent threat **(ST) (T)**	x			x	x	x	x	x	x				x	x			x	x	x	x	x	x	x		x
Spear phishing **(T)**				x	x		x	x					x	x				x	x		x	x	x		
Impersonatie **(ST)**	x					x			x				x				x	x		x	x	x			x
Identity theft **(P) (ST)**	x		x			x			x	x	x	x	x	x	x	x	x	x		x	x	x		x	x

Type of Social engineering attacks

Physical (P)
Social (S)
Social Technical (ST)
Technical (T)

Tabel 14: Beleid versus technieken van SE

4.3 Welke technieken van social engineering aanvallen komen voor bij RWS op het gebied van IA (E3)?

De informatie met betrekking tot welke technieken SE aanvallen er voordoen binnen RWS wordt niet vrijgegeven door de organisatie. Hierdoor is deze informatie niet beschikbaar voor gebruik in het onderzoek. De voornaamste reden is dat de organisatie niet in de media wil komen waardoor imagoschade optreedt.

4.3.1 Technieken social engineering aanval binnen RWS

Om toch informatie hierover te achterhalen is er een zoekopdracht via internet uitgevoerd. Hierbij zijn de technieken die in de tabel 14 van paragraaf 4.2.7 zijn opgenomen in combinatie met Rijkswaterstaat gebruikt als zoekterm gebruikt. Dit heeft geleidt tot de volgende resultaten zie figuur 11 en figuur 12:

Uit de gevonden bron blijkt dat RWS geïnfecteerd is geraakt met een ransomware besmetting.

Figuur 11: Ransomware besmetting
bron: https://www.security.nl/posting/422575/Ransomware+infecteert+computers+Rijkswaterstaat

Figuur 12: Ransomware infecteert computers RWS
Bron: Safe web https://www.safeweb.nl/anti-hacking/ransomware-infecteert-computers-rijkswaterstaat/9__322.php

In figuur 13 hieronder blijkt dat er in 2014 in het kader van de NSS top een phishing mail in omloop was.

Dit bericht is verzonden met de prioriteit Hoog.

Van: Algemene Mededeling (RWS)
Aan: _Heel RWS
CC:
Onderwerp: Waarschuwing NSS phishing mail in omloop!

Verzonden: vr 21-3-2014 20:57

Beste Collega,

Het Nationale Cyber Security Centre (NCSC) heeft gemeld dat er een phishing mail is gezien die in het kader van de Nuclear Security Summit (NSS) wordt rondgestuurd. Het doel hiervan lijkt het verzamelen van gegevens en het installeren van kwaadaardige software te zijn.

Ik verzoek je dringend om de volgende wijze van handelen aan te houden:

- Momenteel worden er e-mails verzonden uit naam van **NSS2014-notice(@)minbuza.nl**
  (let op: de afzender kan aan verandering onderhevig zijn).

- In de in omloop zijnde e-mails word je gevraagd om op een link te klikken. **DOE DIT NOOIT!**

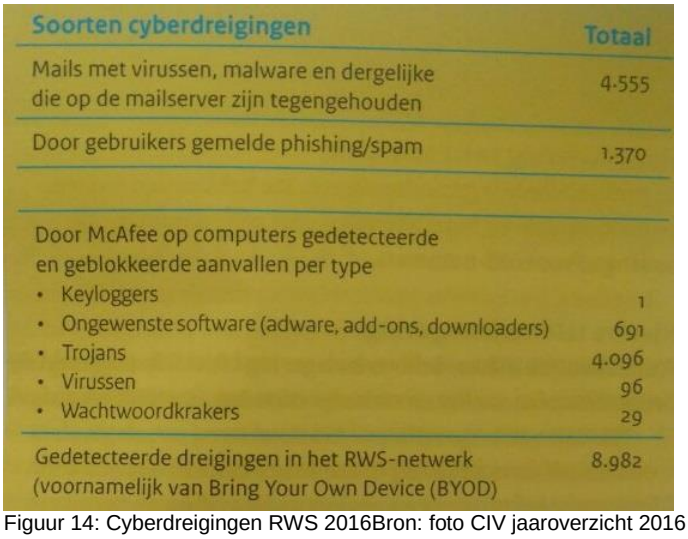
- **Gooi deze phishing mails direct weg en klik niet op de link.**

Ik dank je alvast hartelijk voor je medewerking in deze.

Met vriendelijke groet,

Figuur 13: Phishing mail

Hieronder een aantal cijfers over de cyberdreigingen die het SOC tegen komt en tegenhoudt op een rij binnen RWS zie figuur 14.

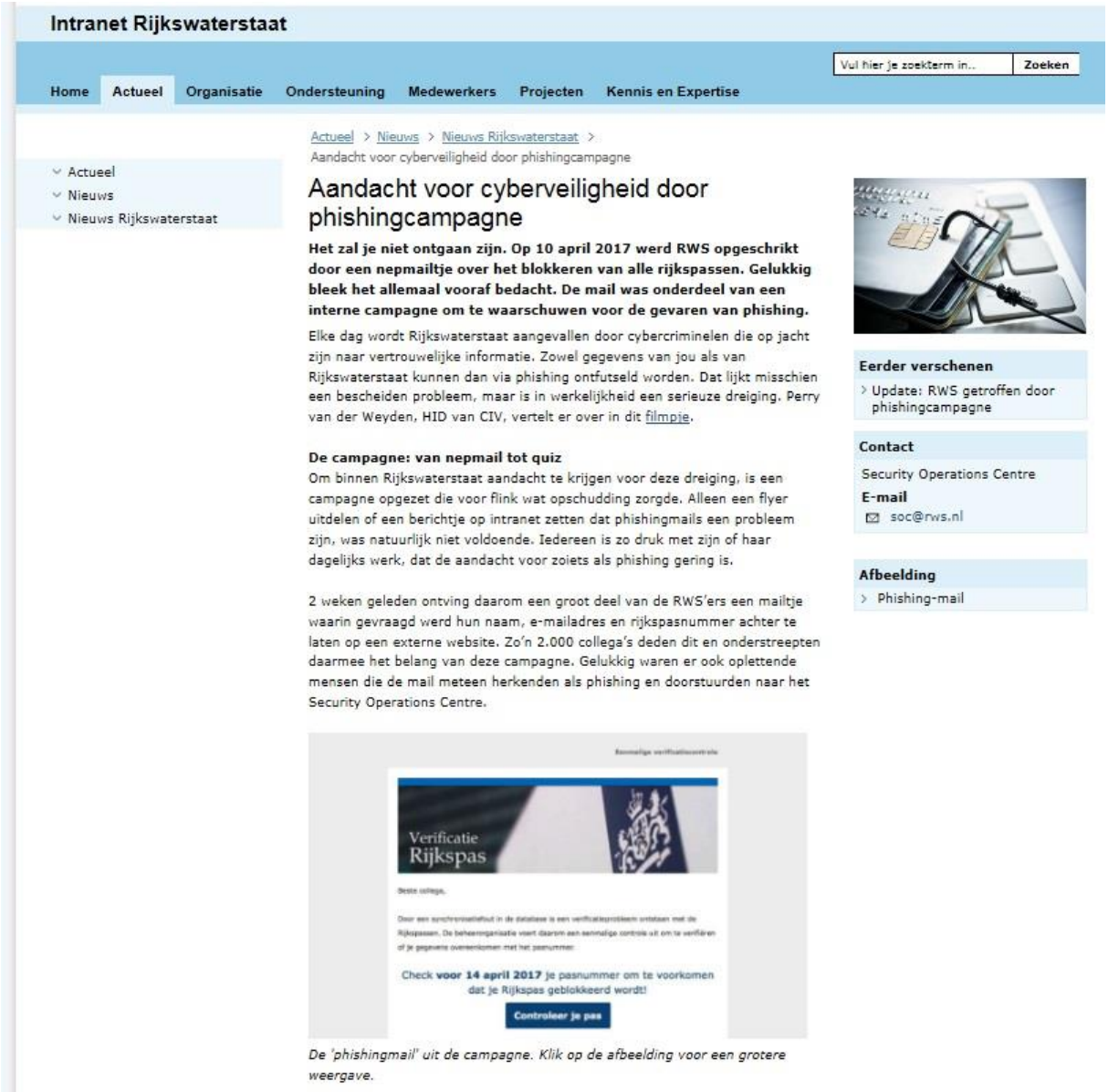


Soorten cyberdreigingen	Totaal
Mails met virussen, malware en dergelijke die op de mailserver zijn tegengehouden	4.555
Door gebruikers gemelde phishing/spam	1.370
Door McAfee op computers gedetecteerde en geblokkeerde aanvallen per type	
• Keyloggers	1
• Ongewenste software (adware, add-ons, downloaders)	691
• Trojans	4.096
• Virussen	96
• Wachtwoordkrakers	29
Gedetecteerde dreigingen in het RWS-netwerk (voornamelijk van Bring Your Own Device (BYOD)	8.982

Figuur 14: Cyberdreigingen RWS 2016Bron: foto CIV jaaroverzicht 2016

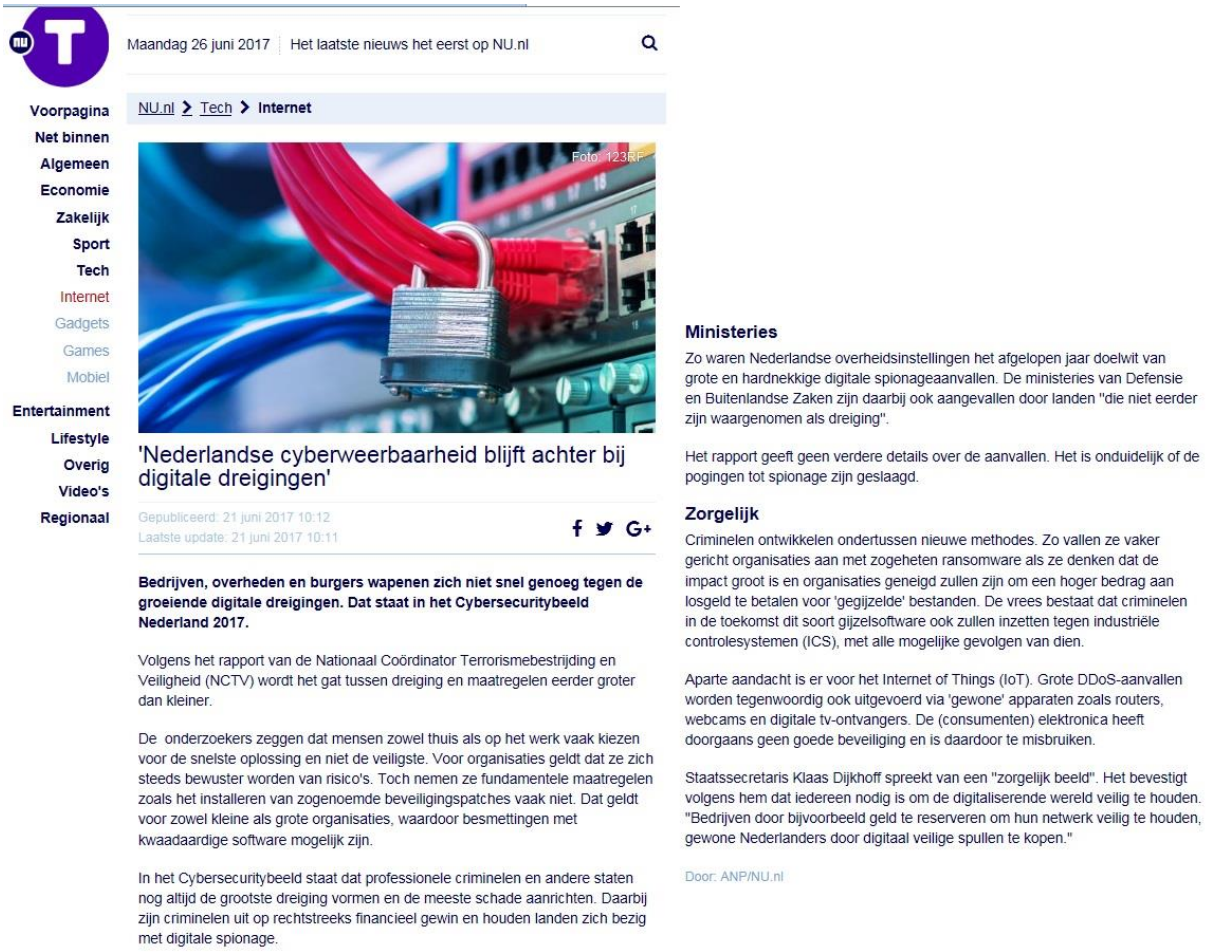
4.3.2 Testen van awareness met betrekking tot Phishing

RWS heeft in 2017 binnen de hele organisatie een test uitgevoerd met de volgende techniek van SE aanval namelijk Phishing zie figuur 15. Deze test is uitgevoerd om de awareness te meten op gebied van SE techniek phishing. Gelukkig ging het hier om de test. De test heeft uitgewezen dat 2000 mensen hun informatie hebben vrijgegeven.



Figuur 15: Phishing mail
Bron:
http://corporate.intranet.rws.nl/actueel/nieuws/nieuws_centrale_informatievoorziening/2017.04.24/aandacht_voor_cyberveiligheid_door_phishingcampagne.htm

4.3.3 Cyberweerbaarheid blijft achter bij digitale dreigingen



Maandag 26 juni 2017 | Het laatste nieuws het eerst op NU.nl

Voorpagina
Net binnen
Algemeen
Economie
Zakelijk
Sport
Tech
Internet
Gadgets
Games
Mobiel
Entertainment
Lifestyle
Overig
Video's
Regionaal

NU.nl > Tech > Internet

Foto: 123RF

'Nederlandse cyberweerbaarheid blijft achter bij digitale dreigingen'

Gepubliceerd: 21 juni 2017 10:12
Laatste update: 21 juni 2017 10:11

Bedrijven, overheden en burgers wapenen zich niet snel genoeg tegen de groeiende digitale dreigingen. Dat staat in het Cybersecuritybeeld Nederland 2017.

Volgens het rapport van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) wordt het gat tussen dreiging en maatregelen eerder groter dan kleiner.

De onderzoekers zeggen dat mensen zowel thuis als op het werk vaak kiezen voor de snelste oplossing en niet de veiligste. Voor organisaties geldt dat ze zich steeds bewuster worden van risico's. Toch nemen ze fundamentele maatregelen zoals het installeren van zogenoemde beveiligingspatches vaak niet. Dat geldt voor zowel kleine als grote organisaties, waardoor besmettingen met kwaadaardige software mogelijk zijn.

In het Cybersecuritybeeld staat dat professionele criminelen en andere staten nog altijd de grootste dreiging vormen en de meeste schade aanrichten. Daarbij zijn criminelen uit op rechtstreeks financieel gewin en houden landen zich bezig met digitale spionage.

Ministeries

Zo waren Nederlandse overheidsinstellingen het afgelopen jaar doelwit van grote en hardnekkige digitale spionageaanvallen. De ministeries van Defensie en Buitenlandse Zaken zijn daarbij ook aangevallen door landen "die niet eerder zijn waargenomen als dreiging".

Het rapport geeft geen verdere details over de aanvallen. Het is onduidelijk of de pogingen tot spionage zijn geslaagd.

Zorgelijk

Criminelen ontwikkelen ondertussen nieuwe methodes. Zo vallen ze vaker gericht organisaties aan met zogeheten ransomware als ze denken dat de impact groot is en organisaties geneigd zullen zijn om een hoger bedrag aan losgeld te betalen voor 'gegijzelde' bestanden. De vrees bestaat dat criminelen in de toekomst dit soort gijzelsoftware ook zullen inzetten tegen industriële controlesystemen (ICS), met alle mogelijke gevolgen van dien.

Aparte aandacht is er voor het Internet of Things (IoT). Grote DDoS-aanvallen worden tegenwoordig ook uitgevoerd via 'gewone' apparaten zoals routers, webcams en digitale tv-ontvangers. De (consumenten) elektronica heeft doorgaans geen goede beveiliging en is daardoor te misbruiken.

Staatssecretaris Klaas Dijkhoff spreekt van een "zorgelijk beeld". Het bevestigt volgens hem dat iedereen nodig is om de digitaliserende wereld veilig te houden. "Bedrijven door bijvoorbeeld geld te reserveren om hun netwerk veilig te houden, gewone Nederlanders door digitaal veilige spullen te kopen."

Door: ANP/NU.nl

Figuur 16: Cyberweerbaarheid blijft achter digitale dreigingen

Bron:
http://www.nu.nl/internet/4783344/nederlandse-cyberweerbaarheid-blijft-achter-bij-digitale-dreigingen.html

Uit bovenstaande nieuwsbericht figuur 16 ,die dateert uit 21 juni 2017 blijkt dat cyberweerbaarheid achter blijft bij digitale dreigingen.

4.4 Welke maatregelen neemt RWS op het gebied van social engineering aanvallen (E4)?

In deze paragraaf wordt beschreven welke maatregelen RWS treft op het gebied van technieken van SE aanvallen.

4.4.1 Cybersecurity

Cyber Security is een actueel onderwerp binnen RWS door de veranderende maatschappij, waarin we steeds meer afhankelijk zijn van automatisering en vanwege een verhoogde cyberdreigingen wil RWS de veilige werking van bedienbare objecten op orde hebben.

Om te kijken wat er nodig is om systemen en objecten te beveiligen, mensen bewust en alert te maken en beheerprocessen op orde te brengen wordt er momenteel via Programma IMPAKT (Impuls Programma Aanpak Kritische infrastructuur) en Security Center van RWS al veel aandacht besteed aan de technische kant van cyber security. Met als einddoel goed beveiligde, betrouwbare en veilig werkende objecten en systemen.

De maatregelen die security center en programma IMPAKT treffen raken het aspect: mens, proces & organisatie en de techniek. In paragraaf 4.4.4 en 4.4.5 worden de maatregelen beschreven, die vanuit programma IMPAKT en Security center zijn genomen. Vanwege het lekken van informatie.

4.4.2 Programma IMPAKT

De IA is de infrastructuur die direct verbonden is met de missie van RWS. Binnen Programma IMPAKT worden de onderstaande maatregelen genomen.

4.4.3 Scope IMPAKT

Het projectteam van IMPAKT heeft tijdens de nulmetingen (schouwrondes) van deze objecten controles uitgevoerd op de volgende aspecten: beveiliging, veiligheid en betrouwbaarheid van deze objecten. RWS heeft verschillende bedienbare kunstwerken. Van bruggen, sluizen tot tunnels en keringen. Hieronder in figuur 17 kunt u aflezen om hoeveel objecten het betreft binnen RWS.

Figuur 17: Impakt
Bron: Impakt Intranet: http://corporate.intranet.rws.nl/projecten/data_en_ict/impakt_beveiligd_werken/

4.4.4 Maatregelen Programma IMPAKT

Maatregel 1: De objecten die vallen onder de volgende primaire infrastructuur netwerken namelijk Hoofdwegennet (HWN), Hoofdvaarwegennet (HVWN) en Hoofdwatersysteem (HWS) voldoen niet aan de eisen volgens de wet- et en regelgeving conform CSIR, upgrading is daarmee noodzakelijk. Momenteel heeft het Programma IMPAKT reeds veel aandacht besteed aan de technische kant van cyber security van alle objecten binnen RWS.

Toelichting aanpak maatregel 1:

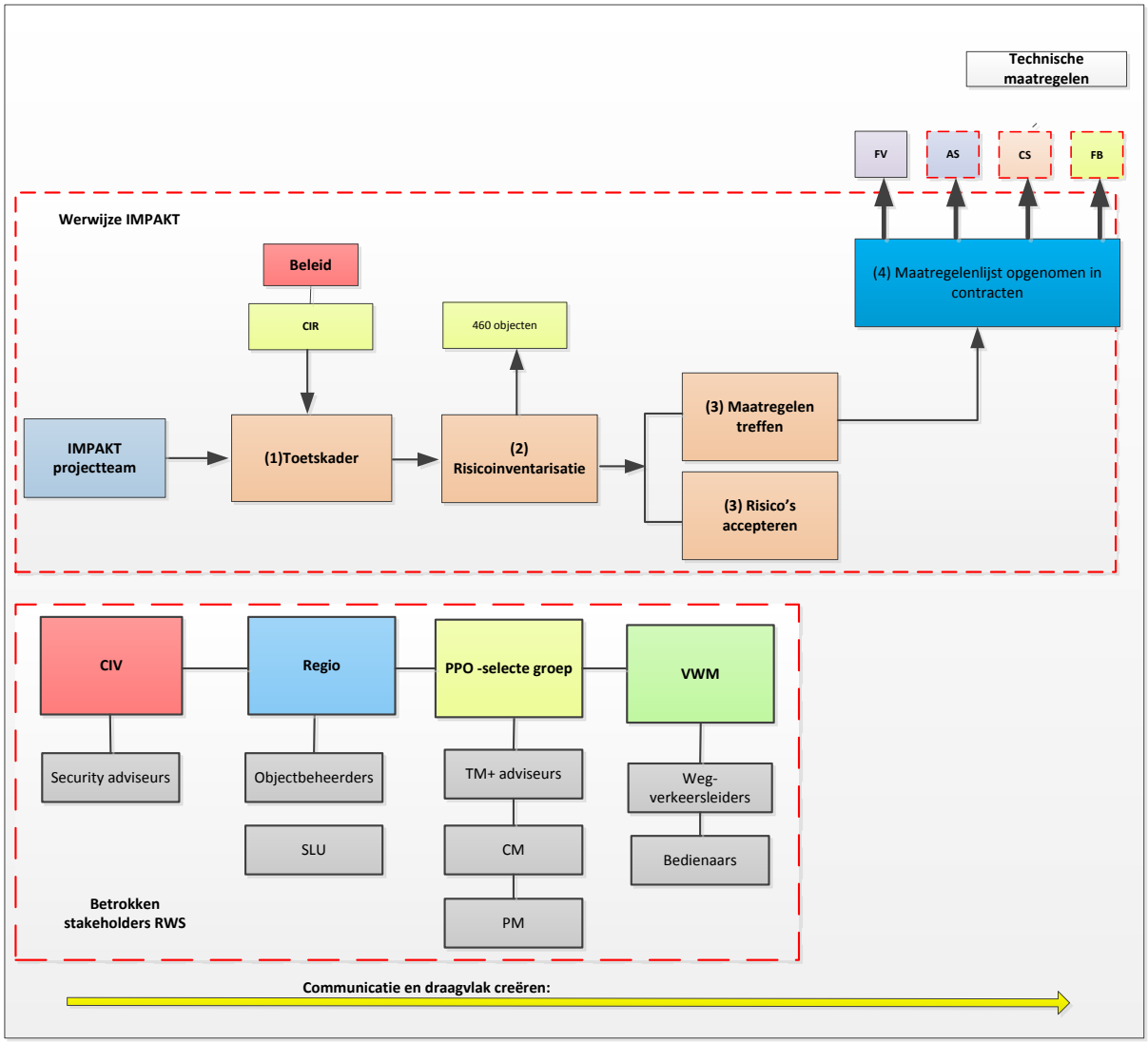
Toets kader: IMPAKT werkt gefaseerd om de kwetsbaarheid van de systemen te inventariseren en beweegbare objecten te beperken, bezoeken ze in het programma IMPAKT waterkeringen, sluizen, stuwen, gemalen, bruggen, verkeerscentrales en tunnels van RWS. Het Impakt projectteam heeft de CSIR maatregelen, die in paragraaf 4.2.4 tabel 9 zijn benoemd opgenomen in een toetskader.

- **Risico inventarisatie:** Het impakt projectteam weet wat het beleid voorschrijft en bezoekt alle objecten, die in scope van Programma IMPAKT zitten.. Programma Impakt kijkt naar de IST-situatie van het desbetreffende object. Hiermee worden de risico's geïnventariseerd, veiligheidstesten uitgevoerd en te nemen maatregelen beschreven met het doel om de veiligheid, beveiliging en betrouwbaarheid van de objecten te verbeteren en te borgen conform de CSIR. Deze inventarisatie vindt plaats met de beheerder van de Regio, de bedienaars van VWM, IPM team van PPO en de aannemer. Dit is schematische weergegeven in figuur 17 hieronder.

- **Treffen/Risico's accepteren:** Na de inventarisatie wordt gekeken welke maatregelen werkelijk uitgevoerd dienen te worden i.v.m. de haalbaarheid van de maatregel. Indien dit niet het geval is wordt hiervoor een explain voor aangemaakt (dan accepteren ze de risico's die zich voordoen).

  Uitvoeren: De te nemen maatregelen worden in een opdracht richting de huidige opdrachtnemer gecommuniceerd en de opdrachtnemer gaat deze maatregelen uit voeren naast de reguliere werkzaamheden waarvoor hij verantwoordelijk is. Het IMPAKT projectteam treft maatregelen voor Functioneel Veiligheid (FV), Assetmanagemanagement Proces (AS), Cybersecurity (CS) en Fysieke Beveiliging (FB).

Het IMPAKT projectteam voert zijn werkzaamheden gefaseerd uit zoals hieronder in figuur 18 aanpak maatregelen is te zien. Gedurende het verloop van het proces informeert het IMPAKT projectteam de betrokken stakeholders om bewustzijn, urgentiebesef en draagvlak te creëren met betrekking tot awareness voor cybersecurity.

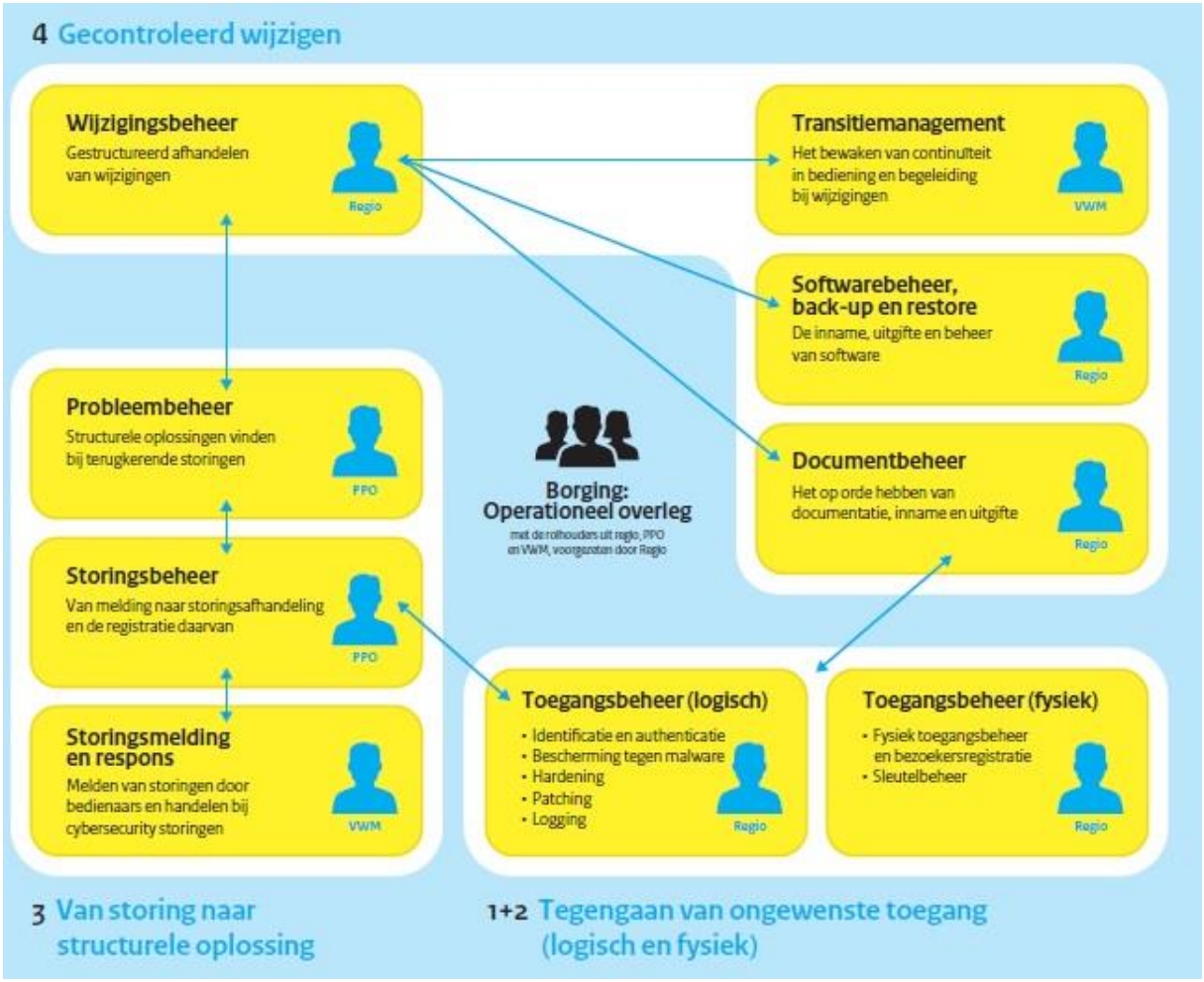


Figuur 18: Aanpak maatregel

Maatregel 2:
Indien informatie behoefte:
Een tweede maatregel wat IMPAKT treft is de beheersing van industriële automatisering. De snelle ontwikkelingen op het gebied van IA hebben grote impact voor de objecten van RWS. Doordat tegenwoordig veel van de processen geautomatiseerd zijn of worden ondersteund door IA, vraagt de beveiliging en veilig werking van de bedienbare objecten een steeds belangrijke rol nu en in de toekomst. Voorbeeld hiervan zijn bediening op afstand en veiligheids- en communicatiesystemen in verkeerscentrales en tunnels.

Om dit goed te beheersen is aanwezigheid van assetmanagement en cybersecurity processen noodzakelijk. Het IMPAKT projectteam is momenteel bezig om de processen binnen RWS te implementeren en workshops te geven over elke proces.

In onderstaande figuur 19 is een overzicht van de Asset Management (AM) en Cybersecurity processen voor IA bij beweegbare objecten weergegeven. De blauwe vlakken zijn processen, de richting van de pijlen geeft de informatiestroom weer en dus ook de onderlinge relatie.



Figuur 19: Handreikingen voor de beheersing van industriële automatisering
Bron: http://corporate.intranet.rws.nl/projecten/data_en_ict/impakt_beveiligd_werken/2016.05.23/handreikingen.htm

Maatregel 3: Awareness trainingen voor wegverkeersleiders. Er wordt alleen aan de WVL die in de verkeercentrale zitten een specifieke cursus gegeven omtrent de volgende punten:

- Bewustmaken van cyber security risico's bij IA
- Bewustmaken van de noodzaak van goede procedures
- Leren herkennen van verdachte situaties
- Bewust maken van nieuwe dreigingen

4.4.5 Afdeling Security Center

Binnen de Security center worden de volgende maatregelen uitgevoerd:

Eerste maatregel: vertaling van CSIR maatregelen naar contract eisen DBFM, D&C, P&C contracten en de bijlagen. In de model- en uitvoeringscontracten, voor PPO m.n. PC en E&C, zijn contractteksten opgenomen om cybersecurity van onze objecten te bevorderen.

Tweede maatregel: Security borgen in de methodiek system engineering.
Om van projectopdracht tot een contract (vraagspecificatie) te komen, wordt binnen RWS gebruik gemaakt van de methodiek systems engineering.

Deze methodiek is als standaard opgenomen binnen Werkwijze Aanleg Onderhoud (WWAO). Systems Engineering wordt naast RWS ook door verschillende partners in de Grond-, Weg- &

Watersector gedragen om zo uniformiteit over de werkwijze uit te dragen en overeenstemming te krijgen over de begrippen die daarin worden gehanteerd.
Op basis van deze afspraken heeft RWS voor haar eigen organisatie een bedrijfsspecifieke invulling aan deze gezamenlijke taal gegeven door het ontwikkelen van de procesbeschrijving system engineering

De methodiek system engineering
System engineering is in essentie een gestructureerde specificatie- en ontwerpmethode. System engineering heeft tot doel structuur te geven aan-, en het inzicht te verschaffen in de complexiteit van het te realiseren object.

Met behulp van system engineering kunnen risico's die ontstaan door verkeerde of niet volledige informatie en uitgangspunten worden beheerst. Het gaat erom dat het systeem als totaal wordt beschouwd, over de gehele cyclus, inclusief de samenhang met zijn omgeving.
Bron: Leidraad SE versie 3.0 (19 november 2013)

System engineering biedt een geïntegreerde en gestructureerde set methodieken om projecten succesvol te verwezenlijken en te beheren. De kernelementen uit de gehanteerde definitie die dit beschrijven kunnen ook als volgt worden samengevat:

- Het op gestructureerde wijze specificeren van een behoefte
- Het op gestructureerde wijze ontwerpen van een passende oplossing bij de behoefte
- Het op een correcte wijze realiseren van deze oplossing
- Het op een juiste wijze beheren van de gerealiseerde oplossing
- Het op een juiste wijze verifiëren en valideren
- Het op een beheerste wijze managen van het gehele project gedurende zijn levensduur

Daarmee wordt inzichtelijk gemaakt dat system engineering een methodiek is die de gehele levenscyclus van projecten ondersteunt.

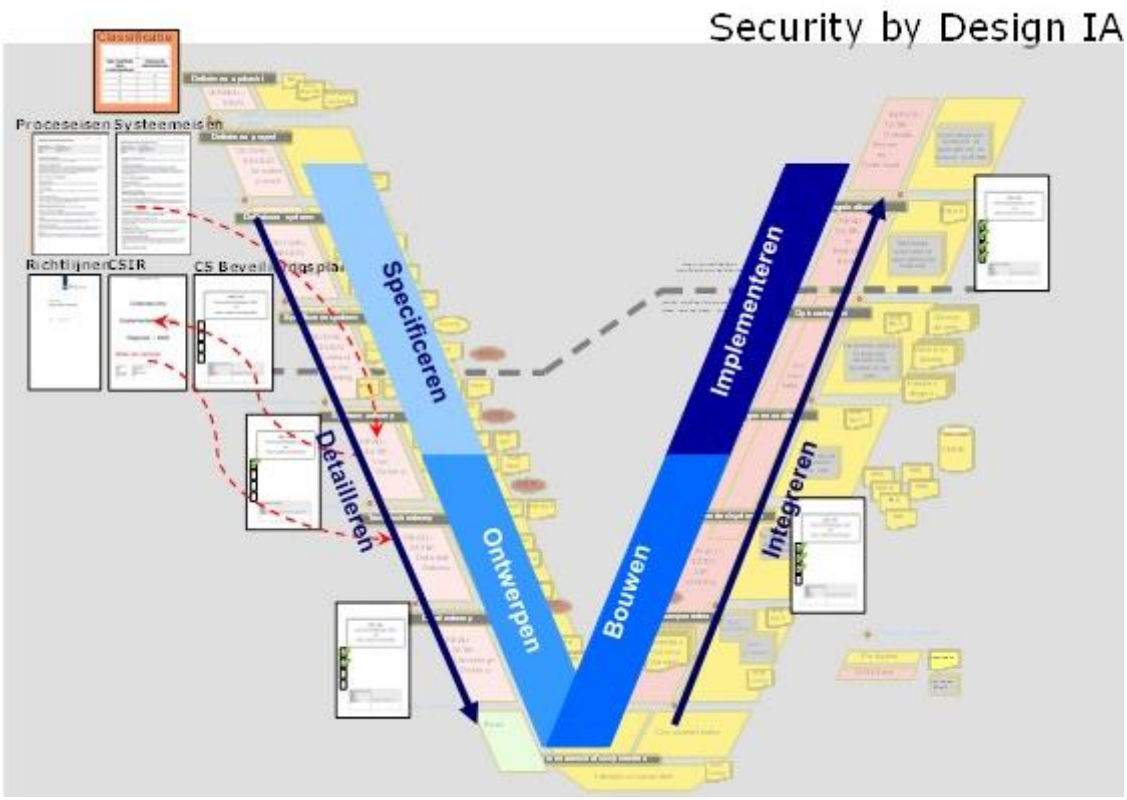
Een belangrijk onderdeel van system engineering is het iteratieve proces. Het iteratieve proces is bij complexe systemen een herhaling van specificeren op meerdere detailniveaus, waarbij op basis van de bestaande set met eisen ontwerpkeuzes worden gemaakt. Van dit ontwerp kunnen eisen worden afgeleid die leiden tot ontwerpkeuzes op een concreter en specifieker niveau (of een kant-en-klaar product).

Dit iteratieve proces leidt tot een decompositie van het te realiseren systeem. Het resultaat van het doorlopen van dit iteratieve proces in de ontwikkelfase is een gespecificeerd systeem, inclusief het daaraan getoetste ontwerp.

Vervolgens wordt het ontworpen systeem bottom-up gerealiseerd en hoofdzakelijk geverifieerd aan het ontwerp. Het detailniveau van specificeren wordt bepaald door het risicoprofiel, de complexiteit van het te realiseren systeem en de benodigde concreetheid van informatie om het systeem te kunnen realiseren. Het iteratieve proces wordt weergegeven in een V-model.
Bron: Procesbeschrijving SE versie 2.1.2 (25 januari 2017)

Security borgen in de system engineering methodiek
Security is een integraal onderdeel van het te ontwerpen, bouwen, realiseren en te onderhouden systeem. In figuur 20 hieronder is aangegeven welke documenten leidend zijn gedurende het V-model.

Het iteratieve proces is ook toepasbaar op security. Het security V-model wordt als volgt weergegeven:



Figuur 20: Security by design IA.
Bron: security by design in V model

Derde maatregel:
Voor de lopende onderhoudscontracten moet er een reparatie worden uitgevoerd. Daar zitten de cybersecurity eisen (beheersdoelen en beheersmaatregelen) nog niet in contracten. Afhankelijk van de looptijd en risico's worden contracten opengebroken en waar nodig gerepareerd. Hierbij wordt tevens rekening gehouden met het geplande groot onderhoudsmoment en de levenscyclus van het object.

Vierde maatregel: De projectteams (PPO) zijn geen goede gesprekspartner voor de marktpartijen wat betreft cybersecurity. Er wordt door afdeling security ondersteuning geboden om kennis te delen, zodat de adviseurs techniek IA worden de Cybersecurity

Vijfde maatregel: Awareness trainingen cybersecurity
Rijkswaterstaat breed wordt er via het CLC leerportaal online trainingen aangeboden voor alle medewerkers om awareness op te doen t.a.v. van de cyber security.

4.5 Wat voor een mening hebben medewerkers van RWS over de factoren die invloed hebben op het gedrag in een IA object(E5)?

4.5.1 Interview resultaten

In het onderzoek is er onderscheid gemaakt tussen de onderstaande 4 onderzoeksgroepen zoals terug te lezen in tabel 15 en daarnaast is vanwege de anonieme afnamen van de interviews bij de respondenten de functiegroep (onderzoeksgroep) waar ze onder vallen getoond en hun definities. In totaal zijn 11 respondenten geïnterviewd.

Reden waarom deze groep is benaderd door de onderzoeker heeft te maken met het feit omdat ketensamenwerking noodzakelijk is binnen het proces van borging van security binnen een organisatie.

Onderzoeksgroep	Definitie	Type interview
Projectleden (IPM team)	Dit zijn mensen die de tunnelprojecten realiseren zonder direct betrokken te zijn met Cybersecurity.	Semi gestructureerd
Experts (Security)	Dit zijn mensen die de CSIR en Cybersecurity eisen hebben opgesteld voor contracten.	Semi gestructureerd
Objectbeheerders	Dit zijn de objectdeskundige en installatieverantwoordelijke.	Semi gestructureerd
Bedienaars	Bediening, bewaken van bijvoorbeeld tunnels en verkeerssignalering	Semi gestructureerd

Tabel 15: Onderzoeksgroepen

4.5.2 Operationalisatie

De interview resultaten zijn gecodeerd naar de factoren die invloed hebben op het gedrag van een individu, daarnaast is gedefinieerd wat de factoren inhouden en is vervolgens aangegeven welk informatie uit interview en enquête wordt gemeten.

Factor	Definitie	Variabele (interview)	Variabele (enquête)
1. Normatieve context	Het door een medewerker ervaren druk vanuit een bepaalde context bij het vertonen van ‘veilig gedrag’.	• Soort druk (groepspatroon/groepsare na/mindset) dat een medewerker ervaart in zijn omgeving bij het vertonen van ‘veilig gedrag’.	• Mate waarin gedrag wordt beïnvloed door een specifiek context waarin een medewerker zich bevindt.
2. Risico-perceptie	Hoe serieus iemand de situatie ziet.	• De beleving die een individu heeft ten aanzien	• Mate waarin een individu de situatie als onveilig ervaart.

			van de kans op informatieverlies en de gevolgschade die betrekking heeft op persoon zelf..	
3.	**Attitude**	De houding van een medewerker over dat een maatregel leidt tot een veilige situatie.	• Verwachting dat met een maatregel het gevaar wegneemt en de individu zelf in staat is om de maatregel succesvol zonder fouten uit te voeren.	• Mate waarin de individu zich positief of wel negatief opstelt ten opzichte van een maatregel.
4.	**Zelf-Doeltreffend-heid**	De mate waarin een individu weet welke kennis en vaardigheden nodig zijn om naar een veilig situatie te komen.	• Aard van het doel die een individu aan zichzelf heeft gesteld om uiteindelijk in staat te zijn om zelf veilig gedrag te vertonen.	• De mate waarin een individu zich wel/niet inzet om een leerdoel te bereiken.

Tabel 16: Operationalisatie

4.5.2 Norm

Interviewresulaten:

In dit onderdeel ligt de basisprincipe ten grondslag, dat menselijk handelen wordt beïnvloed vanuit de context waarin medewerkers zich bevinden. Aan de hand van interview resultaten wordt getracht het waarom te achterhalen van het handelen: eerst wordt nagegaan of in de praktijk bij RWS medewerker ook zo is dat de context invloed heeft op hun gedrag en vervolgens wordt gekeken wat voor een soort gedrag een medewerker beweegt om op een bepaalde wijze te handelen. Daaropvolgend is middels enquête gekeken of deze observaties voor een grote groep geldt, door statistische onderbouwing.

Variabele: Soort druk (groepspatroon/groepsarena/mindset) dat een medewerker ervaart in zijn omgeving bij het vertonen van ‘veilig gedrag’

Uit de resultaten blijkt dat de context waarin medewerkers handelen op verschillende wijze invloed heeft op hoe zij omgaan met vertrouwelijke informatie. Alle medewerkers zijn het eens met de volgende stelling: ‘*de situatie waarin zich een medewerker bevindt, heeft invloed op de wijze waarop met informatie wordt omgaan*’.

Drie van de zeven geïnterviewde geven aan dat ze handelen op basis van wat zij denken dat hun collega’s als goed of fout vinden. De volgende citaten illustreren dit:

Vertrouwelijke informatie indien behoefte kan deze opgevraagd worden bij de auteur.

'Als ik meer wil weten over een object, dan doe ik dat altijd door eerst de objectbeheerder hierover persoonlijk te benaderen, hetzij door te bellen of een afspraak te maken. Dit doe ik omdat ik weet dat dit wordt gewaardeerd door de objectbeheerder. Het geeft hem een gevoel van controle over zijn eigen te beheren object.' (projectlid)

Een van de zeven geïnterviewde geeft aan te handelen op basis van wat zij zelf denken dat goed of fout is. Het volgende citaat illustreren dit:

Vertrouwelijke informatie indien behoefte kan deze opgevraagd worden bij de auteur.

Onderstaande citaat laat zien dat de medewerker handelt door combinatie van persoonlijke norm en gedragspatroon wat hij op de werkvloer zit. Beide normen conflicteren met elkaar (wel/niet aanspreken), en het is interessant te zien dat de persoonlijke norm enigszins wordt afgezwakt:

'Een collega aangesproken dat hij een eigen externe harde schijf niet zomaar aan het RWS netwerk kan koppelen. Ik vind het belangrijk om mensen aan te spreken op wat ze fout doen en aangeven hoe wel te handelen. Echter zie ik op de werkvloer dat collega's elkaar minder snel aanspreken op hun gedrag. Het is voor mijn daarom lastiger om mijn directe collega's aan te spreken, mensen die ik niet ken spreek ik nog wel aan' (objectbeheerder)

Het is interessant om te melden dat dezelfde objectbeheerder (die vanuit een persoonlijke norm acteert) ook aangeeft dat als iemand hem onder druk zet door bv. angst om informatie prijs te geven, hij hier gevoelig voor is en zich niet voor kan stellen dat hij geen informatie prijs geeft. Dit terwijl een andere medewerker (een expert) zich ongevoelig hiertegen over opstelt.

Twee van de zeven geïnterviewde geven aan dat ze handelen op basis van hoe de omgeving zich gedraagt (gedragspatroon). De volgende citaten illustreren dit:

'Op onze bureaublad staat dat we onze pc moeten vergrendelen als we even van onze plek af zijn. Toch zie ik in de praktijk dat mijn collega's hier verschillend mee omgaan. Sommige collega's die vergrendelen hun pc al bij het halen van een koffie, terwijl anderen hun pc pas locken als zij naar een overleg toe gaan en dus wat langer weg zijn van hun werkplek. Afhankelijk naast welke collega ik zit, bepaal ik hoe snel ik mijn pc vergrendel.' (projectlid)

'Er heeft in verleden een collega een tas op plek gezien waar iedereen bij kon. In deze tas zaten wachtwoorden waarmee je toegang krijgt tot systemen om objecten mee te bedienen. Waarschijnlijk is een andere collega de tas daar vergeten. De collega die het heeft gezien, heeft hier een melding van gemaakt aan mij. Waarna ik de tas heb opgehaald en achter slot en grendel heb geplaatst.' (bedienaar)

4.5.3 Risicoperceptie

In dit onderdeel ligt de basisprincipe ten grondslag, dat menselijke handelen wordt beïnvloed vanuit de kans dat situatie optreed en de gevolgen ervan.

De risicoperceptie die een individu ervaart ten aanzien van informatieverlies of –schade risicoperceptie is te meten en is bijvoorbeeld te beïnvloeden door middel van het verschaffen van risico-informatie. Aan de hand van interview resultaten wordt getracht te achterhalen hoe groot de kans is dat een dergelijke situatie optreedt en wat de gevolgen ervan zijn. Daaropvolgend is middels enquête gekeken of deze observaties voor een grote groep geldt, door statistische onderbouwing.

Interview resultaten:

Variabele: De beleving die een individu heeft ten aanzien van de kans op informatieverlies en de gevolgschade die betrekking heeft op persoon zelf.

Uit de resultaten blijkt dat de ernst van het gevaar waaraan medewerkers blootgesteld zijn verschillend wordt ervaren. Alle geïnterviewde zijn het eens met de volgende stelling: '*de IA-objecten zijn een gewilde doel voor mensen met kwade bedoelingen'*. Het verschil zit in het feit dat het ene deel van de geïnterviewde het gevaar op een wat abstractere termen formuleert c.q. ervaart en weer een ander deel het gevaar specifiek benoemt, gerelateerd aan zijn werk.
Hieronder een voorbeeld van een geïnterviewde die het gevaar, specifiek gerelateerd aan zijn werk relateert:

> *'Er is een redelijke kans dat een bedienaar door nalatigheid zijn tas met wachtwoorden vergeet terug te zetten in een locker. Een vreemde persoon kan deze tas meenemen en de wachtwoorden gebruiken om in te loggen op het bediensysteem. Als zo een persoon kwade bedoelingen heeft, dan kan hij de objecten zodanig beheren totdat er zelfs dodelijke ongevallen plaatsvinden.' (bedienaar)*

Hieronder een voorbeeld van een geïnterviewde die het gevaar, abstracter formuleert, en het dus wat verder weg van zijn werk ervaart:

> *'Ik kan me voorstellen dat als vertrouwelijke informatie over onze objecten op straat komt, dat het op het nieuws kan komen en we als Rijkswaterstaat hierdoor imagoschade oplopen bij het publiek, namelijk het gevoel dat RWS haar werk niet goed uitvoert. Als projectlid ben ik ervoor verantwoordelijk dat Opdrachtnemers de fysieke en digitale toegang tot het object volgens de contracteisen dienen te beheren, zodat hij veilig werkt. Het is onze taak om deze eisen mee te geven, echter is het vervolgens de verantwoordelijkheid van de Opdrachtnemer om zich aan de regels houden. Ik ken verder het object niet, om de moeilijkheidsgraad van toegangsbewaking per object in te schatten.' (projectlid)*

Interessant is hier om te weten dat een expert wel het gevaar kan relateren aan hoe een projectlid zijn werk doet. De expert geeft aan dat projectleden niet in staat zijn om Opdrachtnemers op een duidelijke wijze te instrueren over de te treffen beveiligingsmaatregelen. Opdrachtnemers zitten met vragen, die door het project niet beantwoord kunnen worden. Dit kan ertoe leiden dat Opdrachtnemers hun werk niet goed uitvoeren, omdat ze niet goed zijn geïnstrueerd. Vragen waar Opdrachtnemers over de email mee komen richting projectleden zijn onder andere:

> *'Ik had voor de werkgroep een aantal vragen mbt patchmanagement, momenteel natuurlijk erg actueel na het Wannacry-drama, willen inbrengen waarop we eigenlijk snel een antwoord zouden willen hebben. In de eisen die nu bij alle projecten worden gesteld mbt patchmanagement wordt onderscheid gemaakt tussen kritieke en niet kritieke patches. Voor kritieke patches dient binnen 48 uur een implementatieadvies te worden verstrekt aan Opdrachtgever en voor de niet-kritieke patches is dat een termijn van 8 weken. De vraag is, wie en op basis waarvan wordt bepaald wat wel een kritieke en wat een niet-kritieke patch is?' (verstrekte e-mailinformatie door expert)*

Daarnaast geeft ook een bedienaar aan hoe kritisch het werk van een projectlid is, namelijk ervoor zorgen dat de Opdrachtnemer zijn taak goed uitvoert.

> *'Een projectlid weet bv. niet dat als een opdrachtnemer zijn toegangspas verliest, hierdoor een onbevoegde met deze pas het gebouw binnen kan komen, en zo in het gebouw rond kan snuffelen op zoek naar vertrouwelijke informatie (zoals wachtwoord voor toegang tot bijv. bediening). Het kan zijn dat omdat een projectlid dit niet realiseert, hij hierdoor ook niet actief de opdrachtnemer op het veilig omgaan met toegangspas stuurt, maar in plaats daarvan ervan uitgaat dat de opdrachtnemer veilig werkt.' (bedienaar)*

Het lijkt erop dat medewerkers die wel in het object komen en dus het gebouw kennen, dat zijn de bedienaars en objectbeheerders, het gevaar dichter bij hun werk ervaren en dus meer waakzaam zijn. Dit in tegenstelling tot de mensen die niet in het object komen, dat zijn projectleden en de experts. Zij ervaren het gevaar op een wat grotere afstand. Hieronder de citaten van de bedienaar en objectbeheerder:

'Omdat in de verkeercentrale de bediening/bewaking systemen van verschillende objecten aanwezig is, en hier ook de plek is van waaruit je de objecten kan bedienen en ook de wachtwoorden kunt krijgen, is het zeer aantrekkelijk voor een kwaadwillende om dit object binnen te komen.' (bedienaar)

'Het object wordt door 'mensen van buiten', dat zijn mensen van onze aannemer, onderhouden. Voor het gemak, laten aannemers de toegangsdeur open om spullen naar binnen te sjouwen (nalatigheid). Een kwaadwillende kan door het dragen van hetzelfde jasje als een onderhoudsaannemer het vertrouwen bij RWS-medewerkers wekken en hierdoor ongemerkt door het gebouw snuffelen op zoek naar vertrouwelijke informatie.' (objectbeheerder)

Daarentegen vinden de experts en projectleden, die niet op de locatie komen, het lastiger om het gevaar van het lekken van informatie te relateren aan hun werkzaamheden. Dit blijkt uit de volgende citaten:

'Ik ben niet werkzaam op een bepaald object, dus kan ik hierover ook geen vertrouwelijke informatie verschaffen.' (projectlid)

'Voor een gemaal en een sluis is de gevolgschade groot dan wanneer een kwaadwillende een tunnel weet te bedienen. Een tunnel kan hooguit dicht worden gezet, door het bedienen van matrixborden boven snelwegen en het naar beneden halen van de slagbomen, en uitzetten van de lichten. Een tunnel die dicht wordt gezet, zal enkel verminderde bereikbaarheid veroorzaken. Bij een gemaal of een sluis kan water het land binnenstromen wat een dodelijk gevolg kan hebben.' (projectlid)

Vertrouwelijke informatie indien behoefte kan deze opgevraagd worden bij de auteur.

4.5.4 Attitude

In dit onderdeel ligt de basisprincipe ten grondslag, de houding die een individu aanneemt de verwachting dat met een maatregel het gevaar wegneemt en dat de individu zelf in staat is om maatregelen toe te passen wat leidt tot veilig gedrag.
Aan de hand van interview wordt ingegaan hoe medewerkers van RWS omgaan met gevaar. Je hebt twee meetindicatoren namelijk: verwachting dat een individu heeft dat een voorgeschreven maatregelen het gevaar weg kan nemen (nut van een maatregel) en als tweede meetindicator is of een individu in staat is om zelf de maatregel uit te voeren. Daaropvolgend is middels enquête gekeken of deze observaties voor een grote groep geldt, door statistische onderbouwing.

Interview resultaten:
Variabele: Verwachting dat met een maatregel het gevaar wegneemt en de individu zelf in staat is om de maatregel succesvol zonder fouten uit te voeren.

Alleen de expert die de beveiligingsmaatregelen voor IA-objecten heeft opgesteld (CSIR) weet van het bestaan af van dit document, waarin de beveiligingsmaatregelen staan voor IA-objecten. Alle overige geïnterviewde (objectbeheerder, bedienaar, projectlid) kennen dit document niet en weten dus ook welke gedragsregels van hun wordt verwacht. Gedragsregels die niet-specifiek voor IA-objecten gelden, daar zijn alleen de projectleden van op de hoogte.

'Ik ben niet bekend met de CSIR richtlijnen, wel met BIR.' (projectlid)
'Ik ben hier niet persoonlijk bekend mee, maar ik weet dat onze specificeerder deze gebruikt voor de vraagspecificatie.' (projectlid)

'Ik ben niet bekend met de richtlijn, kan hierdoor ook niet aangeven of het van toepassing is op mijn werk en welke invulling ik er aan geef.' (bedienaar)

De objectbeheerders weet vanuit de praktijk dat er binnen zijn object, mensen bezig zijn om technische maatregelen te treffen. Hij ziet dus hoe de technische maatregelen uiteindelijk bijdragen

aan beveiliging. Echter heeft hij minder op het netvlies wat hun rol hierin is en zich afvragen of het effect heeft. Dit blijkt uit de volgende citaten:

Vertrouwelijke informatie indien behoefte kan deze opgevraagd worden bij de auteur.

> *'Ik zie dat heel veel mensen rondlopen om de objecten technisch te beveiligen, maar er is richting mij niet gecommuniceerd wat ik als persoon zelf moet doen.' (objectbeheerder)*
> *'Manipulatief gedrag is menseigen. Tegelijkertijd denk ik dat individuen hier zelf bewust mee om moeten gaan' (projectlid)*

Wel weet alleen 1 geïnterviewde aan te geven dat een maatregel uit CSIR over hoe een mens dient te handelen effect heeft:

> *'Ik sta positief tegenover het maatregelenpakket, omdat dit door voorvallen in de praktijk nodig blijkt te zijn. Het maken van bijvoorbeeld een back-up voorkomt dat gegevens van RWS gegijzeld kunnen worden door derden (wannacry-incident).' (projectlid)*

De experts erkennen de situatie. De eerste prioriteit vanuit CSIR was om de objecten technisch te beveiligen en we zijn nu bezig om de medewerkers te instrueren. Bij het tonen van de gedragsregels uit de CSIR, blijkt dat de medewerkers niet in staat zijn om de maatregelen uit te voeren. Twee voorbeeld maatregelen zijn aan de geïnterviewde personen voorgelegd: (1) maatregel *'BTME5 melden van een beveiligingsincident'* en (2) maatregel 'BTMA2 Manager zorgt ervoor dat Opdrachtnemer toegang tot object volgende bepaalde procedures bewaakt'.

Bij het eerste maatregel geven meerdere personen aan dat zij niet kunnen beoordelen of iets wel of niet een beveiligingsincident is om daar vervolgens op te acteren en dit langs de daarvoor geldende procedures door te melden. Beveiligingsincidenten dienen namelijk sneller opgepakt en afgehandeld te worden;

Vertrouwelijke informatie indien behoefte kan deze opgevraagd worden bij de auteur.

Bij het tweede maatregel geven meerdere personen aan dat een projectlid die de taak heeft om Opdrachtnemers te instrueren, niet in staat zijn dit goed te doen. Overigens is het bij een projectlid ook onduidelijk of hij hiervoor aan de lat staat, uit de CSIR maatregelen is dit niet direct te herleiden.

Er staat wel duidelijk in CSIR wat een Opdrachtnemer dient te doen, maar niet wie ervoor verantwoordelijk is dat de Opdrachtnemer zijn taak goed uitvoert. Er staat alleen in dat een 'Manager' dit moet doen, maar niet wie dat dan is. In ieder geval kan een project lid een opdracht nemer niet instrueren en zijn specifieke vragen beantwoorden.

> *'Ik ben niet bekend met de CSIR eisen die we stellen aan Opdrachtnemers, maar ik weet dat onze specificeerder deze gebruiken voor de vraagspecificatie.' (projectlid)*

> *'De experts geven aan dat de medewerkers van PPO geen goede gesprekspartner zijn richting de markt met betrekking tot vragen over cybersecurity. Ze bezitten de kennis niet en kunnen ook de vragen vanuit markt niet beantwoorden. Ze krijgen ondersteuning vanuit experts momenteel.' (expert)*

4.5.5 Zelf-Doeltreffendheid

In dit onderdeel ligt de basisprincipe ten grondslag, het prijs geven van vertrouwelijke informatie hangt af van de methoden en technieken waarmee een medewerker wordt overgehaald en hoe dit te beheersen. Aan de hand van interview resultaten wordt getracht te achterhalen wat een mogelijk oorzaak kan zijn tot het vrijgeven van de vertrouwelijke informatie. Daaropvolgend is middels enquête gekeken of deze observaties voor een grote groep geldt, door statische onderbouwing.

Interview resultaten:
Variabele: Aard van het doel die een individu aan zichzelf heeft gesteld om uiteindelijk in staat te zijn om zelf veilig gedrag te vertonen.
De objectbeheerders en bedienaars zijn georiënteerd op het minimaliseren van het gevaar in en rondom het object waar ze verantwoordelijk voor zijn. Als het om de gevaren van social-engineering gaat en hoe je dat beheerst, zijn zij vooral geïnteresseerd te weten hoe zij vanuit hun rol en taakomschrijving hieraan bij kunnen dragen. Met andere woorden zij voelen zich verantwoordelijk om de veiligheid te borgen van het object en deze performance willen ze ook in de nieuwe situatie met toenemende cyberdreigingen kunnen leveren. Echter de een heeft voldoende positieve ervaring met het onder de knie krijgen van hoe om te gaan met cyberdreigingen, terwijl een ander hier eerder negatieve ervaringen mee heeft. Dit blijkt uit de volgende citaten:

Onderstaande geïnterviewde is actief opzoek naar nieuwe informatie om zijn taak beter uit te voeren:

> *'Het object wat ik beheer is door Impakt programma op cyberdreigingen beoordeeld. Naast het feit dat ik zie dat er technische maatregelen worden getroffen om dit object beter te beveiligen, ben ik ook opzoek naar wat ik hier als persoon vanuit mijn rol aan kan doen. Zo heeft een collega mij erop geattendeerd dat via het corporate learning center (CLC) van RWS training wordt aangeboden over cyberdreigingen.' (objectbeheerder)*

Onderstaande geïnterviewde zijn niet gemotiveerd om zijn taak beter uit te voeren:

> '*Vanuit de lijnmanager wordt geen toezicht gehouden of ik trainingen heb gevolgd over cyberdreigingen om mijn taak uit te voeren. Ik ben dus hier niet op aangesproken en word er ook niet op beoordeeld. Daarnaast mocht ik het ook willen volgen, dan zit ik heel krap in mijn tijd en zou het dus in mijn eigen tijd moeten volgen.' (bedienaar)*
> *'De afdelingshoofd heeft mij niet erop gewezen dat er trainingen zijn op het gebied van cybersecurity en dat het voor mijn werk ook belangrijk is het ook te volgen. Dus ik ga ervanuit dat andere mensen verantwoordelijk zijn om problemen met cybersecurity op te lossen en niet ik. Ik ga daar niet over.' (projectlid)*

Daarnaast blijkt dat RWS experts trainingen over cybersecurity met een ander doel hebben opgezet, namelijk kennis en awareness creëren bij de medewerkers over wat cybersecurity is (dus het doel is om te leren). Dit terwijl de medewerkers meer geïnteresseerd zijn in hoe zij hun taken beter kunnen doen i.p.v. kennis op doen over alleen cybersecurity en wat de methoden en technieken zijn. Dit blijkt uit het volgende citaat:

> *'Wij als experts hebben trainingen opgezet met als doel eerst de bedienaars te informeren over cyberdreigingen, zodat zij hun werk veilig kunnen uitvoeren. De insteek is om klein te beginnen en te focussen op kennis delen en leren door te doen en de lange termijn maatregelen richten zich op het ontwikkelen en verspreiden van kennis op cybersecurity gebied binnen PPO (organisatieonderdeel RWS). Waaraan gedacht kan worden bv. is het beheersen van cybersecurity risico's is een samenwerking van meerdere onderdelen in de organisatie.' (security expert)*

4.5.6 Enquête resultaten

Enquête

Welkom bij deze enquête over cybersecurity. Deze enquête maakt deel uit van mijn onderzoek. Graag wil ik u uitnodigen om deze enquête in te vullen. De enquête duurt 20 minuten en de antwoorden worden geanonimiseerd verwerkt in het onderzoek.

Door uw deelname hoop ik een breed scala van feiten en ervaringen te verzamelen. Ik wil u erop wijzen dat alle antwoorden strikt vertrouwelijk worden behandeld door mij als onderzoeker.

De enquête gaat over wat voor een mening medewerkers hebben over informatiebeveiliging tegen cybersecurity aanvallen, waarbij kwaadwillenden via medewerkers van Rijkswaterstaat toegang willen krijgen tot vertrouwelijke informatie. De technieken en methodes die daarbij worden gebruikt, worden ook wel social engineering genoemd.

De enquête begint met algemene vragen over de medewerker, vervolgens worden er vragen gesteld over:

1. De kennis van de medewerker op het gebied van informatiebeveiliging
2. De risicoperceptie die de medewerker ervaart ten aanzien van informatieverlies of schade
3. De attitude/houding van de medewerker waarmee hij of zij beveiligingszaken waardeert of niet
4. De subjectieve norm van de medewerker die ontstaat door hoe hij of zij denkt dat de directe omgeving bepaald gedrag waardeert of niet waardeert.

Toelichting enquête antwoorden:

Rondje = één antwoord mogelijk

Vierkant = meerdere antwoorden mogelijk

Other = Iets anders namelijk

Mij dank is groot voor uw deelname.

Mochten er nog vragen zijn, neem dan gerust contact met mij op:
Mustafa Nizami
06xxxxxxxx
mustafa.nizami@rws.nl

Enquête resultaten

QUESTIONS RESPONSES 102

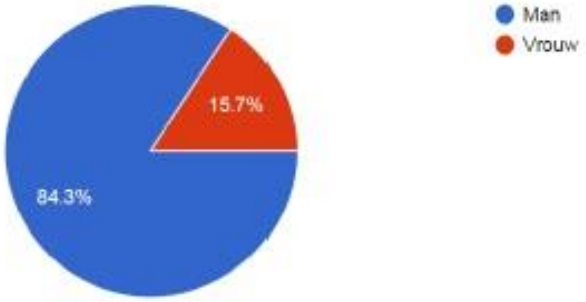
102 responses

Algemene informatie

Vraag 1: Wat is uw leeftijd?

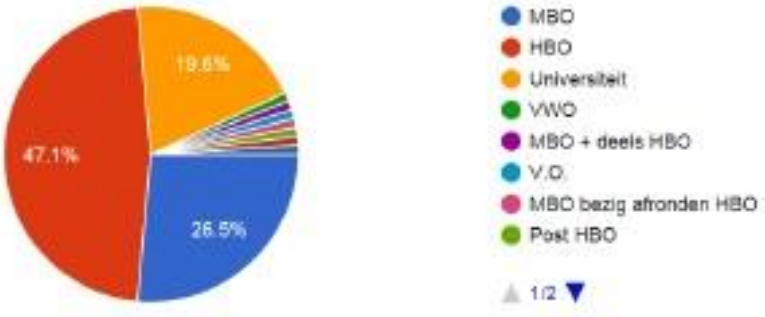
Vraag 2: Wat is uw geslacht?

102 responses



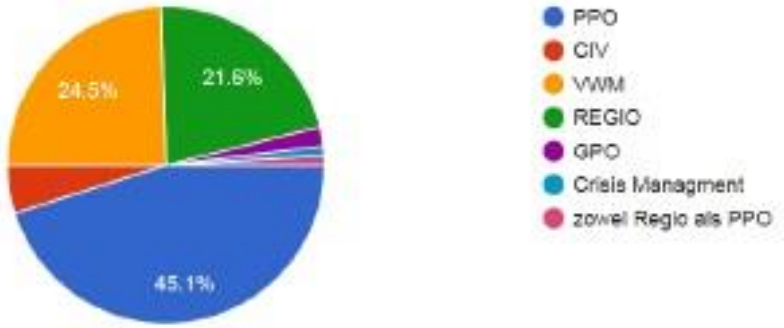
Vraag 3: Wat is uw hoogste genoten opleiding?

102 responses



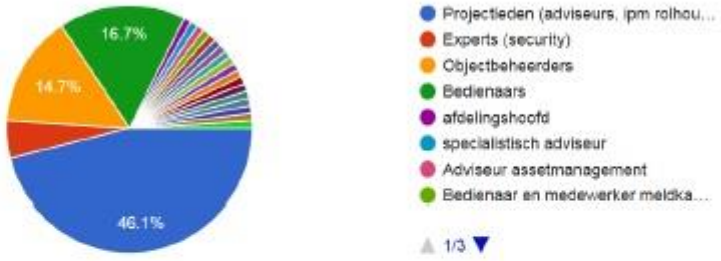
Vraag 4: Onder welk organisatie onderdeel valt u?

102 responses



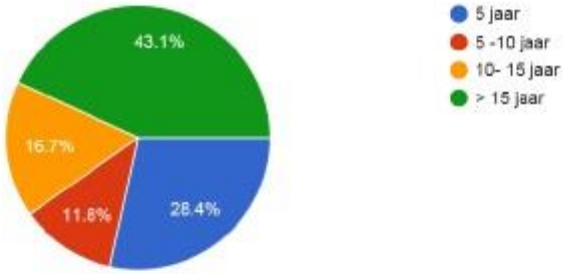
Vraag 5: Onder welke categorie valt uw functie?

102 responses



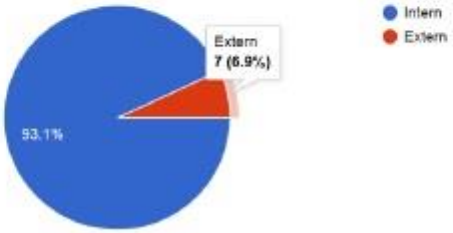
Vraag 6: Hoeveel jaar bent u in dienst bij Rijkswaterstaat?

102 responses



Vraag 7: Bent u een interne medewerker of externe medewerker?

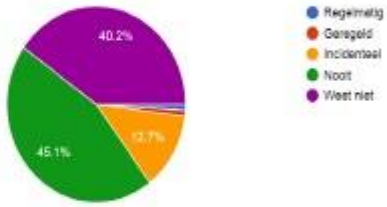
102 responses



Kennis over social engineering

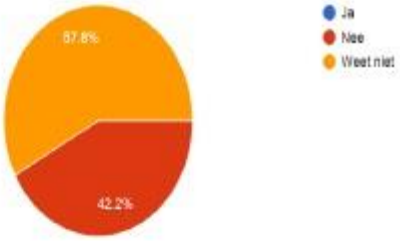
Vraag 8: Is er in uw werkomgeving vertrouwelijke informatie terecht gekomen bij onbevoegde personen?

102 responses



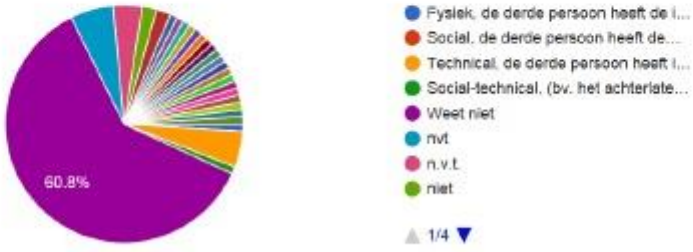
Vraag 9: Was er bij het lekken van deze informatie sprake van beïnvloeding van de medewerker door derden?

102 responses



Vraag 10: Op welke wijze is de social engineer aan de informatie gekomen?

102 responses

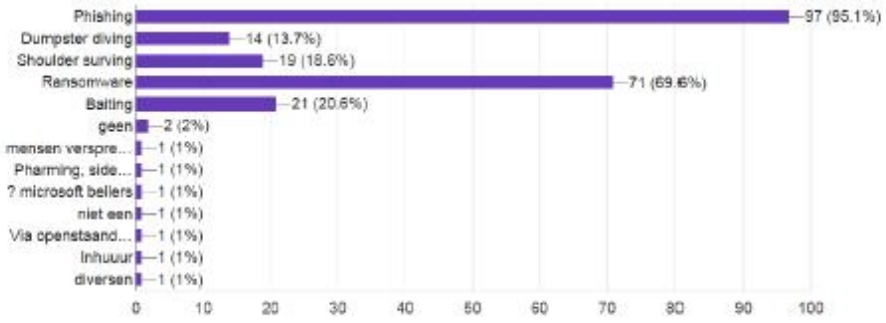


Vraag 11: Hoe wordt volgens u een social engineering aanval in gang gezet?

102 responses

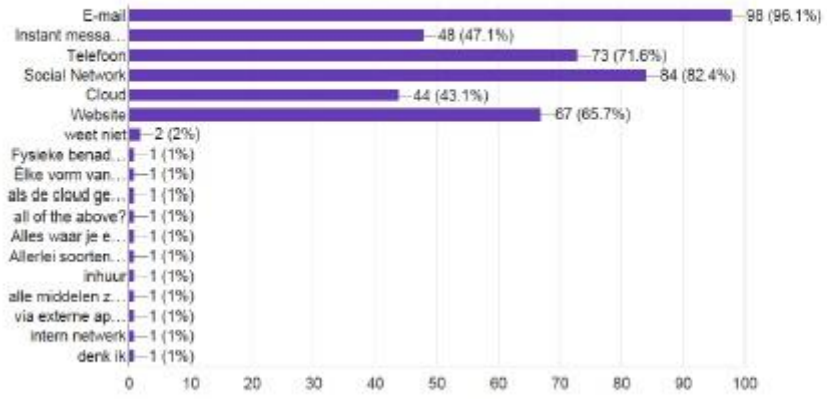
Vraag 12: Met welke van de onderstaande aanvalstechnieken bent u bekend?

102 responses



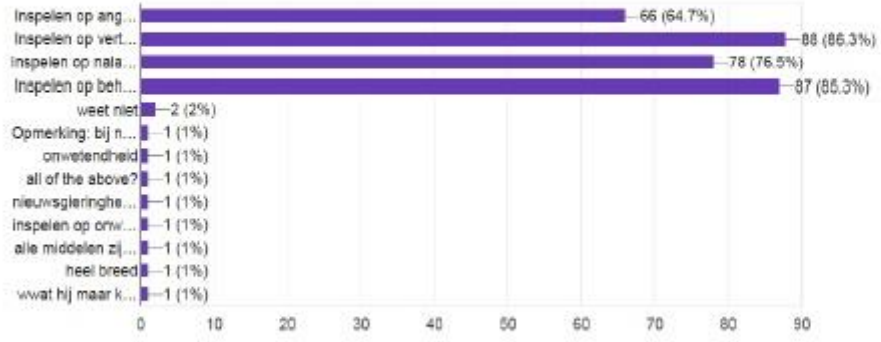
Vraag 13: Langs welke kanaal of kanalen kan een social engineer zijn aanval uitvoeren?

102 responses



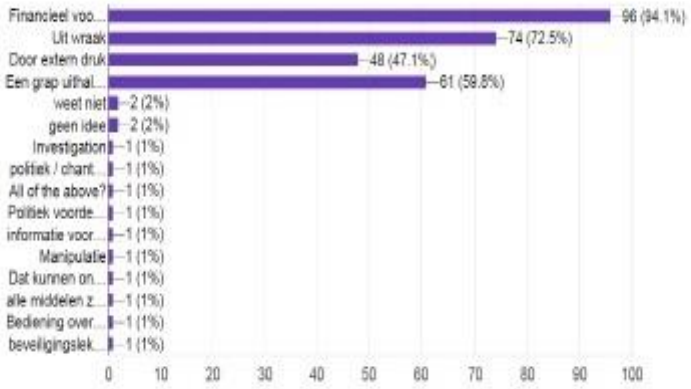
Vraag 14: Welke manipulatievormen zou een social engineer kunnen toepassen?

102 responses



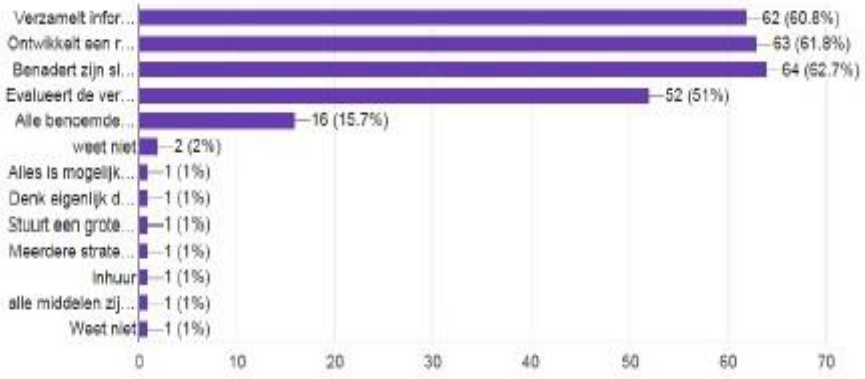
Vraag 15: Wat zouden mogelijke redenen kunnen zijn waarom een social engineer aan informatie wil komen?

102 responses



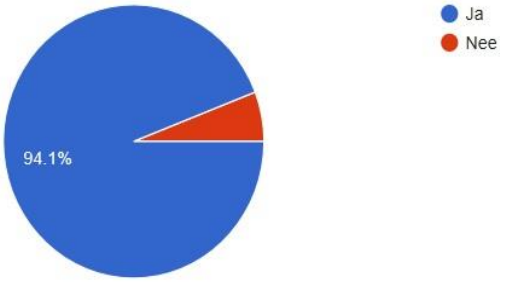
Vraag 16: Hoe gaat volgens u een social engineer te werk?

102 responses



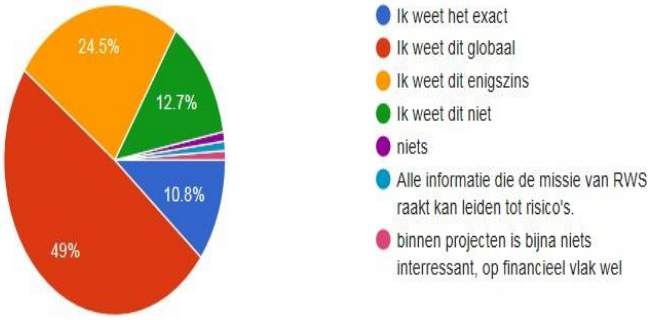
Vraag 17: Denkt u dat Rijkswaterstaat een doelwit zal zijn van een social engineering aanval?

102 responses



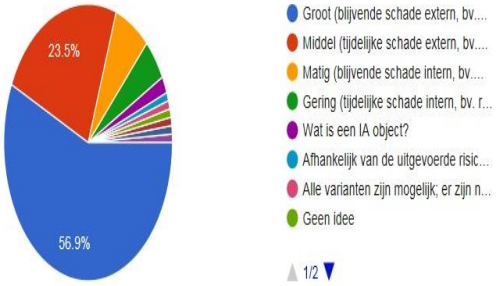
Vraag 18: Weet u welke informatie in uw werk mogelijk interessant zou kunnen zijn voor een social engineer?

102 responses



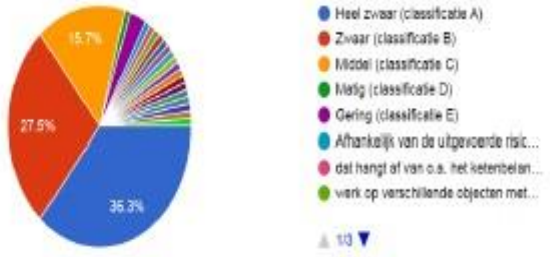
Vraag 19: Hoe groot schat u de mogelijke gevolgschade in van een IA object waarvoor of waarin u werkt als gevolg van een beveiligingsincident?

102 responses



Vraag 20: In welke mate dient volgens u het IA object waar(of waarin) u werkzaam bent, beveiligd te zijn?

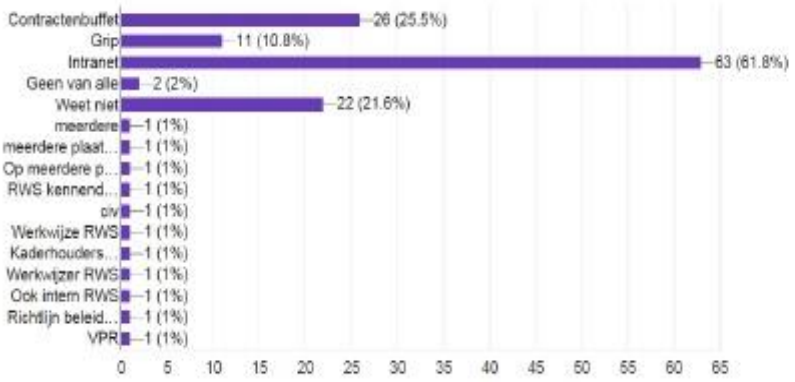
102 responses



Attitude over beveiligingsmaatregelen

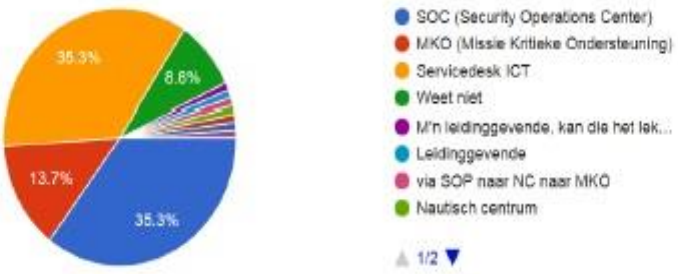
Vraag 21: Waar denkt u dat de Cybersecurity kaders en uitwerkingen terug te vinden zijn?

102 responses



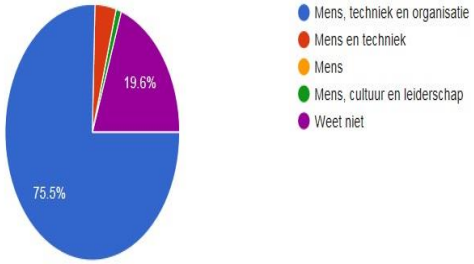
Vraag 22: Kunt u aangeven waar u de beveiligingsincident melding moet maken?

102 responses



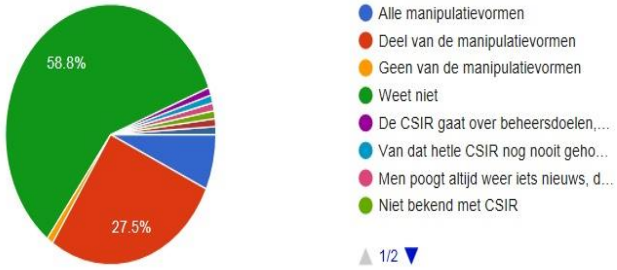
Vraag 23: Waar zijn de informatiebeveiligingsmaatregelen van RWS, zoals beschreven in Cybersecurity Implementatie Richtlijn (CSIR), op gericht?

102 responses



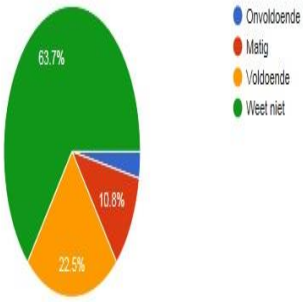
Vraag 24: Dekken de maatregelen die in de CSIR staan de gebruikte manipulatietechnieken van een social engineer?

102 responses



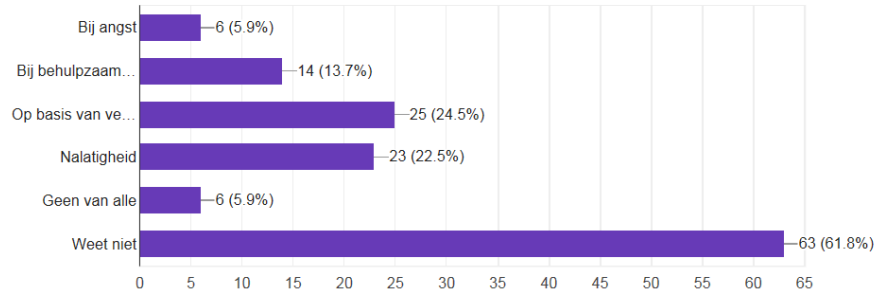
Vraag 25: In welke mate geven de beveiligingsmaatregelen handvatten hoe te handelen wanneer een social engineer u onder druk zet, om aan vertrouwelijke informatie te komen over een IA object?

102 responses



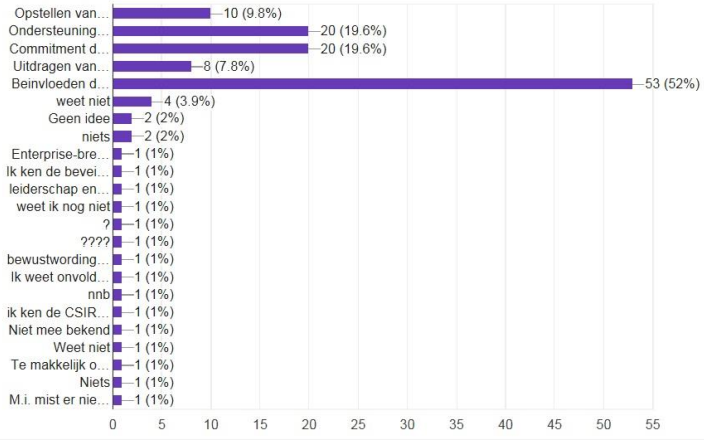
Vraag 26: Tegen welke manipulatievorm bieden de beveiligingsmaatregelen handvatten hoe te handelen?

102 responses



Vraag 27: Wat mist er volgens u in de beveiligingsmaatregelen, om uzelf te kunnen weren tegen aanvallen van de social engineer?

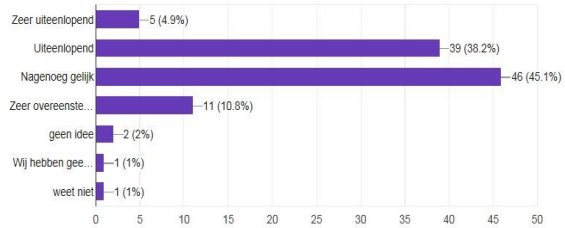
102 responses



De subjectieve norm

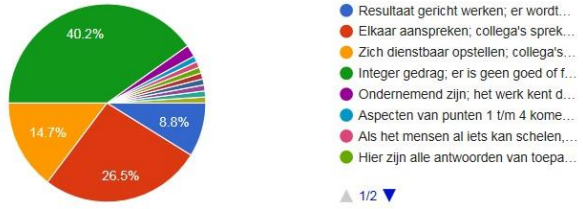
Vraag 28: Hoe verschillend zijn volgens u de meningen van uw collega's op de werkvloer over hoe omgegaan dient te worden met vertrouwelijke informatie?

102 responses



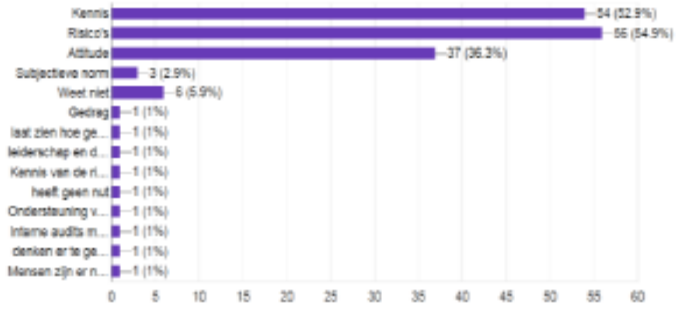
Vraag 29: Hoe zou u de manier, waarop binnen uw werkvloer wordt omgegaan met vertrouwelijke informatie beschrijven?

102 responses



Vraag 30: Waar is volgens u de meeste aandacht nodig om mensen te overtuigen om de beveiligingsmaatregelen te volgen?

102 responses



5. Conclusie, aanbevelingen, product- en procesreflectie

Tot slot worden in dit hoofdstuk de conclusies van het theoretisch (T) en Empirisch (E) deel van het onderzoek weergegeven en vervolgens worden in dit hoofdstuk aanbevelingen en met vervolg onderzoek gegeven.

5.1 Conclusies literatuurstudie

- Wat is Social Engineering? (T1)
- Welke vormen van Social Engineering kunnen we onderscheiden? (T2)

De gemeenschappelijk factor bij al deze definities van SE is dat social engineers zich op mensen, systemen of beide richten om persoonlijke of kritieke werk gerelateerde informatie te krijgen.

Uit de literatuurstudie blijkt dat de technieken van SE aanvallen kunnen variëren van zeer eenvoudig tot ingewikkeld en tevens blijkt dat de technieken van SE aanvallen onderverdeeld kunnen worden in de volgende vormen: physical, social, reverse social engineering, technical en social technical.

Verder blijkt uit de literatuurstudie dat de social engineers op zoek gaan naar de zwakste link in het netwerk waar de mens in betrokken is en daarnaast heb je verscheidene technieken wat een social engineer gebruikt om een aanval plaats te laten vinden.

De meest voorkomende techniek van SE aanval is phishing en daarnaast blijkt uit de empirische onderzoek dat er recent wereldwijd bedrijven en instellingen zijn getroffen door een nieuwe cyberaanval aanval ransomware.

Ransomware is een gijzelsoftware waarbij de toegang van de computer dan wel de bestanden op deze computer geblokkeerd worden en dus niet benaderd kunnen worden. De social engineer vraagt dan om een betaling. Deze aanval heeft ook in Nederland plaats gevonden bij de havenbedrijf van Rotterdam waarbij containerterminals zijn aangevallen.

- Hoe ziet het proces van een Social Engineer eruit? (T3)
- Welke factoren zijn van invloed op het succes van Social Engineering aanvallen? (T4)

De social engineer doorloopt een cyclus waarin hij probeert toegang tot vertrouwelijke informatie over de organisatie te krijgen volgens een bepaalde methode. Een social engineer probeert zijn aanvaller te overtuigen om hem van informatie te voorzien en speelt in op de manipulatietechnieken net zolang tot hij toegang heeft tot de vertrouwelijk informatie en de informatie toereikend is.

- Welke factoren spelen een rol bij gedragsverandering? (T5)

Op basis van gedragsliteratuur studie ben ik gekomen tot onderstaande referentiemodel zie figuur. Hieruit heb ik twee causale relaties en 1 interveniërende (modererende) relaties gevonden. De meest voorspellende factor voor gedrag blijkt de intentie te zijn. Studies tonen aan dat, als mensen de intentie hebben om iets te doen, in 75% van de gevallen het ook daadwerkelijk doen (Azjen, 1991).

In dit model zoals weergegeven zie je drie verschillende opvattingen terug, namelijk (1) dat context invloed heeft op het gedrag (behaviorism), (2) dat hoe iemand als persoon in elkaar zit bepaalt hoe hij zich gedraagt (cognitieve psychologie) en (3) dat de mate waarin de consequenties van het gedrag positief of negatief wordt beleefd, bepaalt hoe vaker of minder vaak iemand overgaat tot een bepaald gedrag.

- (1) De context is door Straathof in drie niveaus uitgewerkt.
- (2) Hoe iemand in elkaar zit, heeft te maken met de motivatie die hij heeft.
- Enerzijds wil een individu zijn behoeftes bevredigen en volgens Maslow heeft een individu ook de behoefte aan veiligheid en zekerheid. En om hieraan te voldoen, zegt de Protection Motivation Theorie dat een individu eerst de ernst van de situatie inschat en vervolgens nagaat of de maatregelen ook helpen.

- (3) Hoe iemand de consequenties van gedrag beleeft (positief of negatief) heeft volgens de motivatietheorie te maken met in welke mate iemand vindt dat hij datgene wat hij wil, ook daadwerkelijk zelfstandig kan uitvoeren. Als iemand vindt dat hij een taak niet kan uitvoeren (negatief) dan zal hij minder snel overgaan tot daadwerkelijk gedrag en omgekeerd als iemand vindt dat hij een taak wel kan uitvoeren (positief) dan zal hij sneller overgaan tot daadwerkelijk gedrag.

  De goal-theorie zegt dat iemand eerder vindt dat hij iets kan, als hij zich ook specifieke leerdoelen en performance doelen stelt. De leerdoelen gaan over het opdoen van nieuwe kennis en de performance doel gaat om de taak succesvol uit te voeren zonder fouten.

5.2 Conclusie empirische onderzoek

- Wat wordt verstaan onder IA binnen RWS? (E1)

In verschillende definities komt duidelijk naar voren dat IA bestaat uit ICT gerelateerde systemen, die verbonden zijn met de fysieke infrastructuur van RWS ten behoeve van bedienen en besturing van objecten.

De ICT onder de motorkap dient veilig, betrouwbaar en beschikbaar te zijn om veiligheid te garanderen voor de automobilist. Dit is ook van toepassing op de fysieke infrastructuur van RWS. RWS heeft zijn objecten geclusterd naar de volgende netwerken: HVWN, HWN en HWS

Een belangrijk verschil tussen kantoor en industriële automatisering is dat voor industriële automatisering zwaardere eisen gelden op het gebied van veiligheid, prestatie en betrouwbaarheid, en verwachtingen ten aanzien van autonoom besturen. Het totaal vormt samen één integraal functionerende keten met IA als verbindend element.

- Hoe ziet het informatiebeveiligingsbeleid van RWS eruit? (E2)

RWS heeft veel IA systemen die los staan van de centrale kantooromgeving. Deze systemen bieden kansen, maar betekent ook dat er aandacht moet worden besteed aan de beveiliging. Dit zijn veelal operationele systemen die een belangrijke functie vervullen. Vb. bediening, besturing van objecten. De systemen hebben een andere dreigingsbeeld en leveren andere risico´s op dan de kantooromgeving.

RWS heeft de risico´s geïnventariseerd voor de IA omgeving en de nodige maatregelen hiervoor getroffen in het beleid, deze kun je nalezen in de CSIR.
Doordat RWS een infraclassificatie voor al zijn objecten heeft vastgesteld wordt op basis van de weerstandsniveau bepaald welke specifieke maatregelen genomen dienen te worden voor een bepaald object.

Interessant is echt in het huidige informatiebeveiligingsbeleid wat RWS hanteert de CSIR wordt alleen aandacht geschonken aan de Mens, Organisatie & Procedure en Techniek. In de praktijk worden de maatregelen afgevinkt, zoals clean-desk policy, maar de vraag blijft of deze maatregelen leiden tot het gewenste ‘veilig gedrag’.

Bijvoorbeeld de groep ‘projectleden’ zetten de opgestelde beveiligingsmaatregelen 1 op 1 door naar een marktpartij die zich hieraan dient te houden, maar kan geen inhoudelijke vragen van een marktpartij over de inhoud ervan beantwoorden. Daar is tot nog de hulp nodig van experts die het document hebben opgesteld.

- Welke technieken van social engineering aanvallen komen voor bij RWS op het gebied van IA? (E3)

In 2015 heeft er een ransomware techniek van SE aanval plaats gevonden binnen RWS. Uit het jaaroverzicht 2016 CIV van cyberdreigingen blijkt dat er door gebruikers 1370 phishing mail en door de mail server 4555 virussen, malware etc. zijn tegengehouden.

- Welke maatregelen neemt RWS op het gebied van social engineering aanvallen?(E4)

Intern:

Binnen RWS zijn verschillende awareness activiteiten in relatie tot onderkende doelgroepen ondernomen. Zo zijn er maatregelen genomen voor alle beweegbare objecten van RWS in het kader van de informatiebeveiligingsbeleid CSIR. Dat zijn bijvoorbeeld risicogerichte maatregelen voor beveiliging van systemen of objecten.
Daarnaast is het van belang dat iedereen in de keten zich bewust moet zijn van veiligheid en beveiliging in onze objecten en zijn of haar rol daarin erkennen. Daarom wordt er awareness trainingen gegeven en daarnaast zijn er assetmanagement processen en cybersecurityprocessen ingericht om de IA in onze objecten goed te beheersen.

Extern:

In de contracten die RWS aangaat met marktpartijen krijgt awareness een prominente plaats in de aanbestedingscontracten. Bewustwording, opleiding en training is een beheersdoel die marktpartijen moeten invullen en onderhouden. Dit wordt ook getoetst vanuit het proces van contractbeheersing. Om hier markt breed aandacht voor de vragen staat Cybersecurity hoog op de agenda van het periodieke overleg dat RWS heeft met de branche vereniging van elektrotechnische installatiebedrijven namelijk Uneto VNI. Marktpartijen moeten investeren in awareness activiteiten om zo de weerbaarheid voor cyberdreigingen te verhogen. Marktpartijen investeren nu ook in toolbox oplossingen en E-learning modules.

- Wat voor een mening hebben medewerkers van RWS over de factoren die invloed hebben op het gedrag in een IA object (E5)?

Conclusie:

Norm: (enquêteresultaten vs. interviewresultaten)
Variabele: Mate waarin gedrag wordt beïnvloed door een specifiek context waarin een medewerker zich bevindt.

Uit de interview resultaten schijnt dat de groepsnorm, namelijk wat iemand denkt wat een ander goed of fout vindt, uiteindelijk bepaalt hoe iemand zich gedraagt. We kunnen op basis van de enquêteresultaten NIET bevestigen of de groepsnorm de dominerende factor is op basis waarvan mensen handelen.

Wat wel afzonderlijk naar voren komt, is dat meer dan de helft (56%) van de respondenten denkt dat andere collega's nagenoeg dezelfde mening hebben over wat goed of fout is als het gaat om hoe om te gaan met vertrouwelijke informatie.

Daarentegen blijkt uit de enquête resultaten op vraag hoe medewerkers hun werkvloer beschrijven hoe omgegaan wordt met vertrouwelijke informatie, dat 26,5% van de respondenten elkaar wel aanspreekt op hoe om te gaan met vertrouwelijke informatie. Dit terwijl uit de interview resultaten het vermoeden ontstaat dat mensen te aardig voor elkaar zijn op de werkvloer. De werkvloer wordt eerder geschetst als een omgeving waar ieder persoonlijke invulling geeft aan hoe om te gaan met vertrouwelijke informatie. 40,2% van de respondenten geeft aan integer te handelen; 'er is geen goed of fout, een ieder schat op basis van eigen expertise in hoe om te gaan met vertrouwelijke informatie.

Wat we ook niet kunnen vaststellen (wat wel uit interview-resultaten is gebleken) dat verschillende personen anders reageren op persoonlijke zwaktes in de mens.

Risicoperceptie: (enquêteresultaten vs. interviewresultaten)

Variabele: Mate waarin een individu de situatie als onveilig ervaart

Medewerkers van IA-objecten zien over het algemeen wel in wat de ernst is van de situatie, maar zijn niet in staat om aan te geven in welke mate zij zelf blootgesteld zijn aan het gevaar van social engineering.

Maar liefst 94% van de respondenten geeft aan dat RWS mogelijk doelwit zou kunnen zijn van een social engineer aanval. Met andere woorden net als de geïnterviewde medewerkers ziet de meerderheid wel in dat RWS informatie heeft die mogelijk interessant is voor kwaadwillenden.

En 56,9% van de respondenten geeft aan dat wanneer de informatie in handen komt van een social engineer er een blijvend schade kan optreden, bv. dodelijke ongevallen in het verkeer.

En dat dus een RWS object volgens 79,5% van de respondenten variërend van heel zwaar tot middel zwaar beveiligd dient te worden. Ook is de meerderheid bekend met zowel de technieken als de kanalen die een social engineer gebruikt om een aanval op te zetten: technieken zoals ransomware (69,6%) en phishing (95,1%); kanalen: e-mail (96,1%), social network (82,4%), telefoon (71,6%), website (65,7%), instant messaging (47,1%).

Het probleem is echter, zoals ook uit interview is gebleken, dat medewerkers deze kans van optreden niet kunnen relateren naar hun eigen praktijk. Medewerkers zijn echter niet in staat om in te schatten hoe groot de kans is dat zij zelf benaderd zouden kunnen worden door een social engineer: 57,8% van de respondenten weet niet of er in hun werk informatie is gelekt door beïnvloeding van derden. Hierbij weet 60,8% van de respondenten niet hoe een social-engineer aan informatie komt. En 73,5% van de respondenten geeft aan tussen enigszins en globaal te weten welke informatie/handelen uit hun werk mogelijk interessant zou kunnen zijn voor een social engineer. Wat we echter bij deze groep niet kunnen vaststellen hoe groot de medewerkers de gevolgschade inschatten/ervaren op basis van door hun gelekte informatie.

Wat we ook niet uit de enquête resultaten kunnen halen, is of afstand tot een object een mogelijke reden zou kunnen zijn voor het niet kunnen vertalen van het SE-gevaar naar eigen situatie. Met andere woorden we weten niet of alleen de projectleden en/of de experts degene zijn die SE in hun werk niet weten te herkennen. Deze groep werkt namelijk op afstand en kent het object minder goed zoals gebleken uit interviews.

Attitude: (enquêteresultaten vs. interviewresultaten)

Variabele: Mate waarin de individu zich positief of wel negatief opstelt ten opzichte van een maatregel.

Op basis van de enquête resultaten kunnen we niet vast te stellen of inderdaad de meerderheid afweet van het bestaan van specifieke beveiligingsmaatregelen voor IA-objecten in CSIR-document, terwijl dit wel uit de interviewresultaten het geval blijkt te zijn.

Wel geeft 58,8% van de respondenten aan niet te weten of maatregelen uit CSIR effect heeft om medewerkers te beschermen tegen gebruikte manipulatietechnieken door derde om aan informatie te komen. Dit komt overeen met de interviewresultaten, waarin de mensen wel inzien dat de technische maatregelen effect hebben, maar slechts een respondent weet aan te geven dat het maken van bv. een back-up (gedragsregel CSIR) wel effect heeft. Op een van de technieken (angst) geeft 63,7% aan niet te weten hoe te handelen als ze onder druk worden gezet.

Wat verder bevestigd lijkt te worden, is dat 52% van de respondenten aangeeft meer kennis nodig te hebben door trainingen, informatie en beoordelen van situaties om zich zelf te kunnen weren tegen aanvallen van social-engineer en de gebruikte manipulatietechnieken. Dit is complementair aan het feit dat uit de interviews blijkt dat medewerkers niet de kennis hebben om de maatregelen zelfstandig uit te voeren.

Verder is uit de enquête resultaten niet te halen, welke medewerkers in meer of mindere mate de maatregelen zelfstandig kunnen uitvoeren.

Zelf-Doeltreffendheid: (enquêteresultaten vs. interviewresultaten)
De resultaten uit interview zijn niet breed onderzocht middels enquête. Interessant is om in het vervolg te onderzoeken of de 'voorlopige' resultaten uit interview daadwerkelijk een trend is binnen de organisatie.

Vragen voor vervolgonderzoek zouden kunnen zijn:

- Wat voor doelen (performance vs. leren) hebben medewerkers voor zichzelf gedefinieerd om in te spelen op het gevaar van SE?
- Wat zijn stimulerende ofwel belemmerende factoren die medewerkers ervaren voor het bereiken van hun leerdoel?
- Wat hebben medewerkers nodig om hun werk goed uit te kunnen voeren?
- Hoe scherp hebben de medewerkers hun leerdoelen gedefinieerd?

5.3 Antwoord op de probleemstelling

De antwoorden op de deelvragen hebben geleid tot het beantwoorden van de probleemsteling. Welke factoren hebben invloed op het 'veilig' gedrag gedrag van RWS medewerkers tegen social engineering (SE) in industriële automatisering (IA) objecten van Rijkswaterstaat.

Uit meerdere onderzoek blijkt zoals in paragraaf 1: Introductie is beschreven, dat awareness programma's niet leiden tot veilig gedrag bij de mens, dat er meer nodig is dan alleen maar kennis bijspijkeren bij de mens.

Mijn hypothese uitspraak:
Kennis is niet de enigste factor waardoor medewerkers niet overgaan tot veilig gedrag, dit klopt dus. In dit onderzoek is van het gedragsmodel van informatiebeveiliging volgens Koers & Nuijten (2006) vanuit gegaan. Zij geven aan dat de volgende factoren namelijk: Kennis, Risico perceptie, attitude en subjectieve norm een rol spelen om als einddoel veilig gedrag bewerk te stellingen bij de mens.

De gedragstheorie van MacInnis, Moorman & Jaworski (1991)ontleedt gedrag in componenten. Specifieker betekent dit dat het gedrag kan worden gezien als resultaat van drie factoren: motivatie, capaciteit en gelegenheid.

5.4 Aanbevelingen

5.4.1 Praktijk

Norm:
Dit brengt ons op het advies dat wil je dat medewerkers beveiligingsmaatregelen daadwerkelijk opvolgen, dat je in ieder geval een op maat instructie dient te geven, afhankelijk van hoe een persoon in elkaar zit in combinatie met het tonen van voorbeeld gedrag als groepsnorm. Het houdt mensen namelijk wel bezig over hoe anderen denken over wat goed of fout is.

Risicoperceptie:
Op de hoogte brengen van de medewerkers hoe hun handelen kan leiden tot verlies van vertrouwelijk informatie. Dit kun je doen door de handelingen van de medewerker in relatie te brengen met de manipulatie techniek, die een social engineer toepast. Het helpt natuurlijk als de experts hierbij ook nog de volgende stap kunnen zetten.

Experts vanuit de classificatie van objecten een vertaling laten maken naar het classificeren van de verschillende soort werkzaamheden, door inzicht te geven hoe kritisch hun werk is. Dit heeft te maken met enerzijds hoe groot de kans is dat iemand hun benadert ofwel als zij hun werk niet goed doen, hoe groot de impact is. Met andere woorden hoeveel schakels zitten zij af van de vertrouwelijke informatie, waar een kwaadwillende opzoek naar is.

Attitude:
Er dient meer aandacht te komen voor het instrueren van medewerkers over wat vanuit de CSIR maatregelen qua gedragsregels van een medewerker wordt gevraagd. Dit betekent dus dat de rol en verantwoordelijkheid helder wordt gemaakt, wie staat waarvoor aan de lat. Ook is het belangrijk om bij de instructies vervolgens een op maat training te geven aan medewerkers. Medewerkers geven namelijk verschillende redenen waarom zij niet in staat zijn om een maatregel uit te voeren. De een wil meer afweten van de techniek, de ander is te gevoelig voor een bepaalde manipulatietechniek en heeft aanvullende instructies nodig hoe hiermee om te gaan.
Ook dient aandacht te worden gegeven waarom de voorgeschreven gedragsregels wel effectief zijn. De nut en noodzaak wordt op dit moment onvoldoende gezien.

Zelf-doeltreffendheid:
Wat voor doelen (performance of leren) hebben medewerkers van Rijkswaterstaat voor zichzelf om maatregelen tegen social engineering zelfstandig te kunnen uitvoeren?
En in welke mate ervaren de medewerkers dat ze in de gelegenheid worden gesteld om hun doelen te bereiken?

5.4.2 Theorie

Norm:
In dit onderzoek is gekeken naar welke soort druk een rol spelen bij het handelen van een individu wat leidt tot veilig gedrag. Echter een aanbeveling zal zijn om te kijken naar of de benoemde factoren ook onderling invloed hebben met elkaar, dit leidt vervolgens tot nieuwe inzichten en mogelijk aanknopingspunten voor de verdere literatuur.
Ook is het aan te bevelen om te onderzoeken of de persoonlijkheid van een individu verband heeft met hoe reageert op de zwaktes in de mens. Wanneer dit helder wordt, dan kan in de instructies die op maat worden gemaakt, hier rekening mee worden gehouden.

Risicoperceptie:
Onderzoeken of de mate waarin iemand ver of dichtbij het object zit, invloed heeft op de mate waarin hij het risico naar zijn eigen werk kan relateren.

Attitude:
Onderzoek naar de effectiviteit van maatregelen tegen SE-aanvallen bij meerdere organisaties, bv. Ingedeeld naar de verschillende manipulatietechnieken (bv. Phishing).

Zelf-doeltreffendheid:
Vragen voor vervolgonderzoek zouden kunnen zijn:

- Wat voor doelen (performance vs. leren) hebben medewerkers voor zichzelf gedefinieerd om in te spelen op het gevaar van SE?
- Wat zijn stimulerende ofwel belemmerende factoren die medewerkers ervaren voor het bereiken van hun leerdoel?
- Wat hebben medewerkers nodig om hun werk goed uit te kunnen voeren?
- Hoe scherp hebben de medewerkers hun leerdoelen gedefinieerd?

5.5 Productreflectie

De gehanteerde methode wat gebruikt is bij dit onderzoek was zowel kwalitatief als kwantitatief bleek een goede methode te zijn om de problematiek bij de onderzoeksgroepen te onderzoeken.

In het eerste deel van dit onderzoek zijn er doormiddel van interviews open vragen gesteld. Hiermee wordt inzichtelijk gemaakt hoe dit onderwerp leeft bij de belangrijkste spelers (medewerkers) van RWS. Dit kan worden beschouwd als een exploratief (verkennend) onderzoek waarbij op basis van een uitgebreide literatuur studie de belangrijkste aspecten van SE worden bevraagd. Het gaat hierbij om kennis, risico's, houding en de subjectieve norm. Dit geeft een globaal beeld waar binnen RWS de belangrijkste issues en uitdagingen zitten voor SE.

In de tweede stap is er gekozen voor het uitzetten van een enquête waarbij de resultaten uit de interviews (eerste stap) de richting (zwaartepunt) bepalen. Hiermee krijgen we een nog scherper beeld en meer diepgang op de hiervoor genoemde 4 aspecten. Deels 'zoomen' deze vragen verder in op aspecten die ook in de interviews aan bod zijn gekomen.

Enerzijds wordt hiermee getoetst of de beelden die uit de interviews zijn opgehaald ook kloppen, een soort herbevestiging van de opgehaalde beelden. Anderzijds wordt op sommige aspecten nog meer diepgang gezocht om nog een scherper beeld te krijgen van de meest belangrijke aspecten van SE. Met deze opzet kan een scherpe analyse worden gemaakt van de belangrijkste nalatigheden van SE binnen het bredere domein van IA binnen objecten van Rijkswaterstaat.

De enquête die ik uit heb gezet kwam eigenlijk in een ongunstige moment namelijk de vakantieperiode.Hierdoor zijn veel van de medewerkers van de onderzoeksgroepen met vakantie en een aantal vervingen iemand anders waardoor de werkdruk echt hoog was en konden hierdoor dus weinig medewerkers vanuit RWS de enquête online invullen.

5.6 Procesreflectie

Terugkijkend op het uitvoeren van onderzoek was er voor de onderzoeker in het begin onduidelijkheid over de onderzoeksthema's en de onderzoeksvragen. Daarnaast had de onderzoeker nog steeds geen goedkeuring van zijn werkgever gekregen om het onderzoek uit te voeren. De keuze van de afstudeer thema security lag in interesse gebied van de onderzoeker en daardoor wilde de onderzoeker ook niet een andere thema kiezen. Combinatie van fulltime baan en privéomstandigheden en in de avond uren het onderzoek uitvoeren bleek achteraf zwaar.

De afstudeerhandleiding heeft de onderzoeker geholpen in het proces van afstuderen om focus erin te houden welke producten in welke fase geleverd moesten worden. Gedurende de literatuurstudie is de onderzoeker erachter gekomen dat de awareness trainingen niet leiden tot veilig gedrag bij de mens en dit is ook bevestigd door de begeleider. Hierdoor heeft de onderzoeker nadere literatuur opgezocht om te achterhalen welke factoren een rol spelen bij veilig gedrag.
Tijdens het empirische deel van het onderzoek heeft de onderzoeker extra inspanning verricht bij kwalitatief onderzoek (afnemen van interviews) en kwantitatief onderzoek.

Uit de pilot interview bleek al gauw dat de tijdsbestek van 1 uur kort was voor het uitvoeren van de interviews. Hierdoor heb ik mijn definitief interview aangepast naar 1.5 uur.
Nadat ik de enquête online had gepubliceerd en de respondenten erop konden reageren kwam ik erachter, dat ik voor het onderdeel zelf doeltreffendheid niet de juiste specifieke vragen had gesteld, wat ik niet kon terug draaien. Ik heb alsnog in paragraaf 5.4.2 de juiste vragen gesteld die ik had willen vragen.

De onderzoeker heeft veel gereisd naar verschillende locaties om de onderzoeksgroepen te informeren over het onderzoek en benadrukt welke belangrijke rol zijn kunnen vervullen aan dit onderzoek. Dit heeft een positief effect gehad en ondanks de vakantieperiode hebben 102 respondenten deel genomen aan het onderzoek.

6. Referenties

6.1 Wetenschappelijke bronnen

Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. In *Action control* (pp. 11-39). Springer Berlin Heidelberg.

Ajzen, I. (1991). The theory of planned behavior. *Organizational behavior and human decision processes*, *50*(2), 179-211.

Aloul, F. (2012). The need for effective information security awareness. Journal of Advances in Information Technology, 3(3), 176-183.

Applegate, S. D. (2009). Social engineering: hacking the wetware!. Information Security Journal: A Global Perspective, 18(1), 40-46.

Bogaerts, S., & Poiesz, T. (2007). Het Triade-model. *Maatwerk, 2007*, *8*(2), 57.

Boshmaf, Y., Muslukhov, I., Beznosov, K., Ripeanu, M (2011) The socialbot network: when bots socialize for fame and money. In: Proceedings of the 2th Annual Computer Security Applications Conference.

Brody, R.G., Richard,G., Brizzee, W.B., & Cano, L. (2012). Flying under the radar: social engineering, International Journal of Accounting & Information Management, 20(4), pp. 335-347

Chitrey, A., Singh, D., & Singh, V. (2012). A comprehensive study of social engineering based attacks in India to develop a conceptual model. International Journal of Information and Network Security, 1(2), 45.

Cialdini, R. B. (2001). Science and practice.

Cialdini, R. B., Kallgren, C. A., & Reno, R. R. (1991). A focus theory of normative conduct: A theoretical refinement and reevaluation of the role of norms in human behavior. *Advances in experimental social psychology*, *24*, 201-234.

Cieslewicz, J (2004) Attacks and accidents: Policy to protect the power grid's critical computing and communication needs. Senior interdisciplinary honors thesis in international security studies, Stanford University.

Cooke, N. J., D'Amico, A., Decisions, S., Gonzalez, C., & Salas, E. (2012). PERSPECTIVES ON THE ROLE OF COGNITION IN CYBER SECURITY.

Coopers, P. (2015). Turnaround and transformation in cybersecurity: Key findings from The Global State of Information Security Survey 2016.

De Caluwé, L., & Vermaak, H. (2000). *Leren veranderen*. Kluwer

De Graaf, N. D. (2002). De verklaringskracht van cultuur

De Vries, H., Dijkstra, M., & Kuhlman, P. (1988). Self-efficacy: the third factor besides attitude and subjective norm as a predictor of behavioural intentions. *Health education research*, *3*(3), 273-282.

Dweck, C. S. (1986). Motivational processes affecting learning. *American psychologist*, *41*(10), 1040.

Eeten van, M., Roe, E., Schulman, P., andBruijne de , M (2006). The enemy within: Sys- tem complexity and organizational surprises. In M. Dunn and V. Mauer (eds.), International CIIP Handbook 2006, volume II, pages 89–110. Center for Security Studies, ETH Zurich.

Fishbein, M., & Ajzen, I. (1977). Belief, attitude, intention, and behavior: An introduction to theory and research.

Ghoshal, S., Bartlett, C. A., & Kovner, P. C. (1997). *The individualized corporation*. Harper Audio.

Goldberg, L. R. (1990). An alternative" description of personality": the big-five factor structure. *Journal of personality and social psychology*, *59*(6), 1216.

Granger, S. (2010). Social engineering fundamentals, Part I: hacker tactics (white paper): Symantec.

Greiner, L. (2008). Hacking your network's weakest link: you, netWorker, 12(1), pp. 9-11

Hasle, H., et al.,(2005) Measuring resistance to social engineering, in Information Security Practice and Experience (Lecture Notes in Computer Science 3439). In F.B. Robert H. Deng, Hwee Hwa Pang,

Jianying Zhou, Editor. 2005, Springer: Heidelberg.

Hofstee, H., Kusters,R. (2012) Afstudeertraject Introductie tot Business Process Management de cursus and IT. Heerlen: Open Universiteit

Holz, T., and Bos, H, (eds.)(2011) Detection of intrusions and malware, and vunerability assessment. Heildelberg: Springer.

Hull, C. L. (1943). Principles of behavior: An introduction to behavior theory.

Ivaturi, K. & Janczewski, L. (2011). A Taxonomy for Social Engineering attacks. CONF-IRM 2011 Proceedings. Paper 15. http://aisel.aisnet.org/confirm2011/15

Ivaturi, K., and Janczewski, L (2012) A typology of social engineering attacks – an information science perspective. Presented in Pacific Asia Conference on Information Systems (PACIS) Paper 145, van http://aisel.aisnet.org/pacis2012/145

Irani, D., Balduzzi, M., Balzarotti, D., Kirda, E., and Pu, C. (2011) Reverse social engineering attacks in online social networks. In: T. Holz., and H. Bos (eds.) Detection of intrusions and malware, and vulnerability assessement. pp.55- 74. Heidelberg: Springer.

Jagatic, T.N., Johnson, N.A., Jakobsson, M., Menczer, F., (2007). Social Phishing. Communications of the ACM. 50 (10): 94-100.

Koers & Nuijten (2006) Informatiebeveilging
https://www.deitauditor.nl/wp-content/uploads/2014/09/artikel-3-Informatiebeveiliging-%E2%80%93.pdf

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

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. Journal of Information Security and applications, 22, 113-122.

Li, H., Rosenwald, G. W., Jung, J., and Liu.C (2005) Strategic power infrastructure defense. Proceedings of the IEEE, 93(5):918–933.

Luiijf, H., and Klaver, M (2004). The current state of threats. In e-Security in Europe: Todays Status and The Next Step.

Locke, E. A. (1968). Toward a theory of task motivation and incentives. *Organizational behavior and human performance*, *3*(2), 157-189.

Maan, P. S., & Sharma, M. (2012). Social engineering: A partial technical attack. International Journal of Computer Science Issues, 9(2), 1694-0814.

Madani, V., and Novosel. D (2005) Getting a grip on the grid. IEEE Spectrum, 42(12):42– 47.
Manske, K. (2000). An introduction to social engineering. Information systems security, 9(5), 1-7.

Maslow, A. H. (1943). A theory of human motivation. *Psychological review*, *50*(4), 370.

Mataracioglu, T., Ozkan, S., and Hackney, R (2013) Towards a security lifecycle model against social engineering attacks: SLM-SEA. Presented at the Nineteenth Americas Conference on Information Systems. Chicago, Illinois, August 15-17.

McBride, M., Carter, L., & Warkentin, M. (2012). *One size doesn't fit all: cybersecurity training should be customized*. Technical report, Institute for Homeland Security Solutions, 2012.

Mitnick, K. D., & Simon, W. L. (2011). The art of deception: Controlling the human element of security. John Wiley & Sons.

Nicholson, A., Webber, S., Dyer, S., Patel, T., & Janicke, H. (2012). SCADA security in the light of Cyber-Warfare. Computers & Security, 31(4), 418-436.

Nelson, R. Methods of Hacking: Social Engineering. online, 2008.

Ogbanufe, O., & Kim, D. (2015, December). The Role of Trust and Familiarity in Click-through Intention: A Perception Transfer Theory in a Cybersecurity Context. WISP;

Peltier, T. R. (2006). Social engineering: Concepts and solutions. Information Systems Security, 15(5), 13-21.

Ponemon Institute (2016). Cost of Cyber Crime Study & the Risk of Business Innovation. Sponsored by Hewlett Packard Enterprise. Publication Data: October 2016. From https://www.ponemon.org/local/upload/file/2016%20HPE%20CCC%20GLOBAL%20REPORT%20FINAL%203.pdf

PWC (2016). Turnaround in Transformation in cybersecurity. Keyfindings from the Global State of Information Security Survey 2016.

Reardon, L. (2009). Email Statistics Report, 2009-2013. Retrieved 20 June, 2017, from http://www.radicati.com/?p=3237

Redmiles, E., Malone, A., & Mazurek, M. L. (2015). How I Learned To Be Secure: Advice Sources and Personality Factors in Cybersecurity. In *Symposium on Usable Privacy and Security Poster*.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *The journal of psychology*, *91*(1), 93-114.

Saunders, M., Lewis, P., Thornhill, A., Booij, M., & Verckens, J. P. (2011). Methoden en technieken van onderzoek (5 ed.). Amsterdam: Pearson Education Benelux BV.

Schwartz, S. H. (1977). Normative influences on altruism. *Advances in experimental social psychology*, *10*, 221-279.

Sheeran, P. (2002). Intention—behavior relations: A conceptual and empirical review. *European review of social psychology*, *12*(1), 1-36.

Spruit, M. E. (2010). Informatiebeveiliging en bewustzijn. *De IT-Auditor*, (1), 24-27.

Straathof, A., & Dijk, H. M. G. (2003). *Cultuurverandering bij de overheid: Sturen of sleuren?*. Lemma.

Sutton, S. (1998). Predicting and explaining intentions and behavior: How well are we doing?. *Journal of applied social psychology*, *28*(15), 1317-1338.

Thierry, H. (1998). Motivation and satisfaction. *PJD Drenth, Hk. Thierry, Ch. J. de Wolff (Eds.), Handbook of Work and Organizational Psychology*, *4*, 253-289.

Thornburgh, T. (2004, October). Social engineering: the dark art. In Proceedings of the 1st annual conference on Information security curriculum development (pp. 133-135). ACM.

Thorndike, E. L. (1927). The law of effect. *The American Journal of Psychology*, *39*(1/4), 212-222.

TNS, 2016 Cybersecurity awareness en skills in Nederland van https://www.alertonline.nl/media/toolkit/onderzoek/Cybersecurity-Awareness-en-Gedrag-2016.pdf
Townsend, K. (2010). The art of social engineering. Infosecurity, 7(4), 32-35.

Vance, A., Anderson, B. B., & Kirwan, C. B. (2014) Using Measures of Risk Perception to Predict Information Security Behavior: Insights from Electroencephalography (EEG).

Vernooij, P. J. (2008). *De Rabobank Groep: invloed op operationeel risico. Een analyse van determinanten van risicobewust gedrag* (Master's thesis, University of Twente).

Vroom, V. H. (1964). Work and motivation. 1964. *NY: John Wiley &sons*, *45*.

Watson, J. B. (1913). Psychology as the behaviorist views it. *Psychological review*, *20*(2), 158

Wetze, I. (2016) Voorbij Awareness. Grip op cyberveilig gedrag. Informatiebeveiliging Magazine. Hoffmann. From https://hoffmannbv.nl/var/downloads/var/mediamanager/files/uploads/VOORBIJ%20AWARENESS%20IB.pdf

Wilson, C. (2006) Terrorist capabilities for cyber-attack. In M. Dunn and V. Mauer (eds.), International CIIP Handbook, volume II, pages 69–88. Center for Security Studies, ETH Zurich, 2006.

Workman, M. (2008). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. Journal of the Association for Information Science and Technology, 59(4), 662-674.

6.2 Niet wetenschappelijke bronnen

De onderstaande documenten , internet en intranet zijn tijdens het archiefonderzoek gevonden en toegepast:

Documenten

- Architectuur voor industriële automatisering bij Rijkswaterstaat 0.99 / 10 februari 2011
- Baseline Informatiebeveiliging Rijksdienst (BIR) 1.0 / 01 december 2012
- Baseline Informatiebeveiliging Rijkswaterstaat (BIR RWS) 1.1/ 11 november 2013
- Bestuurbesluit Beveiligde Werken, Beveiligde Infrastructuur, 2003
- *CIV Jaaroverzicht 2016*
- Cybersecurity Implementatierichtlijn Objecten RWS (CSIR) 1.01 / 02 december 2013
- Cybersecurity voor KerenBeheren ISAC (powerpoint presentatie)
- Handreiking industriële automatisering Juni 2016
- Inleiding EAR Architectuur Industriële automatisering RWS 0.1 / 7 juli 2011
- Leidraad SE versie 3.0 (19 november 2013)
- Procesbeschrijving SE versie 2.1.2 (25 januari 2017)
- Response-Ability RWS-Strategie 2014 Digitale Beveiliging voor RWS infrastructuur
- Security by Design IA PowerPointpresentatie
- Speerpuntenbrief RWS 2018

Internet & Intranet

- Basisprincipes van gedragstheorien
  http://nl.viva-read.com/article/wat-zijn-de-basisprincipes-van-de-gedrags-theorien
- Cyberweerbaarheid blijft achter digitale dreigingen (internet)
  http://www.nu.nl/internet/4783344/nederlandse-cyberweerbaarheid-blijft-achter-bij-digitale-dreigingen.html
- Gedrags theorieën
  http://www.wikisailor.com/soorten-gedrags-theorieen.html
- Handreikingen voor de beheersing van industriële automatisering (intranet)
  http://corporate.intranet.rws.nl/projecten/data_en_ict/impakt_beveiligd_werken/2016.05.23/handreikingen.htm
- Henry, A. (2014). Why Social Engineering Should be Your Biggest Security Concern. Life hacker. Retrieved 20, june, 2017 van http://lifehacker.com/why-social-engineering- should-be-your-biggest-security-1630321227
- Hoeffnagel, W. (2015). Cybercrimebende opgerold die Europese bedrijven voor miljoenen euro's heeft opgelicht. Geraadpleegd op 4 juli 2015, van http://executive-

people.nl/530421/cybercrimebende-opgerold-die-europese-bedrijven-voor-miljoenen-euroa-s-heeft-opgelicht.html.

- Eenvandaag bericht security-incident Gemeente Veere (internet) http://20jaareenvandaag.eenvandaag.nl/hoogtepunten/39770/sluizen_gemalen_en_bruggen_slecht_beveiligd

- Impakt (intranet) http://corporate.intranet.rws.nl/projecten/data_en_ict/impakt_beveiligd_werken/

- Impakt (intranet) http://corporate.intranet.rws.nl/projecten/data_en_ict/impakt_beveiligd_werken/

- McAfee (juni 2014) Net Losses: Estimating the Global. Cost of Cybercrime. Economic impact of cybercrime II. Center for Strategic and International Studies. van https://www.mcafee.com/de/resources/reports/rp-economic-impact-cybercrime2.pdf

- NCSC (2016). Cybersecuritybeeld Nederland. Nationaal Cyber Security Centrum. Nationaal Coordinator Terrorismebestrijding en Veiligheid. from https://www.nctv.nl/binaries/CSBN%206-2016_tcm31-95298.pdf

- Nu.nl bericht oprollen cybercrime bende door Europol (internet) http://www.nu.nl/internet/4075471/europol-rolt-oekrainse-banktrojan-bende.html

- Phishing mail (intranet) http://corporate.intranet.rws.nl/actueel/nieuws/nieuws_centrale_informatievoorziening/2017.04.24/aandacht_voor_cyberveiligheid_door_phishingcampagne.htm

- Ransomware besmetting: (internet) https://www.security.nl/posting/422575/Ransomware+infecteert+computers+Rijkswaterstaat

- Ransomware besmetting (Internet) https://www.safeweb.nl/anti-hacking/ransomware-infecteert-computers-rijkswaterstaat/9__322.php

- Stasiukonis S. (2006), Social Engineering, the USB way¸Dark Reading Online Magazine, Retrieved 20 June 2017 van http://www.darkreading.com/document.asp?doc_id=95556

Bijlagen:

Bijlage 1: Mail interview

Beste Allen,
Ik zal me eerst kort introduceren:
Ik ben Mustafa Nizami en ben bezig met mijn afstudeeronderzoek ter afronding van de Masterstudie BPMIT. Ik ben daarnaast werkzaam bij de PPO van Rijkswaterstaat als Technische Adviseur IA. Mijn afstudeeronderzoek richt zich op het vraagstuk: Welke factoren leiden tot veilig gedrag bij medewerkers van RWS om zich te kunnen weren tegen Social engineering aanvallen gericht op de medewerkers, die werkzaam zijn in industriële automatisering objecten? en voer ik dit uit voor Rijkswaterstaat
Ik ben momenteel bezig met een literatuuronderzoek en documentenreview om zoveel mogelijk relevante informatie te vergaren over het onderwerp. Vanuit het literatuuronderzoek zal ik vanuit de theorie een eerste beeld kunnen vormen van het onderwerp. Uit het lopende literatuuronderzoek zullen ook nog een hoop vragen komen. Doormiddel van het houden van interviews wil ik mijn bevindingen uit het literatuuronderzoek toetsen aan de praktijk en wil ik daarnaast nog meer relevante informatie verzamelen over het onderwerp.
ik zou graag met jou in gesprek willen gaan over het onderwerp “Social engineering binnen Rijkswaterstaat” en een interview met je willen afnemen.
Aanpak interview:
1) Het interview wordt waar mogelijk gepland in de 2de/3de week van juni, de inschatting is dat het interview maximaal 1,5 uur zal duren.
2) Minimaal 3 dagen voor het interview ontvang je van mij ter voorbereiding de lijst met interviewvragen per mail.
3) Het interview zal worden opgenomen om de informatie later te kunnen verwerken. (Met opgenomen data zal vertrouwelijk worden omgegaan de data wordt anoniem verwerkt en zal door andere niet op personen herleidbaar zijn.) Als je hier bezwaar tegen hebt hoor ik dat graag.
4) Na het interview zal de verzamelde informatie verwerkt worden en zal dit ter controle aan je worden voorgelegd.
Graag verneem ik van je of je je medewerking wil verlenen aan mijn afstudeeronderzoek. Als je ermee instemt ontvang ik graag jou mogelijkheden om het interview te houden in de 2de of 3de week van juni.
Ik verneem graag uiterlijk 6 juni een reactie van je als dat mogelijk is, alvast bedankt.
Met vriendelijke groet,
Mustafa Nizami

Bijlage 2: Interview vragen

Interview-vragen over de factoren die invloed hebben op het gedrag van een medewerker bij het veilig werken in de op afstand te bedienen objecten van Rijkswaterstaat

Inleiding [15 minuten]

Naar aanleiding van een gebeurtenis in februari 2012 in de gemeente Veere, waarbij een hacker een pomp uitschakelde waardoor rioolwater niet afgevoerd kon worden, en de in 2011 al door de Algemene Rekenkamer (ARK) geconstateerde onvolkomenheid of “rode kaart” op informatiebeveiliging bij RWS, heeft de tweede kamer haar zorgen geuit over de digitale beveiliging van RWS systemen die op afstand worden bediend.
Als reactie hierop heeft RWS, via het programma IMPAKT waarin ik ook werkzaam ben als coördinerende adviseur vanuit WNN (Tunnels), o.a. gekeken naar wat er nodig is in 460 van RWS objecten om deze te beveiligen tegen hacken van de infrastructuur en lekken van vertrouwelijke informatie. Dit door mensen bv. bewust en alert te maken van het belang van een adequate informatiebeveiliging, zoals training modules en het vastleggen en communiceren van beveiligingsincidenten.
De kern van het probleem is dat we niet weten of we met de set aan maatregelen ook het gewenste ‘veilig’ gedrag bij de medewerkers bereiken. Ik doe daarom onderzoek naar een betere beheersing van hieraan gerelateerde risico van onveilig gedrag:

> *“het lekken van vertrouwelijke informatie door medewerkers van Rijkswaterstaat aan zogenaamde ‘social’ hackers (onveilig gedrag)”*

Een social-hacker, ook wel social-engineer genoemd, gebruikt sociale vaardigheden (manipulatie en emotie) om mensen over te halen vertrouwelijke informatie prijs te geven, zodat hij of zij bij de informatie(bron) kan komen. Een belangrijk emotie die veelvuldig wordt gebruikt is het scheppen van vertrouwen bij mensen, waarvan ze informatie willen verkrijgen.
De vraag die in dit interview daarom centraal staat is wat de huidige situatie is van factoren die invloed hebben op het gedrag (veilig/onveilig) van de medewerker In mijn onderzoek interview ik de volgende personen: objectbeheerders, bedienaars, projectleden(ipm team), experts (security).
De antwoorden uit de interviews geven aan wat het probleem is, door vast te stellen of het onkunde is, gebrek aan kennis, een attitude probleem of het ontbreken van een groepsnorm. De uitkomst van de antwoorden leidt tot een probleemdefinitie, en een startpunt van een opmaat pakket van mogelijke maatregelen. Het dient als toetssteen om te bepalen in welke mate de huidige set aan maatregelen leiden tot gewenste gedragsverandering. De bevindingen daaruit leg ik u binnenkort voor in de vorm van een enquête met de vraag uw mening hierover te vormen.

De opzet van dit interview is als volgt: eerst volgen enkele algemene vragen over uw functie en de mate waarin u in uw werk omgaat met beveiligingsrichtlijnen, daarna vragen we over uw kennis van social-engineering aanvallen, vervolgens vragen we over uw perceptie bij de kans en mogelijke gevolgen van een dergelijk aanval, aansluitend vragen we over uw houding over de getroffen maatregelen door RWS en het effect daarvan en afsluitend enkele vragen over de mate waarin in uw werkomgeving elkaar aanspreken op veilig gedrag.
We hebben 120 minuten de tijd, waarvan we de eerste 20 minuten besteden aan uitleg en enkele algemene vragen over uw werk. Daarna besteden we 20 min. per onderdeel. In totaal voor 5 onderdelen (kennis en risico-perceptie over social-engineering, invulling van maatregelen en attitude hiertegenover en als laatste groepsnorm) komen we op 100 min. Per onderdeel geef ik eerst een toelichting bij de vragen en terwijl u antwoord geeft maak ik notities van de antwoorden om deze later uit te werken.
Voordat we beginnen, wil ik u vragen of u bezwaar heeft als ik het gesprek opneem? De opname helpt mij bij het uitwerken van het interview en zal dit ook uitsluitend hiervoor gebruiken en daarna verwijderen.

Vragen

A) Algemeen [5 minuten]

1. Kunt u uw functie in het kort omschrijving (afdeling, werkzaamheden, aantal jaren in dienst)?
2. Worden medewerkers gescreend voordat deze aangenomen worden. Zo ja, op welke zaken? Heeft u toegang tot vertrouwelijke informatie tijdens het uitvoeren van uw functie? Zo ja, kunt u dan omschrijving om wat voor informatie het dan gaat?

B) Kennis over social-engineering [20 minuten]

Toelichting bij de vragen
Social-engineers hebben als doel om onder valse intenties geheime of vertrouwelijke informatie te verkrijgen om deze voor eigen gewin te misbruiken. Het feit dat social-engineers het lukt om aan deze informatie te komen, komt omdat de mens de zwakste schakel is. Social-engineers spelen in op deze zwaktes om mensen te overtuigen en te beïnvloeden en om zo uiteindelijk toegang te krijgen tot informatie.

In beginsel wil de mens namelijk aardig gevonden worden, en heeft hij ontzag voor autoriteit. Bovendien is hij gevoelig voor complimenten en weet niet altijd welke informatie vertrouwelijk is.

3. Heeft u of in u directe omgeving te maken gehad met informatie die gestolen is als gevolg van social engineering, zo ja zou u nader kunnen beschrijven welke informatie dit dat betrof en via welk kanaal bv. Email, telefoon, sociaal netwerk, website etc.?

4. Zou u per zwakte aspect/manipulatietechniek aan kunnen geven of u dit herkent, en zo ja nader willen toelichten hoe de inzet van deze techniek kan leiden tot het prijs geven van informatie door een medewerker (onder kopje SE-risico?

Nr.	Zwakte van de mens	Kennis (ja/nee)	SE-risico
1.	De angst om in problemen te komen: tegenwoordig zetten de aanvallers (social engineer) mensen onder druk om bepaalde handelingen te verrichten met als doel het verkrijgen van bepaalde informatie.		
2.	Behulpzaamheid: Social engineer doet zich voor als klant op basis van het principe 'klant de koning' worden medewerkers getraind om klanten te helpen met hun klantbehoefte. Dit kan soms leiden tot het vrijgeven van meer informatie aan klanten (social engineer) dan nodig is.		
3.	De neiging om mensen te vertrouwen: het zit in de menselijke natuur om mensen te vertrouwen tot het tegendeel bewezen is hier maakt de social engineer gebruik van.		
4.	Nalatigheid: dit treed op als we onze wachtwoorden op het bureau achterlaten of materialen achterlaten welke vertrouwelijke informatie bevatten, hierdoor kan de social engineer eenvoudig aan vertrouwelijk		

Nr.	Zwakte van de mens	Kennis (ja/nee)	SE-risico
	informatie komen.		

5. Op welke wijze worden de medewerkers van RWS getraind of opgeleid om het bewustzijn ten aanzien van manipulatie te vergroten?

6. Social engineers gebruiken hiervoor genoemde manipulatietechnieken of een combinatie ervan om aanvallen op te zetten. Welke van de technieken van Social Engineering aanvallen uit het schema in bijlage A herkent u, en zou u dit nader kunnen beschrijven?

C) Risicoperceptie over social engineering [20 minuten]

Toelichting bij de vragen
"De risicoperceptie die een individu ervaart ten aanzien van informatieverlies of -schade; risicoperceptie is te meten en is bijvoorbeeld te beïnvloeden door middel het verschaffen van risico-informatie".[6]

1. Hoe groot schat u het dreigingsprofiel in van desbetreffende object waarvoor u werkzaam bent? M.a.w. hoe aantrekkelijk is de vertrouwelijke informatie over dit object voor een social engineer en kunt u dit nader toelichten?

2. Wat zouden mogelijke gevolgen of schade kunnen zijn, mocht een social engineer toegang krijgen tot geheime of vertrouwelijke informatie over de objecten, zou je hier een voorbeeld van kunnen geven?

3. Zou u op basis van de technieken van SE aanvallen in bijlage B kunnen aangeven welke van deze vanuit u werk van toepassing kunnen zijn, en zo ja zou u kunnen aangeven hoe groot de kans hierop acht en wat voor schade de aanval zou kunnen aanrichten?

D) Invulling van beveiligingsmaatregelen [20 minuten]

Toelichting bij de vragen
RWS wil voor nu en in de toekomst de beveiliging en veilige werking van haar bedienbare objecten, zoals keringen, sluizen, verkeerscentrales en tunnels op orde hebben. Het mag duidelijk zijn dat het zorgvuldig en veilig omgaan met de objectgegevens cruciaal is voor Rijkswaterstaat.
Een organisatie kan op vijf verschillende wijze interveniëren met als doel veilig gedrag: (1) het opzetten van een formele organisatie, denk aan maatregelen als gedragscode, functiescheiding, beleid, standaarden, instructies et cetera; (2) het tonen van leiderschap, denk aan voorbeeldgedrag, overdragen van kennis, belonen, sanctioneren en toezicht; (3) bevorderen van passende cultuur, denk aan visuele uitwerking in symbolen, helden, rituelen en waarden; (4) mensen diepgaand begrip te geven, denk aan bv. trainingen in de vorm van bijvoorbeeld workshops en (5) middelen beschikbaar stellen, dit zijn alle technologische voorzieningen of andere middelen bedoeld die ingezet kunnen worden.
RWS heeft 10-maatregelenpakket in het document Cybersecurity Implementatie Richtlijn voor objecten opgesteld. In dit onderdeel willen we achter komen welke van die maatregelen van toepassing zijn op uw werk en hoe u hier invulling aan geeft.

1. Kunt u een beschrijving geven van de taken en verantwoordelijkheden die u bekleedt en voor welke objecten deze werkzaamheden bestemd zijn?

[6] Koers & Nuijten (2006)

2. Ben je bekend met Cybersecurity Implementatie Richtlijn? Zo ja kunt u hieronder per maatregel uit Cybersecurity Implementatie Richtlijn (CSIR) aangegeven of deze van toepassing is op uw werk, en zo ja aangeven hoe u hier invulling aan geeft?

Nr	Maatregel uit richtlijn	Van toepassing (ja/nee/weet niet)	Invulling door de medewerker
1	Fysieke toegang (toegang tot object)		
2	Logische toegang (toegang tot IA systemen)		
3	Beveiligingsincidenten en incident Response Plan (registreren en rapporteren van incidenten)		
4	Netwerkkoppelingen (rechtstreekse toegang tot ICS/SCADA systemen is verboden)		
5	Bescherming tegen malware, hardening en patching (procedure voor detectie en preventie)		
6	Logging en Monitoring		
7	Bewustwording en Training		
8	Gecontroleerd wijzigen		
9	Beheer en onderhoud		
10	Back-ups		

3. Bovengenoemde lijst aan maatregelen zijn interventies in het domein: organisatie, mensen en middelen. Zijn er naast deze ook aanvullende maatregelen op het gebied van cultuur en leiderschap?

E) Attitude over beveiligingsmaatregelen [20 minuten]

Toelichting bij de vragen
Met attitude omschrijven we als het gevoel van iemand, negatief of positief, bij het verrichten van een bepaald gedrag. In dit geval gaat het om het uitvoeren van de beveiligingsmaatregelen. Plausibel is, dat iemand die een negatieve attitude ten opzichte van beveiliging erop nahoudt, zeker niet bereid is een inspanning te leveren voor veilig gedrag. Plausibel is ook, dat als iemand eerder last ondervindt van bepaalde veiligheidsmaatregelen, hij of zij een negatieve attitude vormt.

1. Hoe waardeert u de getroffen 10-maatregelenpakket vanuit cybersecurity implementatie richtlijnen document en dan ook specifiek de maatregelen gericht tegen SE-aanvallen, staat u eerder positief of negatief ten opzichte van de beveiliging erop na en waarom?

2. In welke mate dragen de beveiligingsmaatregelen positief dan wel negatief bij in het dagelijkse werk wat u doet en waarom? Ondervindt u eerder last van de maatregelen, of helpt het uw werk beter uit te voeren en waarom?

F) De subjectieve norm [20 minuten]

Toelichting bij vragen
RWS organisatie heeft enkele kernbegrippen, waarmee ze de organisatie identificeert. Dat is het acroniem: RADIO-V; R= resultaatgericht, A=aanspreekbaar, D=dienstbaar, I=Integer, O=organisatiesensitief en V=verbindend. Dit is natuurlijk van bovenaf geprojecteerd als een norm van hoe we zouden moeten zijn. Waar het hier om gaat is om bottum-up te achterhalen, wat een individu als een norm(en) ervaart in zijn dagelijks werk, een set van ongeschreven regels. Deze subjectieve norm van een individu ontstaat door hoe hij of zij denkt dat de directe omgeving bepaald gedrag waardeert of niet waardeert:

1. Welke gedrag wordt volgens u door u collega's wel of niet toelaatbaar geacht in uw werk als het gaat over het voorkomen van lekken van vertrouwelijke informatie? Op welk gedrag zou u denkt u aangesproken kunnen worden? Heeft dit zich in het verleden bij u of in u directe omgeving voorgedaan, zo ja zou u hier een voorbeeld van kunnen geven?

2. In welke mate voelt u geroepen om hieraan te houden en waarom?

3. In welke mate ervaart u dat deze ongeschreven regels aan het veranderen zijn, zoals bv. door komst van nieuwe personeel of het werken op verschillende locaties?

Bijlage A:

Technieken van Social engineering aanval	Beschrijving aanval
Dumpster diving	
Shoulder surfing	
Baiting	
Reverse social Engineering	
Ransomware	
Waterholing	
Prextexting	
Phishing	
Advanced persistent threat	
Spear phishing	
Impersonatie	
Identity theft	

Bijlage B:

Technieken van Social engineering aanval	Van toepassing Ja/Nee/Weet niet	Aangerichte schade
Dumpster diving		
Shoulder surfing		
Baiting		
Reverse social Engineering		
Ransomware		
Waterholing		
Prextexting		
Phishing		
Advanced persistent threat		
Spear phishing		
Impersonatie		
Identity theft		

Hartelijk dank voor het tijd en het beantwoorden van de vragen!

Bijlage 3: Enquête vragen

Enquête

Welkom bij deze enquête over cybersecurity. Deze enquête maakt deel uit van mijn onderzoek. Graag wil ik u uitnodigen om deze enquête in te vullen. De enquête duurt 20 minuten en de antwoorden worden geanonimiseerd verwerkt in het onderzoek.
Door uw deelname hoop ik een breed scala van feiten en ervaringen te verzamelen. Ik wil u erop wijzen dat alle antwoorden strikt vertrouwelijk worden behandeld door mij als onderzoeker.

De enquête gaat over welk beeld medewerkers hebben over informatiebeveiliging tegen cybersecurity aanvallen, waarbij kwaadwillenden via medewerkers van Rijkswaterstaat toegang willen krijgen tot vertrouwelijke informatie. De technieken en methodes die daarbij worden gebruikt, worden ook wel social engineering genoemd.

De enquête begint met algemene vragen over de medewerker, vervolgens worden er vragen gesteld over:

1. De kennis van de medewerker op het gebied van informatiebeveiliging
2. De risicoperceptie die de medewerker ervaart ten aanzien van informatieverlies of schade
3. De attitude/houding van de medewerker waarmee hij of zij beveiligingszaken waardeert of niet
4. De subjectieve norm van de medewerker die ontstaat door hoe hij of zij denkt dat de directe omgeving bepaald gedrag waardeert of niet waardeert.

Toelichting enquête antwoorden:

Rondje = één antwoord mogelijk

Vierkant = meerdere antwoorden mogelijk

Other = Iets anders namelijk

Mij dank is groot voor uw deelname.

Mochten er nog vragen zijn, neem dan gerust contact met mij op:
Mustafa Nizami
06xxxx
mustafa.nizami@rws.nl

Algemene informatie

Vraag 1: Wat is uw leeftijd?
Vraag 2: Wat is uw geslacht?
- Man
- Vrouw
-

Vraag 3: Wat is uw hoogst genoten opleiding?
- MBO
- HBO
- Universiteit
- Other …

Vraag 4: Onder welk organisatie onderdeel valt u?
- PPO
- CIV
- VWM
- Regio
- Other ...

Vraag 5: Onder welke categorie valt uw functie?
- Projectleden (adviseurs, ipm rolhouder)
- Experts (security)
- Objectbeheerders
- Bedienaars
- Other ...

Vraag 6: Hoeveel jaar bent u in dienst bij Rijkswaterstaat?
- 5 jaar
- 5 - 10 jaar
- 10 - 15 jaar
- > 15 jaar

Vraag 7: Bent u een interne medewerker of externe medewerker?
- Intern
- Extern

Kennis over social engineering
Een social-hacker, ook wel social engineer genoemd, gebruikt sociale vaardigheden (manipulatie en emotie) om mensen over te halen vertrouwelijke informatie prijs te geven, zodat hij of zij bij de informatie(bron) kan komen. Een belangrijke emotie die veelvuldig wordt gebruikt is het scheppen van vertrouwen bij mensen, waar ze informatie van willen verkrijgen.
Vraag 8: Is er in uw werkomgeving vertrouwelijke informatie terecht gekomen bij onbevoegde personen?

- Regelmatig
- Geregeld
- Incidenteel
- Nooit
- Weet niet

Vraag 9: Was er bij het lekken van deze informatie sprake van beïnvloeding van de medewerker door derden?

- Ja
- Nee
- Weet niet

Vraag 10: Op welke wijze is de social engineer aan de informatie gekomen?

- Fysiek, de derde persoon heeft de informatie zelf gevonden (bv. uit afvalbak)
- Social, de derde persoon heeft de medewerker gemanipuleerd om informatie vrij te geven
- Technical, de derde persoon heeft informatie via inzet van een techniek gevonden (vaak online)
- Social-technical, (bv. het achterlaten van een usb-stick, waarop een virus is geïnstalleerd)
- Weet niet
- Other …

Vraag 11: Hoe wordt volgens u een social engineering aanval in gang gezet?

- Door een persoon
- Door een software (geautomatiseerde) aanval
- Door een van beide (persoon of software)
- Other,..

Vraag 12: Met welke van de onderstaande aanvalstechnieken bent u bekend?

- Phishing
- Dumpster diving
- Shoulder surving
- Ransomware
- Baiting
- Other ...

Vraag 13: Langs welk kanaal of welke kanalen kan een social engineer zijn aanval uitvoeren?

- E-mail
- Instant messaging
- Telefoon
- Social Network
- Cloud
- Website
- Other ...

Vraag 14: Welke manipulatievormen zou een social engineer kunnen toepassen?

- Inspelen op angst van de mens
- Inspelen op vertrouwen van de mens

- Inspelen op nalatigheid van de mens
- Inspelen op behulpzaamheid van de mens
- Other ….

Vraag 15: Wat zouden mogelijke redenen kunnen zijn waarom een social engineer aan informatie wil komen?

- Financieel voordeel
- Uit wraak
- Door extern druk
- Een grap uithalen
- Other….

Vraag 16: Hoe gaat volgens u een social engineer te werk?

- Verzamelt informatie over zijn slachtoffer
- Ontwikkelt een relatie met zijn slachtoffer
- Benadert zijn slachtoffer
- Evalueert de verkregen informatie
- Other….

Risico perceptie over social engineering

Vraag 17: Denkt u dat Rijkswaterstaat een doelwit zal zijn van een social engineering aanval?

- Ja
- Nee

Vraag 18: Weet u welke informatie in uw werk mogelijk interessant zou kunnen zijn voor een social engineer?

- Ik weet het exact
- Ik weet dit globaal
- Ik weet dit enigszins
- Ik weet dit niet
- Other …

Vraag 19: Hoe groot schat u de mogelijke gevolgschade in van een IA object waarvoor of waarin u werkt als gevolg van een beveiligingsincident?

- Groot (blijvende schade extern, bv. imagoschade, veiligheid)
- Middel (tijdelijke schade extern, bv. overlast gebruiker)
- Matig (blijvende schade intern, bv. opzetten nieuw programma)
- Gering (tijdelijke schade intern, bv. repareren van schade)
- Other …

Vraag 20: In welke mate dient volgens u het IA object waar (of waarin) u werkzaam bent, beveiligd te zijn?

- Heel zwaar (classificatie A)
- Zwaar (classificatie B)
- Middel ((classificatie C)
- Matig ((classificatie D)
- Gering ((classificatie E)
- Other

Attitude over beveiligingsmaatregelen

Vraag 21: Waar denkt u dat de Cybersecurity kaders en uitwerkingen terug te vinden zijn?

- Contractenbuffet
- Grip
- Intranet
- Geen van alle
- Weet niet
- Other …

Vraag 22: Kunt u aangeven waar u de beveiligingsincident melding moet maken?

- SOC (Security Operation Center)
- MKO (Missie Kritieke Ondersteuning)
- Servicedesk ICT
- Weet niet
- Other …

Vraag 23: Waar zijn de informatiebeveiligingsmaatregelen van RWS, zoals beschreven in Cybersecurity Implementatie Richtlijn (CSIR), op gericht?

- Mens, techniek en organisatie
- Mens en techniek
- Mens
- Mens, cultuur en leiderschap
- Weet niet
-

Vraag 24: Dekken de maatregelen die in de CSIR staan de gebruikte manipulatietechnieken van een social engineer?

- Alle manipulatievormen
- Deel van de manipulatievormen
- Geen van de manipulatievormen

- Weet niet
- Other…

Vraag 25: In welke mate geven de beveiligingsmaatregelen handvatten hoe te handelen wanneer een social engineer u onder druk zet, om aan vertrouwelijke informatie te komen?

- Onvoldoende
- Matig
- Voldoende
- Weet niet

Vraag 26: Tegen welke manipulatievorm bieden de beveiligingsmaatregelen handvatten hoe te handelen?

- Bij angst
- Bij behulpzaamheid
- Op basis van vertrouwen
- Nalatigheid
- Geen van alle
- Weet niet

Vraag 27: Wat mist er volgens u in de beveiligingsmaatregelen, om uzelf te kunnen weren tegen aanvallen van de social engineer?

- Opstellen van beleid, organisatiestructuur, procedures, maatregelen, etc.
- Ondersteuning door inzet van technologie, fysieke middelen, kantoormiddelen
- Commitment door voorbeeldgedrag, toezicht, belonen, sancties
- Uitdragen van normen, rituelen, helden, symbolen
- Beinvloeden (door training, informatie, beoordelen)
- Other….

De subjectieve norm

Vraag 28: Hoe verschillend zijn volgens u de meningen van uw collega's op de werkvloer over hoe omgegaan dient te worden met vertrouwelijke informatie?

- Zeer uiteenlopend
- Uiteenlopend
- Nagenoeg gelijk
- Zeer overeenstemmend

- Other …

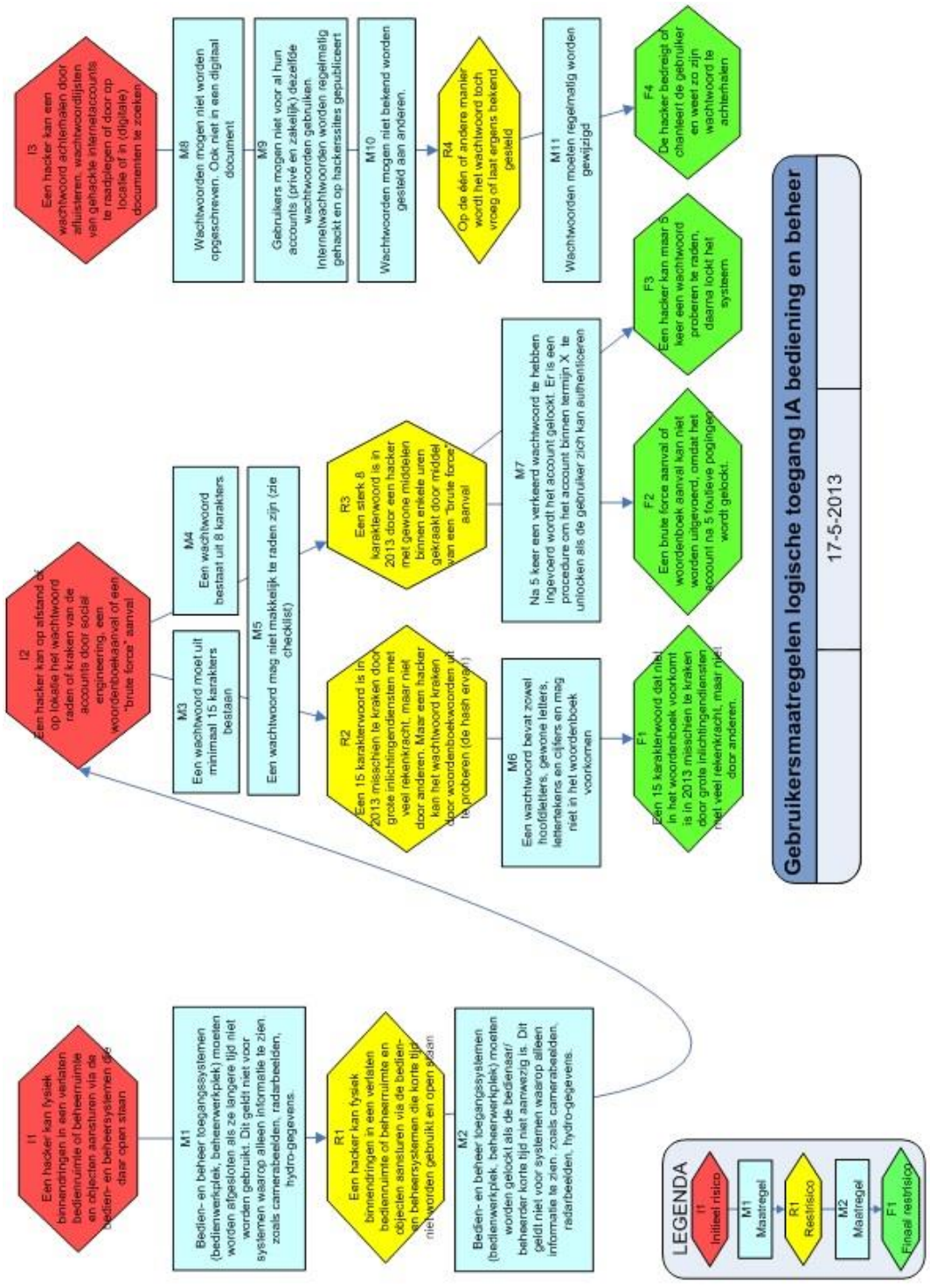
Vraag 29: Hoe zou u de manier, waarop binnen uw werkvloer wordt omgegaan met vertrouwelijke informatie, beschrijven?

- Resultaat gericht werken; er wordt gestuurd op het zo min mogelijk lekken van informatie
- Elkaar aanspreken; collega's spreken elkaar aan bij eventueel onveilig gedrag
- Zich dienstbaar opstellen; collega's staan klaar voor elkaar bij eventuele vragen over informatiebeveiliging
- Integer gedrag; er is geen goed of fout, een ieder schat op basis van eigen expertise in hoe om te gaan met vertrouwelijke informatie
- Ondernemend zijn; het werk kent de nodige risico's, deze worden geaccepteerd en kan niet worden voorkomen
- Other …

Vraag 30: Waar is volgens u de meeste aandacht nodig om mensen te overtuigen om de beveiligingsmaatregelen te volgen?

- Kennis
- Risico's
- Attitude
- Subjectieve norm
- Weet niet
- Other …

Bijlage 4: Risicoreductie



Bijlage 5: Gedragsregels

3.7 Maatregelen Bewustwording en Training

Niveau	Medewerker	Manager
4	BTME1 t/m 22	BTMA1 t/m 6
3	BTME1 t/m 22	BTMA1 t/m 6
2	BTME1 t/m 22	BTMA1, 2, 3, 5 en 6
1	BTME1 t/m 22	BTMA1, 2, 5 en 6

Medewerker	BTME1	Bedienaars, beheerders en overig ondersteunend personeel zijn verplicht om de door het management aangegeven en beschikbaar gestelde periodieke Cybersecurity cursussen, trainingen, E-Learning modulen te volgen en hiernaar te handelen.
	BTME2	Iedere medewerker is zich bewust van de voor hem/haar van toepassing zijnde taken, bevoegdheden en verantwoordelijkheden voor beveiliging en weet dat gebruikers- en systeemactiviteiten worden gelogd.
	BTME3	Bedienaars, beheerders en overig ondersteunend personeel nemen de Cybersecurity beveiligingsinstructies strikt in acht en zijn verantwoordelijk voor hun aandeel in de beveiliging van het object.
	BTME4	Bedienaars, beheerders en overig ondersteunend personeel doen aan sociale controle, spreken elkaar aan op ontoelaatbaar en risicovol gedrag en bespreken geconstateerde onregelmatigheden in het periodieke werkoverleg met het eigen management/Objectbeheerder.
	BTME5	Bij het constateren van een beveiligingsincident dienen bedienaars, beheerders en overig ondersteunend personeel dit direct als een beveiligingsincident te melden bij de verantwoordelijke objecteigenaar/ -beheerder. Er is sprake van een beveiligingsincident bij het manifest worden van een (dreigend of reeds opgetreden) beveiligingsrisico als gevolg van een (mogelijke) overtreding van het beveiligingsbeleid of onregelmatigheid. Voorbeelden van beveiligingsincidenten zijn: - verlies van dienst, apparatuur of voorzieningen; - systeemstoringen of overbelasting; - menselijke fouten die leiden tot functionele verstoring of uitval van systemen; - inbreuk op fysieke en logische beveiligingsvoorzieningen van het object; - inbreuk op de bediening en beheer; - ongeautoriseerde systeemwijzingen;

		- niet-naleving van beleid of gedragsregels; - virusmeldingen; - verlies of diefstal van bedrijfsmiddelen; - oneigenlijk gebruik van bevoegdheden; - vandalisme, moedwillige beschadiging.
	BTME6	Afwijkend systeemgedrag kan een aanwijzing zijn voor een aanval op de beveiliging of voor een daadwerkelijk beveiligingslek en behoort daarom altijd direct te worden gerapporteerd als een beveiligingsincident en gemeld aan de Objectverantwoordelijke/-beheerder.
	BTME7	Bedienaars, beheerders en overig ondersteunend personeel moeten bij het constateren van eventuele onregelmatigheden dan wel onveilige situaties die handelingen verrichten of maatregelen treffen die verdere uitbreiding van het incident kunnen voorkomen dan wel de schade beperken.
	BTME8	Bedienaars, beheerders en overig ondersteunend personeel gaan zorgvuldig om met de verstrekte persoonsgebonden fysieke toegangmiddelen voor het object en de (systeem, bedien, technische) ruimten hierbinnen en delen deze niet met collega's.
	BTME9	Bedienaars, beheerders en overig ondersteunend personeel creëren geen eigen netwerkkoppelingen op het object en melden dit als een beveiligingsincident als er een zelf aangelegde netwerkkoppeling wordt geconstateerd.
	BTME10	Bedienaars, beheerders en overig ondersteunend personeel nemen de wachtwoordrichtlijn voor de logische toegang tot ICS/SCADA en overige ondersteunende ICT-systemen in acht.
	BTME11	Bedienaars, beheerders en overig ondersteunend personeel koppelen geen mobiele apparatuur of removable media aan de ICS/SCADA, overige ondersteunende ICT-systemen en object netwerken. Uitgezonderd zijn de beheerders die dit alleen na autorisatie van de hiertoe gemandateerde functionaris en uitgevoerde actuele viruscontrole van apparatuur/media mogen doen.
	BTME12	Voor bedienaars, beheerders en overig ondersteunend personeel is toegang tot internet en het gebruik van email vanaf ICS/SCADA en overige daaraan ondersteunende ICT-systemen strikt verboden.
	BTME13	Bedienaars, beheerders en overig ondersteunend personeel mogen de beschikbaar gestelde toegangsmiddelen (tokens, pasjes) tot ICS/SCADA en ondersteunende systemen en –netwerken alleen gebruiken voor het doel waarvoor ze ontworpen zijn. Hierbij mogen de getroffen beveiligingsmaatregelen niet omzeild worden.
	BTME14	Bedienaars, beheerders en overig ondersteunend personeel houden hun accountgegevens strikt geheim; zij gebruiken hun account en uitgegeven autorisaties alleen zelf en staan niet toe dat anderen onder hun account kunnen inloggen. Handelingen zijn altijd te herleiden naar

		de voor dat account geautoriseerde persoon.
	BTME15	Bedienaars, beheerders en overig ondersteunend personeel dienen op ICS/SCADA en de overige ondersteunende ICT systemen en –netwerken de standaard/default/fabrieks accounts en/of wachtwoorden bij ingebruikname te wijzigen conform de wachtwoordrichtlijn van RWS.
	BTME16	Bij het constateren van onregelmatigheden in de logische toegang tot ICS/SCADA en overige ondersteunende ICT-systemen dient iedere medewerker dit onverwijld als een beveiligingsincident te melden bij de Objectverantwoordelijke/-beheerder.
	BTME17	Ongeautoriseerd aan- of afkoppelen van removable apparatuur of usb-sticks aan het netwerk of ICS/SCADA systemen is strikt verboden.
	BTME18	Alleen geautoriseerde medewerkers/beheerders mogen systemen die voorzien zijn van de laatste security updates, patches en actuele viruscontroleprogrammatuur koppelen aan objectdatanetwerken of ICS/SCADA systemen.
	BTME19	Gegevensdragers worden altijd vooraf op virussen gecontroleerd voordat deze worden gekoppeld aan ICS/SCADA of overige ondersteunende ICT-systemen en netwerken.
	BTME20	Incidenten die zich voordoen binnen het wijzigingsproces en afwijkingen van het wijzigingsproces moeten worden gemeld bij de Objectverantwoordelijke/ -beheerder.
	BTME21	Onregelmatigheden, incidenten en storingen binnen het back-up en recovery proces moeten worden gemeld bij de Objectverantwoordelijke/ -beheerder.
	BTME22	Bedienaars, beheerders en overig ondersteunend personeel zorgen ervoor dat onbeheerde ICS/SCADA-systemen en overige ICT-apparatuur – zo mogelijk - wordt gelocked.
Manager	BTMA1	Er dient bewerkstelligd te worden dat bedienaars, beheerders en overig ondersteunend personeel continu bewust worden gemaakt en geschikte training en regelmatige bijscholing krijgen met betrekking tot het beveiligingsbeleid en procedures, voor zover relevant voor hun functie.
	BTMA2	Opdrachtnemer draagt zorg voor en ziet erop toe dat bedienaars, beheerders en overig ondersteunend personeel: • de periodieke Cybersecurity cursussen, trainingen en E-Learningmodulen volgen en een actuele administratie hiervan aanwezig is; • de beschikking hebben over actuele (technische) beheerdocumentatie, gebruikers- en/of installatiehandleidingen voor de ICS/SCADA en overige ondersteunende ICT-systemen en bedrijfsmiddelen; • dat werkzaamheden door gescreend personeel uitgevoerd worden en dat geheimhouding is overeengekomen voor ingehuurd personeel, objectverantwoordelijke/-beheerder bepaalt in welke situaties dit aan de orde is en de vorm waarin; • ingehuurd personeel een geheimhoudingsverklaring heeft ondertekend; • dat bedienaars, beheerders en overig ondersteunend personeel van zowel RWS als die van externe partijen alle

		bedrijfsmiddelen, ICS/SCADA en overige ondersteunende ICT-systeemdocumentatie van RWS die ze in hun bezit hebben retourneren bij beëindiging van hun dienstverband, contract of overeenkomst; • dat de toegangsrechten van alle bedienaars, beheerders en overig ondersteunend personeel van zowel RWS als die van externe partijen de verstrekte toegangsmiddelen direct worden geblokkeerd bij beëindiging van het dienstverband, het contract of na wijziging van de overeenkomst worden aangepast; • dat calamiteitenplannen worden betrokken in de bewustwordingstrainingen, trainingen en testactiviteiten; • gebruik van de centraal beschikbaar gestelde technische middelen voor fysieke en logische toegang op medewerkers niveau.
	BTMA3	De objectverantwoordelijke/-beheerder/verantwoordelijk management bespreekt en evalueert in de periodieke werkoverleggen de beveiligingsincidenten van de afgelopen periode, hoe op dergelijke incidenten is geacteerd, hoe het beter kan en hoe deze in de toekomst vermeden kunnen worden alsmede de feedback van de bewustwordingsactiviteiten en specifieke trainingen.
	BTMA4	Opdrachtnemer ziet erop toe dat werknemers en ingehuurd personeel zich houden aan de gedragsregels voor beveiliging zoals fysieke en logische toegang en melding van beveiligingsincidenten. Voor zover controle op naleving van gedragsregels mogelijk is, wordt hiervoor een controleprogramma met steeksproefsgewijze controles vastgesteld en uitgevoerd.
	BTMA5	Opdrachtnemer besteedt en bespreekt Cybersecurity in de functioneringsgesprekken met medewerkers en beheerders en maakt hiertoe opleidingsplannen waarbij wordt toegezien op uitvoering.
	BTMA6	Opdrachtnemer dient bij het constateren van onregelmatigheden in de logische toegang tot ICS/SCADA en overige ondersteunende ICT-systemen uit voorzorg in dergelijke situaties het betreffende account en wachtwoord altijd te laten wijzigen.