Social engineering binnen Nederlandse zelfstandige bestuursorganen

Onderzoek naar het informatiebeveiligingsbeleid bij de Nederlandse zelfstandige bestuursorganen inzake social engineering

Student:	Alex Trappenberg
Identiteitsnummer:	851058292
Datum rapport:	31 augustus 2018
Datum presentatie:	13 september 2018

Social engineering in independent governing bodies in the Netherlands

Research into the information security policy at the independent governing bodies in the Netherlands regarding social engineering

Opleiding:	Open Universiteit, faculteit Management, Science & Technology Masteropleiding Business Process Management & IT
Programme:	Open University of the Netherlands, faculty of Management, Science & Technology Master Business Process Management & IT
Cursus:	IM9806 Afstudeertraject Business Process Management and IT
Student:	Alex Trappenberg
Identiteitsnummer:	851058292
Datum:	31 augustus 2018
Afstudeerbegeleider	dr. ir. H.L. Jonker
Meelezer	prof. dr. R.J. Kusters
Versie nummer:	1.0
Status:	Final

Abstract

Social engineering (of social hacking) is een techniek waarbij een computerkraker een aanval op computersystemen tracht te ondernemen door de zwakste schakel in de computerbeveiliging, namelijk de mens, te kraken. (Wikipedia, 2018). Social engineering is zeer actueel, uit recent onderzoek ("2018 Data Breach Investigations Report | Verizon Enterprise Solutions", z.d.) blijkt dat social engineering tactieken op de vierde plaats staat op de lijst van gebruikte cyberaanval tactieken. Binnen de scope van de centrale Rijksoverheid is er reeds onderzocht in hoeverre er beleid is op social engineering, hoe bewust de medewerkers hiervan zijn en of er slachtoffers zijn gevallen. Bij deze onderzoeken zijn Zelfstandige Bestuursorganen buiten scope gebleven.
Daarom wordt in deze studie onderzocht in hoeverre ZBO's een informatiebeleid hebben dat de gevaren van social engineering afdoende dekt en of de medewerkers zich voldoende bewust zijn van het beleid. Ook worden de resultaten van dit onderzoek naast de bevindingen van eerdere onderzoeken gelegd.

In dit rapport wordt het resultaat beschreven van een initieel verkennend onderzoek bij één ZBO. Vier interviews met informatiebeleid functionarissen en een enquête onder de medewerkers liggen ten grondslag aan de resultaten. Het aantal valide reacties op deze enquête was 149.

Het informatiebeleid van de onderzochte ZBO is afgestemd op de Baseline Informatiebeveiliging Rijksdienst (BIR) en ISO27001 net als bij de andere rijksoverheidsinstellingen. Het informatiebeveiligingsbeleid dekt alle punten die aanwezig dienen te zijn om social engineering gevaar in te perken. Op awareness valt winst te boeken. Van de tien onderzochte maatregelen tegen social engineering scoren er vier daarvan vrij laag bij awareness onder het personeel, dat zijn: Informatie classificatie, Document afhandeling/vernietiging, Clean Desk en Incident Afhandeling. Bij thema's van social engineering scoren er drie vrij laag bij awareness onder het personeel: Begrip social engineering, Motieven van social engineering en bekendheid van een Reverse social engineering aanval.

Het empirisch onderzoek laat verder geen grote verschillen zien voor wat betreft awareness van het informatiebeleid en social engineering vergeleken met de voorgaande onderzoeken bij rijksoverheidsinstellingen. Verder blijkt uit het onderzoek dat er geen verschil is tussen interne en externe medewerkers als het gaat om awareness van de informatiebeveiliging van de ZBO.

De onderzoeksresultaten bij één ZBO zijn hoopgevend en leggen de vinger op de zere plekken waardoor er gericht gewerkt kan worden aan verbetering van social engineering awareness en beleid hieromtrent.

Sleutelbegrippen

Social engineering, Zelfstandige Bestuursorganen, informatiebeveiligingsbeleid, medewerker awareness.

Voorwoord

De masteropleiding Business Proces Management & IT aan de Open Universiteit wordt afgesloten met een empirisch onderzoek dat de student (ik) met succes moet uitvoeren en verdedigen. Mijn onderzoek en bevindingen heb ik in dit document vastgelegd. Het onderzoek is een vervolgonderzoek dat zich afspeelt binnen een Zelfstandig Bestuursorgaan (ZBO) welke onderdeel uitmaakt van de rijksoverheid maar dan toch anders is dan een ministerie. Ik word ingehuurd door deze ZBO voor specifieke kennis en heb toestemming gekregen om mijn onderzoek hier uit te mogen voeren.

Ik wil iedereen bedanken die mij hebben geholpen met deze scriptie. Ook wens ik iedereen te bedanken die de moeite hebben genomen om mijn enquête in te vullen en de informatiebeveiliging functionarissen die aan het interview hebben meegedaan.

Alex Trappenberg
Augustus 2018

Samenvatting

Social engineering (of social hacking) is een techniek waarbij een computerkraker een aanval op computersystemen tracht te ondernemen door de zwakste schakel in de computerbeveiliging, namelijk de mens, te kraken (Wikipedia, 2018). Binnen de scope van de centrale Rijksoverheid is er reeds onderzocht in hoeverre er beleid is op social engineering, hoe bewust de medewerkers hiervan zijn en of er slachtoffers zijn gevallen. Bij deze onderzoeken zijn Zelfstandige Bestuursorganen buiten scope gebleven, deze hoeven zich niet te conformeren aan de Baseline Informatiebeveiliging Rijksdienst (BIR). Daarom wordt in dit onderzoek onderzocht in hoeverre ZBO's een informatiebeleid hebben dat de gevaren van social engineering afdoende dekt en of de interne en externe medewerkers zich voldoende bewust zijn van het beleid. Ook worden deze resultaten vergeleken met de voorgaande onderzoeken bij rijksoverheidsinstellingen.

In dit rapport wordt het resultaat beschreven van een initieel verkennend onderzoek bij één ZBO. De resultaten zijn verkregen door een casestudy waarbij data is verkregen door middel van interviews die gehouden werden met vier informatiebeveiligingsfunctionarissen. Verder is er een enquête gehouden onder de medewerkers waarbij er 149 hieraan meededen. Tot slot is archiefonderzoek uitgevoerd om een compleet beeld van hun informatiebeleid te kunnen schetsen.

Het informatiebeleid van de onderzochte ZBO is afgestemd op de Baseline Informatiebeveiliging Rijksdienst net als bij de andere rijksoverheidsinstellingen. Social engineering awareness onder de medewerkers verdient aandacht. Ongeveer 1 op de 3 deelnemers (34%) weten niet hoe ze met een beveiligingsincident moeten omgaan en bijna 30% van de deelnemers vinden dat het beveiligingsbeleid niet actief genoeg wordt verspreid. De cijfers van social engineering aanvallen voor de laatste 6 maanden is 25%. Van de medewerkers zijn 58% onvoldoende bekend met het begrip social engineering.

Als de resultaten van dit onderzoek vergeleken worden met de voorgaande onderzoeken bij rijksoverheidsinstellingen liggen de cijfers van social engineering aanvallen voor de laatste 6 maanden voor bijna de helft minder dan uit het onderzoek uit 2017. Voor wat betreft informatiebeleid awareness op 10 gezamenlijk gemeten maatregelen om Social Engineering tegen te gaan liggen de cijfers niet ver uit elkaar.

Bij de onderzochte ZBO is de uitkomst dat er geen verschil van awareness van het informatiebeleid tussen Internen en externen is geconstateerd. Awareness van Social engineering ligt bij de externen hoger dan bij internen, maar dat is deels te danken aan het hoge percentage IT-specialisten (48%) die meer kennis hebben op dit gebied.

Wetenschappelijke aanbeveling is voor vervolgonderzoek bij meerdere ZBO’s, er is met dit onderzoek slechts één ZBO (casestudy) onderzocht.

Praktijk-aanbevelingen zijn gericht op verbetering van awareness. Onderdelen die aandacht nodig hebben voor informatiebeleid zijn: Informatie classificatie, Document afhandeling/vernietiging, Clean Desk en Incident Afhandeling.
Bij social engineering awareness: Begrip social engineering, Motieven en Reverse social engineering.

Summary

Social engineering (or social hacking) is a technique in which a computer hacker attempts to attack computer systems by cracking the weakest link in computer security, namely the human being (Wikipedia, 2018). Within the scope of central government, research has already been carried out into the extent to which there is a policy on social engineering, how aware the employees are of this and whether there have been casualties. In these investigations, Independent Administrative Bodies were out of scope, they do not have to conform to the Baseline Informatiebeveiliging Rijksdienst (BIR). That is why this study investigates to what extent ZBOs have an information policy that adequately covers the dangers of social engineering and that the internal and external employees are sufficiently aware of the policy. These results are also compared with the previous studies at central government institutions.

This report describes the result of an initial exploratory study at one ZBO. The results were obtained by a case study in which data was obtained through interviews held with four information security officers. In addition, a survey was held among the employees in which 149 participated. Finally, archival research was carried out to paint a complete picture of their information policy.

The information policy of the ZBO surveyed is in line with the Baseline Informatiebeveiliging Rijksdienst, as is the case with the other government institutions. Social engineering awareness among employees deserves attention. Approximately 1 in 3 participants (34%) do not know how to deal with a security incident and almost 30% of participants feel that the security policy is not being actively distributed enough. The figures of social engineering attacks for the last 6 months is 25%. Of the employees, 58% are insufficiently familiar with the concept of social engineering.

If the results of this study are compared with the previous surveys at central government institutions, the figures for social engineering attacks for the last six months are almost half less than those from the 2017 survey. As far as information policy is concerned, 10 jointly measured measures to combat social engineering, the figures are not far apart.

In the ZBO surveyed, the result is that no difference of awareness of the information policy between internal and hired employees has been detected. Awareness of Social Engineering is better among hired employees but that is partly due to the high percentage of IT specialists (48%) who have more knowledge in this area.

Scientific recommendation is for follow-up research at several ZBOs. Only one ZBO (case study) has been investigated with this study.

Practical recommendations are aimed at improving awareness. Parts of the information security policy that require attention are: Information classification, Document handling/destruction, Clean Desk and Incident Handling.

Parts of social engineering awareness that need to be improved are: Understanding social engineering, Motives and Reverse social engineering.

Inhoudsopgave

1. Introductie

1.1. Inleiding

Nagenoeg iedereen is ooit met Social Engineering in aanraking geweest. Een van de meest bekende vormen is phishing. Niet alleen individuen hebben er last van, ook overheidsinstellingen kunnen hier de dupe van zijn. Eerdere onderzoeken naar Social Engineering bij de Nederlandse overheid (Van der Laan, 2016; Spijker, 2017) hebben getracht de effecten en aanpak hiervan in kaart te brengen. Social Engineering problematiek speelt ook een rol bij Industrieel automatisering bij de Nederlandse overheid (Nizami, 2017).
Er is ook naar social engineering bij een Nederlandse gemeentelijke gekeken (Goes, 2012) en phishing aanvallen in België (Schoofs, 2014). Echter is het niet duidelijk hoe zelfstandig bestuursorganen (ZBO's), die weliswaar bij de Nederlandse overheid horen maar toch een behoorlijk verschil vertonen met rijksoverheidsinstellingen, het effect van social engineering ervaren en wat voor beleid deze hieromtrent hebben. Dit vervolgonderzoek probeert op basis van de eerdere onderzoeken naar social engineering bij de Nederlandse rijksoverheidsinstellingen het awareness van social engineering en het beleid hieromtrent bij ZBO's in kaart te brengen.
Dit onderzoek maakt gebruik van hetzelfde raamwerk dat gebruikt werd bij twee eerdere onderzoeken. Dit raamwerk zal worden geüpdatet waar nodig en zal worden toegepast op één ZBO (maximaal haalbaar binnen dit onderzoek) om te kijken hoe deze ervoor staat. Er wordt verder naar de rol van externe medewerkers gekeken: is het risicoprofiel met betrekking tot social engineering anders dan voor interne medewerkers. Dit onderzoek is een eerste aanzet om dit nog onbekend gebied binnen een ZBO in kaart te brengen.

1.2. Leeswijzer

1. Introductie. In dit hoofdstuk wordt de aanleiding voor dit empirisch onderzoek gepresenteerd. Verder komt zowel de wetenschappelijke als de maatschappelijke relevantie van dit onderzoek aan bod. Als laatste wordt de probleemstelling en opdrachtformulering behandeld.
2. Doel van het empirisch onderzoek. Hoofdstuk 2 gaat in op het doel van dit onderzoek, opzet en referentieraamwerk dat gebruikt is bij dit onderzoek.
3. Methode. Hier worden de gekozen onderzoeksstrategie en aanpak behandeld. Ook komen de maatregelen die genomen worden ten behoeve van betrouwbaarheid, validiteit en ethische aspecten aan bod.
4. Uitvoering. Details van dit empirische onderzoek worden hier behandeld.
5. Resultaten. De resultaten van dit onderzoek.
6. Discussie. Hier worden de aspecten die bij dit onderzoek naar voren zijn gekomen besproken.
7. Conclusies en aanbevelingen. Samenvatting van de resultaten worden hier gepresenteerd en conclusies getrokken. Ook de aanbevelingen, zowel maatschappelijk als wetenschappelijk, worden hier behandeld.
8. Reflectie. Het laatste hoofdstuk is een persoonlijke reflectie van de onderzoeker over hoe dit onderzoek is verlopen.

Extra informatie is te vinden in de bijlagen. De referenties zijn opgenomen in de bibliografie.

1.3. Context

Social engineering is een probleem dat steeds vaker voorkomt en technologische ontwikkelingen kunnen moeilijk toegepast worden om deze hardnekkige vorm van misbruik tegen te gaan.
Uit eerdere onderzoek is gebleken dat er onvoldoende wetenschappelijke literatuur aanwezig was naar social engineering binnen overheden en dan met name Nederlandse Rijksoverheid (Van der Laan, 2016). Dit resulteerde in een conceptueel model waar de verschillende aanvalstechnieken zijn gepositioneerd tegenover de informatiebeveiligingsbeleid maatregelen om de kans van deze aanvallen in te perken. Dit conceptueel model was gebruikt bij drie empirische onderzoeken bij Nederlandse overheid (Van der Laan, 2016; Spijker,2017; Nizami, 2017). Na het bestuderen van de hierboven genoemde onderzoeken is me opgevallen dat Zelfstandig bestuursorgaan (ZBO) in een adem wordt genoemd met rijksoverheidsinstellingen, terwijl sommige ZBO's enorm verschillen van rijksdiensten. De rijksoverheid is verplicht zich aan de Baseline Informatiebeveiliging Rijk (BIR) te houden, hierop is hun informatiebeveiligingsbeleid op afgestemd. Een ZBO niet, dit staat dan ook letterlijk in deze BIR: "Zelfstandige bestuursorganen (ZBO's) zijn niet verplicht de BIR2017 toe te passen" (BIR 2017). Hierdoor is het onduidelijk of de hierboven genoemde onderzoeken extrapoleert kunnen worden naar ZBO's, onderzoek tot nu toe is alleen gedaan op rijksoverheidsinstellingen. Semi-overheden, en in het bijzonder Zelfstandige bestuursorganen, kunnen met hun eigen beleid dat niet in lijn is met de BIR verschillen van rijksoverheden. Dit onderzoek heeft als doel inzicht te verschaffen in het verschil tussen ZBO's en de Nederlandse Rijsoverheid op het gebied van social engineering beleid en effectiviteit.

1.4. Relevantie

1.4.1. Wetenschappelijke relevantie

Het is niet duidelijk hoe Zelfstandig bestuursorganen, die weliswaar bij de Nederlandse overheid horen maar toch andere informatiebeveiligingsbeleidsregels hanteren, verschillen met betrekking tot social engineering beleid en awareness. Door hetzelfde raamwerk en dezelfde onderzoeksmethodes te gebruiken als bij de vorige onderzoeken (Van der Laan, 2016; Spijker, 2016; Nizami, 2017) kunnen hier de resultaten vergeleken worden om het verschil bekend te maken. Verder hebben de voorgaande onderzoeken vervolgonderzoek als advies meegegeven. Deze worden dan ook meegenomen om dit wetenschappelijke gat te dichten. Dat zijn:

- Social engineering problematiek binnen Zelfstandig bestuursorganen.
- De verschillen en overeenkomsten tussen de Nederlandse Rijksoverheid en ZBO's op het gebied van informatiebeveiliging en SE in het bijzonder.
- Verschil tussen interne en externe medewerkers (inhuur/zzp) met betrekking tot social engineering bewustzijn en bekendheid met beleid hieromtrent.
- Of aantal dienstjaren binnen het bedrijf een verschil maakt bij het SE-problematiek.

De hierboven genoemde wetenschappelijke relevante vraagstukken zijn direct te relateren aan de twee eerdere onderzoeken. De relatie hiervan is te zien in tabel 1.

Wetenschappelijke gat (Vervolg adviezen)	2017	2016
Verbreding van de scope	x	x
Verband awareness jaar in dienst		x
Verband awareness interne externe medewerkers		x
Verder in tijd		x

Tabel 1Mapping wetenschappelijke relevantie keuzes

1.4.2. Praktische relevantie

Praktische relevantie dat een toegevoegde waarde biedt aan de maatschappij:

• De ZBO krijgt inzicht hoe zij ervoor staan vergeleken met Rijksoverheidsdiensten op het gebied van social engineering. Deze “benchmark” kan gebruikt worden om de huidige risicobeheersing met betrekking tot social engineering te optimaliseren.
• Indien er een duidelijk verschil wordt geconstateerd tussen interne en externe medewerkers op het gebied van social engineering en informatiebeleid awareness kan verder naar de mogelijke oorzaken gezocht worden en manieren om deze te optimaliseren zodat deze effectiever is voor beide doelgroepen.
• Dit onderzoek kan als basis dienen voor andere ZBO’s om meer informatie te krijgen over social engineering en beleid hieromtrent.

1.5. Probleemstelling

Er ligt een aardig inzet aan onderzoek naar social engineering bij de Nederlandse rijksoverheid, maar ZBO’s blijven uit beeld. Dit vullen we met dit onderzoek in zodat het beeld compleet wordt. ZBO’s zijn zelfstandig en doorgaans gericht op een specifieke uitvoerende taak, en daardoor moeten zij vaak voldoen aan specifieke (internationale/sectorale) wet- en regelgeving en kunnen daardoor een afwijkend informatiebeveiligingsbeleid hebben. Hierdoor zijn de conclusies van voorgaande onderzoeken niet persé van toepassing, dit is de kern van het probleem.

Dit onderzoek heeft als doel het beveiligingsbeleid op het gebied van social engineering bij ZBO’s in kaart te brengen en de bekendheid van dit beveiligingsbeleid en van social engineering onder de medewerkers inzichtelijk te maken. Dit wordt vergeleken met resultaten uit eerdere onderzoeken bij Nederlandse rijksoverheid instellingen voor verschillen en overeenkomsten. Er wordt verondersteld dat ZBO’s die onderhevig zijn aan internationale brancheregelgeving effectiever zijn met hun social engineering beleid vanwege de kennisdeling dat bestaat binnen deze branche en de hogere eisen waar ze aan moeten voldoen.

1.6. Opdrachtformulering

Het doel van de opdracht is het in kaart brengen van het informatiebeleid omtrent social engineering bij ZBO's en de awareness van social engineering en het informatiebeleid bij de medewerkers. Om deze opdracht uit te kunnen voeren moet antwoord worden gezocht op een aantal vragen.

De twee centrale vragen voor deze scriptie zijn:

Hoe gaan ZBO's om met de social engineering problematiek?

Wat zijn de verschillen en overeenkomsten ten opzichte van andere rijksoverheidsinstellingen voor wat betreft het aanpakken van social engineering en awareness?

Concreet betekent dit dat dit onderzoek moet:

- Vaststellen hoe social engineering wordt aangepakt bij ZBO's;
- De verschillen en overeenkomsten van aanpak van social engineering tussen rijksoverheidsinstellingen en ZBO's inzichtelijk maken.

Na het bestuderen van de resultaten van de drie eerdergenoemde onderzoeken kreeg ik de indruk dat het informatiebeveiligingsbeleid van een ZBO misschien het gevaar van social engineering beter dekt (hogere dekkingsgraad) dan die van de rijksoverheid. Voor dit onderzoek heb ik een aantal hypothesen geformuleerd:

H1: ZBO's scoren hoger qua dekkingsgraad op het gebied van SE met hun Informatiebeveiligingsbeleid vergeleken met andere rijksoverheidsinstellingen.

Voor deze hypothese is de veronderstelling dat zelfstandige bestuursorganen het beter doen op het gebied van SE omdat hun informatiebeveiligingsbeleid dynamischer is dan die van de rijksoverheid en zo sneller in staat zijn om op SE-trends in te spelen. Bepaalde brancheorganisaties moeten voldoen aan internationale regelgevingen naast nationale regelgeving. De samenwerking die hierdoor ontstaat zorgt ervoor dat ZBO's die binnen deze kaders opereren van een zekere synergie profiteren waardoor hun informatiebeveiliging op het gebied van SE actueler is dan organisaties die alleen nationaal opereren.

H2: Er is een verschil tussen intern en extern personeel bij awareness van het informatiebeleid.

Met intern personeel wordt medewerkers in vaste dienst bedoeld, externen zijn medewerkers die ingehuurd worden, meestal van tijdelijke aard voor hun expertise. Soms is de termijn van inhuur vrij kort waardoor zij niet voldoende bekend raken met bestaande informatiebeveiliging beleid van de organisatie. Vanuit de optiek van de inhuur heeft hij ook weinig binding met de organisatie en probeert dan ook net genoeg van de organisatie te weten om zijn taak te kunnen vervullen. Zo begint het tenminste (eigen ervaring). Hoe langer een inhuur "rondloopt" des de meer bekend hij raakt met bestaand beleid. Dit geldt mogelijk dan ook voor alle personeel, niet alleen inhuur. Een medewerker die niet bekend is met het informatiebeleid en in het bijzonder de social engineering maatregelen kan een "zwakkere" schakel zijn dan een medewerker die dat wel kent.

De deelvragen die horen bij de onderzoeksvragen:

Theoretische Deelvragen
Deelvraag 1: Wat is social engineering?
Deelvraag 2: Wat zijn ZBO's?
Deelvraag 3: Welke informatiebeveiligingsdocumenten zijn leidend binnen de Nederlandse Rijksoverheid en dienen ZBO's zich hieraan te houden?
Deelvraag 4: Wat is er in de literatuur bekend over social engineering binnen Nederlandse overheidsorganen?

Onderzoek Deelvragen
Deelvraag 5: Hoe wordt met de social engineering problematiek omgegaan bij Zelfstandig Bestuursorganen (ZBO's)?
Deelvraag 6: Zijn de medewerkers binnen ZBO's inhoudelijk bekend met deze informatiebeveiligingsdocumenten?
Deelvraag 7: Zijn de medewerkers binnen ZBO's bekend met de terminologie van social engineering?
Deelvraag 8: Welke social engineering maatregelen worden op beleidsniveau direct of indirect afgedekt door het aanwezige informatiebeveiligingsbeleid binnen de ZBO's?
Deelvraag 9: Wat is de mate van awareness van de medewerkers binnen de ZBO's van het informatiebeveiligingsbeleid met betrekking tot social engineering?
Deelvraag 10: Is er een verschil waarneembaar tussen de interne en externe (inhuur) medewerkers, qua bekendheid met het informatiebeveiligingsbeleid en de kennis over social engineering?
Deelvraag 11: Is er een verband tussen het aantal dienstjaren met awareness van SE en beleid hieromtrent binnen de ZBO?
Deelvraag 12: In hoeverre zijn de ZBO's zelf het doelwit of slachtoffer van social engineering aanvallen?

2. Doel van het empirisch onderzoek

Het maatschappelijke doel van dit onderzoek is meer duidelijkheid scheppen over social engineering bij de Nederlandse overheid danwel de Zelfstandig bestuursorganen (ZBO's). Een Zelfstandig bestuursorgaan voert een overheidstaak uit en hoort bij de Rijksoverheid, maar is geen onderdeel van een ministerie. Specifieke ZBO's kunnen dan ook onderhevig zijn aan andere regelgevingen.

De onderzochte ZBO heeft een informatiebeveiligingsbeleid dat moet voldoen aan Europees breed branche richtlijnen, Internationale Branche richtlijnen, ISO (27001/27002), NEN-EN, BIR, VIRBI en andere Nederlandse regelgeving.

Eerdere onderzoeken op het gebied van social engineering bij de Rijksoverheid zouden een verkeerd beeld kunnen schetsen, zoals hierboven is beschreven kan een ZBO een informatiebeleid hebben dat kan verschillen van andere rijksoverheidsdiensten en dus anders omgaan met het social engineering vraagstuk.

Dit onderzoek heeft als doel inzicht te verschaffen in het verschil tussen ZBO's en de Nederlandse Rijsoverheid op het gebied van social engineering beleid en effectiviteit en de resultaten te vergelijken met andere rijksoverheidsinstellingen die al eerder zijn onderzocht. Verder zal gekeken worden of er een verschil waarneembaar is tussen interne en externe (lees inhuur/zzp) medewerkers voor wat betreft bekendheid met het informatiebeveiliging beleid van de organisatie en dan specifiek het SE-vraagstuk. Bij sommige organisaties bestaat een groot deel van het personeel uit inhuurkrachten en is dus een belangrijke doelgroep.

2.1. Onderzoeksbenadering

Dit is een herhalingsonderzoek gericht op ZBO's. Voorgaande onderzoeken (Van der Laan, 2016; Spijker,2017; Nizami, 2017) waren gericht op rijksoverheid. Zelfstandige bestuursorganen behoren weliswaar tot de overheid, zij vallen echter onder een minister. Voor ZBO's geldt de Kaderwet zelfstandige bestuursorganen (http://wetten.overheid.nl/BWBR0020495/2015-01-01). Het bestaansrecht van een ZBO, volgens de kaderwet, is een orgaan waarbij deze factoren een rol spelen:

a. er behoefte is aan onafhankelijke oordeelsvorming op grond van specifieke deskundigheid;
b. er sprake is van strikt regel gebonden uitvoering in een groot aantal individuele gevallen;
c. participatie van maatschappelijke organisaties in verband met de aard van de betrokken bestuurstaak bijzonder aangewezen moet worden geacht.

In "layman's terms" betekent dit dat er een scheiding is tussen beleid en uitvoering, dat de uitvoering gebonden is aan regels en dat het wenselijk is dat de bestuursleden een weerspiegeling is van de samenleving. Dit kan betekenen dat de resultaten van de drie eerdere onderzoeken wellicht anders kunnen zijn bij de ZBO-populatie waarbij andere regels van kracht zijn dan ministeries.

De drie eerdere onderzoeken waren deductief van aard, dat is met dit onderzoek ook het geval.

De deductieve onderzoeksmethode gebruikt een theoretische veronderstelling die getest wordt door een onderzoekstrategie die speciaal voor het testen hiervan is ontworpen (Saunders et al., 2015)

De theoretische veronderstelling was door Van der Laan uit literatuurstudie verkregen waarna een referentie raamwerk is ontworpen. Deze is vervolgens door Spijker verfijnd en door Nizami toegepast op industriële automatisering. In dit onderzoek wordt gekeken of ZBO's, die onderling ook veel kunnen verschillen, anders met de social engineering problematiek omgaan dan puur rijkoverheidsinstellingen. Hetzelfde raamwerk wordt hiervoor gebruikt.

Een belangrijke methode die ook hier wordt toegepast is het zogenaamde triangulatie, dat is het verzamelen van data door meer dan een methode om er zeker van te zijn dat de gegevens je werkelijk vertellen wat je denkt dat ze je vertellen (Saunders et al., 2015). Er zal gebruik worden gemaakt van archiefonderzoek om een aantal deelvragen te kunnen beantwoorden. Verder zal de populatie onderzocht worden door middel van enquêtes aangevuld met interviews. Keuze voor deze methodes worden later in dit rapport toegelicht echter de belangrijkste reden is herhaalbaarheid van het onderzoek met de voorgaande onderzoeken.

2.2. Doelstellingen

De doelstellingen die dit empirisch vervolgonderzoek bij ZBO's voor ogen heeft worden hier op een rijtje gezet.

1. In kaart brengen wat de maatregelen die getroffen worden binnen het informatiebeleid bij ZBO's voor wat betreft social engineering en zijn er duidelijke verschillen ten opzichte van de eerder onderzochte rijksoverheidsinstellingen. De eerste hypothese voor dit onderzoek is dat ZBO's met hun informatiebeleid het beter doen vergeleken met rijksoverheidsinstellingen vanwege extra eisen waar ze aan moeten voldoen.
2. Hoe bewust ZBO-medewerkers zijn van het bestaande informatiebeleid en wat hun kennis op het gebied van SE is en hoe staat dit tegenover rijksoverheidsmedewerkers.
3. Of er verschillen zijn tussen interne en externe medewerkers voor wat betreft bekendheid van het informatiebeleid. De tweede hypothese gaat ervanuit dat er een verschil is tussen interne en externe medewerkers omdat een externe meer de focus legt op de taken waar hij voor ingehuurd wordt en in mindere mate op het informatiebeleid van de organisatie waar hij "tijdelijk" zit. Dit zou als gevolg kunnen hebben dat de externen ook niet bekend zijn met de social engineering aanpak dat voor de organisatie van kracht is.
4. Welke andere verschillen er zijn bij medewerkers voor wat betreft awareness over social engineering en bekendheid van het informatiebeleid.

2.3. Referentieraamwerk

Er is een referentie raamwerk ontwikkeld (van der Laan, 2016) en later verfijnd (Spijker, 2017) om de type aanvallen van social engineering en de maatregelen die nodig zijn deze tegen te gaan in kaart te brengen. Dit raamwerk werd vervolgens in empirische onderzoeken gebruikt om de awareness van social engineering onder personeel en dekkingsgraad van informatiebeleid op het gebied van social engineering bij de rijksoverheid vast te kunnen stellen.

Er is gecontroleerd of er nieuwe aanvalstechnieken zijn bijgekomen. Dit is als volgt gedaan:
Via de digitale bibliotheek is gezocht met de steekwoorden **social engineering threats .**
Dit leverde 197,571 hits. Vervolgens is er gefilterd op "last 12 months". Dit leverde 14.583 hits. Vervolgens is er gefilterd met "SUBJECT TERMS=computer information security". Dit leverde 290 hits op. Deze titels waren gescand voor social engineering aanvallen die niet meegenomen waren in het raamwerk.
Wat er ontbreekt is "Wiphishing" (Chiew et al, 2018; Ohaya, 2006; Heartfield & Loukas, 2016) dat ook "Rogue WiFi-access point" wordt genoemd. De mogelijk reden waarom dit niet is meegenomen in de voorgaande onderzoeken (zeker niet nieuw) is dat het door sommigen als "normaal" hacking wordt beschouwd. Dit echter is niet helemaal het geval. De gebruiker krijgt wel degelijk een melding dat iets niet in de haak is en hoort niet in te trappen. Bijvoorbeeld, je krijgt een certificaat melding wanneer je toestel automatisch probeert te authentiseren tegen het SSID (Service Set Identifier, wat toegang tot een bekend draadloos netwerk geeft) van de open universiteit terwijl je niet eens in de buurt bent van een OU-locatie. Dit is dan een geval van Wifi Phishing en gebruikers moeten hierop attent zijn. En bij "open wireless" moeten de gebruikers al helemaal op hun hoede zijn want daar is de kans dat je via een rogue wifi een verbinding maakt nog groter. Steeds meer (zo niet alle) organisaties beschikken over een wifi-netwerk en bedrijfsapparatuur die wifi ondersteunen en dienen hun gebruikers hiervan bewust te maken en waar nodig technische maatregelen te treffen om dit gevaar in te perken.

De andere variant van phishing is "smishing" (Chiew et al, 2018). In dit geval gaat het om persoonlijke informatie van iemand innen met behulp van SMS. Smishing staat op de lijst van opkomende threats volgens de Security softwareleverancier Norton voor 2018.

Verder is de aard van de social engineeringsaanval uit het herleide model (Spijker, 2017) verfijnd. Hier wordt per type aanval aangegeven of dit Persoon, Computer of Mobiel is. Ook "management buy-in" is verwijderd uit het model, gezien dit niet een primair mitigerende maatregel is tegen social engineering maar een ondersteunende (net als bijv. voldoende budget voor cursussen). Verder ontbreken een aantal ISO27001 voorschriften die bij de onderzochte ZBO wel zijn geïmplementeerd om social engineering tegen te gaan en mogelijk ook bij rijksdiensten. Deze zijn echter niet in de onderzoeksrapporten meegenomen. Een van de belangrijkste en voor de meeste organisaties van cruciaal belang is werken op afstand, hetzij via een portaal of met systemen (laptops of andere mobiele apparaten) die door de organisatie beschikbaar worden gesteld. Voor de volledigheid is zowel de BIR 2017 als ISO27001 binnen het referentieraamwerk verwerkt.

Voor de duidelijkheid, de voorgaande onderzoeken hebben BIR 2012 gebruikt, de huidige BIR is in september 2017 uitgekomen en is van kracht vanaf 1 Januari 2018. Hierdoor is het raamwerk niet alleen verfijnd en meer relevant gemaakt maar ook nog eens rechtgetrokken met de huidige BIR. Het raamwerk is in de volgende tabel te zien.

		Nr	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	
		BIR2017	7.1.1	7.1.2	7.2.2	7.2.3	8.2.1	9.2.6	nvt	nvt	nvt	nvt	nvt	8.2.1	nvt	9.4.1	9.4.3	11.2.9	11.2.9	12.2.1	13.2.3	16.1	18.2	6.2	
		ISO 27001	8.12	8.1.3	8.2.2	8.2.3	8.3.2	8.3.3	9.1.1	9.1.2	9.1.2	9.1.2	9.1.3	7.2.1	10.7.3	10.9.3	11.3.1	11.3.2	11.3.3	10.4.1	10.8.4	13.1.1	15.2.1	11.7		
		Maatregel	Screening CV, Referenties	Arbeidsvoorwaarden	Opleiding en bewustwording	Disciplinaire maatregelen	Retourneren bedrijfsmiddelen	Blockering Toegangsrechten	Bevelingscamera's	Aanmeldprocedure bezoekers	Bezoekerspas	Foto-identificatiepasjes	Toegangsdeuren	Informatie classificatie	Document afhandeling/vernietiging	Beperken publieke informatie	Wachtwoordmanagement	Locken van computer	Clean Desk	Antivirus/antiphishing	Email filtering	Incident Afhandeling	Auditbeleid/ Audit controles	Mobiele apparatuur en telewerken beleid	Aantal maatregelen per aanval
Nr	**Aard**	**Aanvalstechniek**																							
1	P	Dumpser driving			X				X		X		X		X							X	X		7
2	P	People spotting			X				X										X			X	X		5
3	P	Physical recogn/shoulder surfing			X				X	X	X		X					X				X	X		8
4	P	Pretexting/Profiling	X		X		X			X	X	X	X	X	X	X	X					X	X		13
5	C	Mail-outs			X											X				X	X	X	X		6
6	C	Phishing			X									X		X	X			X	X	X	X		8
7	M	Smishing			X									X		X						X	X	X	6
8	M	Phreaking /Vishing			X		X	X						X		X						X	X		7
9	C	Virtual reconnaissance/Waterholing			X											X	X					X	X		5
10	C	Web Search			X									X		X							X		4
11	P	Physical Impersonation	X		X		X	X	X	X	X	X	X		X	X						X	X		13
12	P	Reverse Social engineering	X		X				X	X	X		X	X		X						X	X		10
13	C	Virtual Impersonation / Fake profiles	X		X			X								X						X	X		6
14	C	Wiphishing			X	X							X				X					X	X	X	7
15	P	Direct approach		X	X	X			X	X	X	X	X	X								X	X		11
16	P	Office Snooping/Desk sniffing		X	X	X			X	X	X	X	X		X		X	X	X			X	X		14
17	P	Piggybacking /Tailgating		X	X	X			X	X	X		X									X	X		9
18	C	Baiting / Item dropping		X	X	X							X							X		X	X		7
19	C	Data leakage			X		X	X					X	X	X			X		X	X	X	X	X	12
20	P/C	Identity theft			X		X	X		X		X	X	X			X					X	X		10
21	C/M	Malicious software			X			X												X	X	X	X	X	7
		Aantal aanval gedekt door maatregel	4	4	21	5	5	6	8	8	8	5	12	9	5	10	6	3	2	5	4	20	21	4	
		Legenda:																							
		P=Persoon																							
		M=Mobiel																							
		C=Computer																							

Tabel 2 Social Engineering raamwerk

Wat uit de hierboven tabel opvalt (in geel gearceerd) zijn de maximale aanvalstechnieken die een maatregel dekt. De belangrijkste zijn “Opleiding en bewustwording”, “Incidentafhandeling” en “Auditbeleid controles”. Ook de aanvalstechniek die het minst wordt afgedekt door het palet aan maatregelen. Hier dient een organisatie extra op te focussen.

De complete en herziende lijst van aanvallen is te vinden in de bijlage.

3. Methode

Omdat dit onderzoek een vervolgonderzoek is, zal gebruik gemaakt worden van dezelfde referentie raamwerk en methodes die bij de voorgaande onderzoeken gebruikt werden. Methodes die gebruikt waren zijn casestudy samen met interview, enquête. Er zal een vergelijking gemaakt worden tussen de eerdere onderzoeken bij rijksoverheidsinstellingen en de ZBO op gebied van social engineering beleid en awareness. Dit is alleen mogelijk door dezelfde methodes voor onderzoek en raamwerk te hanteren.

3.1. Onderzoekstrategie

Voor het empirisch onderzoek gedeelte van het BPM & IT (Business Process Managment and IT) opleiding wordt gebruik gemaakt van methoden en technieken uit “het boek van Saunders” (Saunders et al., 2015). Er worden zeven methodes behandeld die gebruikt kunnen worden. Deze worden hierna in het kort doorlopen en de reden waarom er wel of niet voor een bepaalde methode is gekozen.

Experiment
Bij experiment ligt de focus op causale verbanden waarbij het manipuleren van een onafhankelijke variabele er ook een verandering brengt in een andere variabele. Deze methode wordt vaak toegepast in laboratoria. Dit is een methode die **niet** past bij deze onderzoek, het doel van dit onderzoek is het vaststellen hoe informatiebeveiliging is geregeld in verband met social engineering bij ZBO’s en awareness hiervan om de uitkomsten te vergelijken met andere overheidsinstellingen. Manipuleren van variabelen is hier geen sprake van en organisaties of personen in een gecontroleerde omgeving (laboratoria) bestuderen ook niet.

Enquête
Enquêtes worden gebruikt bij vragen als ‘wie, wat, waar en hoeveel’ die beantwoord moeten worden, het is relatief makkelijk veel gegevens te verzamelen bij grote populaties. Er wordt gewerkt met vragenlijsten om vergelijkingen te kunnen doen. Gegevens kunnen gebruikt worden om mogelijke oorzaken te geven voor bepaalde verbanden tussen variabelen. Dit is een zeer geschikte methode voor dit onderzoek, gegevens van een grote populatie moeten verzameld worden door één persoon en verbanden tussen variabelen dienen gelegd te worden. Bij deze methode worden ook vaak gestructureerde interviews gebruikt waarbij alle geïnterviewden gestandaardiseerde vragen krijgen. Dit is dan “triangulatie”. Dat betekent dat er een, twee of meer methodes van gegevensverzameling wordt gebruikt als controle om er zeker van te zijn dat de gegevens je werkelijk vertellen wat je denkt dat ze je vertellen.

Case study
Een case study is een zeer beperkt studie, vaak van een enkel onderzoeksobject (een persoon of een individueel geval) met als doel zoveel mogelijk “het waarom” van dit specifieke geval te achterhalen. Dit type onderzoekstrategie wordt meestal in verklarend en verkennend onderzoek gebruikt. Triangulatie wordt dan vaak toegepast om alle aspecten van een specifiek geval te kunnen

waarnemen. Deze onderzoekstrategie is niet optimaal om invloed van social engineering op ZBO's te onderzoeken echter heeft alleen één ZBO volledig aan dit onderzoek meegewerkt waardoor dit onderzoek grotendeels een case study is geworden. Ook zijn alleen informatiebeleid functionarissen geïnterviewd, dit is ook een vorm van casestudy.

Action research
Met action research methodiek ga je aan de slag met het oplossen van problemen in het bedrijf, je betrekt ook de mensen om samen problemen op te pakken. De onderzoeker behoort tot de organisatie van het bedrijf. Er is een heel proces dat ervoor zorgt dat er een diagnose wordt gesteld, plannen gemaakt en acties ondernomen (action-researchspiraal). Uiteindelijk zal action research een bijdrage leveren waar andere organisatie ook wat mee kunnen, wellicht ook buiten de context waar het onderzoek heeft plaats gevonden. Deze vorm is **niet** geschikt om bij dit onderzoek toe te passen, het is niet de bedoeling om social engineering bij ZBO's met acties te gaan beïnvloeden.

Grounded theory
Gefundeerde theoriebenadering wordt gebruikt om gedrag te voorspellen en te verklaren, waarbij de nadruk ligt op het ontwikkelen van een theorie. In grounded theory begint het verzamelen van gegevens zonder dat er eerst een theoretisch kader is gemaakt. Aan de hand van de gegevens worden er voorspellingen gemaakt en wederom met het verzamelen van meer gegevens bevestigd of ontkracht om zo tot een theorie te komen. Het zou mogelijk zijn om in de toekomst voor de social engineering problematiek bij overheid een gefundeerde theorie vast te stellen echter is dat voor nu **niet** aan de orde.

Etnografie
Etnografie is afkomstig uit de antropologie en heeft als doel "het beschrijven en verklaren van de maatschappelijke wereld waarin de onderzochte personen leven, op de manier zoals zij die zouden beschrijven en verklaren" Hiervoor heb je veel tijd voor nodig en het onderzoek gebeurt over een vrij lange periode. De onderzoeker verzamelt gegevens door zich "op te trekken" binnen de groep/wereld die onderzocht wordt om vanaf dit perspectief de situatie te bestuderen. Deze methode is **niet** geschikt om social engineering bij ZBO's ten opzichte van andere overheidsinstellingen te bestuderen. De onderzoeker maakt wel deel uit van een ZBO-organisatie maar daar blijft het ook bij.

Archiefonderzoek
Archiefonderzoek gebruikt brongegevens en documenten. Belangrijk verschil tussen archiefonderzoek en secundaire gegevensanalyse is dat bij een archiefonderzoeksstrategie er onderzoeksvragen worden gesteld die gericht zijn op het verleden en de veranderingen in de loop van de tijd, of ze nu verkennend, beschrijvend of verklarend zijn. Archiefonderzoek is niet geschikt om social engineering bij ZBO's ten op zicht van andere overheidsinstellingen in kaart te kunnen brengen maar kan gebruikt worden om het informatiebeleid van ZBO's in kaart te brengen.

Van de hierboven genoemde onderzoekstrategieën zullen er een aantal worden toegepast om tezamen tot het doel te komen. Om in kaart te brengen welk informatiebeleid er gehanteerd wordt bij ZBO's zal er **Archiefonderzoek** uitgevoerd worden. Voornamelijk deskresearch en gesprekken met informatiebeleid-functionarissen om alle informatie hieromtrent te kunnen verkrijgen en te analyseren. Informatie uit beleidsstukken die voor de rijksoverheid van toepassing zijn zullen dan

ook doorgenomen worden om het complete plaatje te kunnen schetsen. Hoe bekend de gebruikers zijn met social engineering en het informatiebeleid zal door middel van een **enquête** in kaart worden gebracht om het grootste deel van de populatie te kunnen ondervragen. Ook informatie die nodig is voor verdere analyse (aantal jaren in dienst, extern-intern, slachtoffer van SE, etc.) zal door middel van deze enquête worden verzameld. Voor triangulatie zullen de informatiebeleid-functionarissen door middel van **gestructureerde interviews** worden ondervraagd. Het informatiebeleid wordt naast archiefonderzoek ook met deze interviews verrijkt. Dit onderzoek is gericht op één ZBO, een **Case study** (gevalsituatie social engineering bij één ZBO).

3.2. Onderzoeksaanpak

Om te kunnen achterhalen hoe ZBO's het doen ten opzichte van andere Rijksoverheidsinstellingen zal dit onderzoek niet te veel van eerdere onderzoeken kunnen afwijken, desnoods mogen wel andere factoren meegenomen worden bij informatieverzameling om meer duidelijkheid te kunnen scheppen op dit gebeid. De referentiekaders van eerdere onderzoeken worden hier ook gebruikt om "appels met appels" te kunnen vergelijken. In grote lijnen zullen deze stappen worden genomen:

- Verdiepen in de SE problematiek en kritisch naar voorgaande onderzoeken kijken.
- Begeleiding: De studiebegeleider wordt regelmatig geraadpleegd en gebruikt als klankbord, dit is gedurende het complete onderzoek zo.
- Draagvlak: Er is een gesprek gevoerd met de "Chief Security Officer" van de ZBO waar ik ICT-diensten voor verricht om de onderzoeksplannen bekend te maken en draagvlak hiervoor te krijgen. Verder is er onderzocht of hij als "springplank" wil fungeren om andere ZBO-functionarissen hierbij te betrekken om de populatie van dit onderzoek te kunnen vergroten.
- Deskresearch uitvoeren naar beleidsstukken en regelgeving bij de ZBO waar ik werk voor verricht en wat de verhoudingen zijn tussen beleid waar andere Rijksoverheidsinstellingen aan moeten voldoen.
- Interviews houden met IB-functionarissen.
- Enquête uitzetten, na aankondiging/goedkeuring van de organisatie.
- Informatie analyseren
- Rapportage/scriptie afronden en indienen aan OU ter review
- Presentatie en verdediging van uitgevoerde onderzoek.

Om de betrouwbaarheid en validiteit van dit onderzoek te kunnen waarborgen zal volgens de eerdere onderzoeken worden gehandeld. Hierna wordt kort beschreven wat voor maatregelen hiervoor zijn getroffen.

3.2.1. Betrouwbaarheid

Betrouwbaarheid is een belangrijk onderdeel van elk onderzoek. Definitie van betrouwbaarheid in deze context is de mate dat de verzameling van datatechnieken en analyse bevindingen geven die consistent zijn (Saunders et al., 2015). De drie factoren die de betrouwbaarheid negatief beïnvloedden en hoe hier rekening mee werd gehouden zijn:

a. *Subject-of deelnemers fout*. Voorbeeld hiervan is de tijdstip/dag die gebruikt wordt om een enquête uit te sturen waardoor de stemming van de deelnemers op een bepaalde dag het resultaat kunnen beïnvloeden. De enquête is op intranet gepubliceerd en verschillende keren "naar boven" op de pagina gezet om zo neutraal mogelijk (tijdstip/dag) deze aan de

deelnemers te presenteren. Ik had geen verdere invloed op het tijdstip waarop de gebruikers actief deze pagina bezochten.

b. *Subject- of deelnemersvertekening (bias).* Voorbeeld hiervan is een antwoord geven dat de werkgever graag wil horen. De enquête is volledig anoniem waardoor de deelnemers zonder consequenties hun mening konden geven. Dit punt is tevens ook van toepassing op de interne validiteit (zie verder). Dit is echter in mindere mate bij de interviews die gehouden werden omdat de onderzochte ZBO slechts zes informatiebeleid-functionarissen telt en de CSO dient het rapport goed te keuren. Vóór het starten van het interview is uitgelegd dat dit onderzoek onderdeel is van mijn studie en niet in opdracht van de werkgever en dat het rapport geanonimiseerd zal worden. Hierdoor konden ze zonder consequenties hun mening uiten.
c. *Waarnemersfout.* Verschillende structuren kunnen andere waarnemingen tot gevolg hebben. De interviewvragen hebben dezelfde structuur en zijn allemaal door mezelf uitgevoerd. De enquête is uiteraard voor iedereen hetzelfde, hier is waarnemersfout niet van toepassing.
d. *Waarnemersbias.* Verschillende interpretaties (door bijv. meerdere personen) kunnen een invloed hebben op de resultaten. Waarnemersbias is binnen dit onderzoek niet van toepassing omdat ik al enige waarnemer ben. De interviewvragen en enquête zijn zoveel mogelijk gelijk gehouden om de waarnemersbias beperkt te houden.

3.2.2. Validiteit

Voorwaarde voor validiteit is dat het onderzoek eerst betrouwbaar moet zijn (Saunders et al., 2015). De volgende stap is validiteit van het onderzoek waarbij deze intern (meet je wat je denkt te meten?) en extern (generaliseerbaarheid van het onderzoek) valide is. Dit onderzoek naar SE heeft als een van de doelen het toetsen of de eerdere onderzoeken extern valide zijn.

Voor wat betreft externe validiteit van dit onderzoek bij ZBO's is dat vrij lastig vanwege het feit dat:

1. ZBO's onderling zeer divers kunnen zijn;
2. ZBO's kunnen ook sterke verschillen hebben qua Informatiebeleid dan Rijksoverheidsinstellingen;
3. Slechts één ZBO is onderzocht.

Hierna worden de interne en externe validiteit voor dit onderzoek verder behandeld en welke maatregelen hiervoor zijn getroffen.

Interne validiteit

Met interne validiteit wordt hier bedoeld de mate dat de onderzoeker zelf de resultaten beïnvloedt met de gebruikte methodes. Dit is een van de belangrijkste criteria bij een "experiment" maar is ook voor dit onderzoek van belang. Het doel is data te verzamelen om de "bias" (sturen in een bepaalde richting) zo laag mogelijk te houden en liefst helemaal te elimineren. De maatregelen die hiervoor getroffen zijn staan hier op een rij.

1. De interviewvragen zijn gestandaardiseerd zodat elk ondervraagde precies dezelfde kreeg. Antwoord hierop is uiteraard afwijkend echter informatie uit de interviews wordt gebruikt om de problematiek van SE bij ZBO's beter te kunnen begrijpen en meer inzicht te krijgen in het informatiebeleid.
2. Anonimiseren van de deelnemers zodat deze zonder consequenties hun mening mochten uiten. De enquête is volledig anoniem en de interviews die genomen werden zijn alleen door de onderzoeker traceerbaar.
3. Vragenlijst is nagenoeg hetzelfde als de voorgaande onderzoeken die op hun beurt gebaseerd zijn op een referentiewerk. De vragen zijn zodanig gepresenteerd dat ze door de enquête niet overgeslagen kunnen worden zonder te beantwoorden (required optie). Dit zijn de zogenaamde "gedwongen-keuzevragen" (Saunders et al., 2015) en bestaan uit multiple choice, ja/nee en schaalvragen.
4. De populatie die aan de enquête heeft meegedaan zijn via intranet benaderd. Iedereen krijgt deze pagina te zien en hiermee ook de oproep om mee te doen. Er is getracht ook iedereen via een ander medium te benaderen (email) echter hiervoor is toestemming van afdeling communicatie nodig. Dit is helaas niet gelukt. Dit heeft mogelijk een negatieve invloed op de interne validiteit.

Externe validiteit

De drie eerdere onderzoeken hebben getracht per onderzoek meer dan één Rijksoverheid te onderzoeken om zo de externe validiteit te kunnen verbeteren. Bij het oorspronkelijke onderzoek (Van der Laan, 2016) was deze uitgevoerd bij drie sectoren die onder twee verschillende ministeries vallen. De andere twee onderzoeken zijn slechts elk bij één ministerie uitgevoerd. Samen is dit nog een zeer beperkt aantal om hiermee te kunnen generaliseren. Helaas is bij dit onderzoek naar ZBO ook het geval. Er is getracht zoveel mogelijk ZBO's mee te nemen echter is het alleen gelukt om bij slechts één instantie voldoende data te kunnen verzamelen om het onderzoek af te kunnen ronden. Echter zal de externe validiteit van de voorgaande onderzoeken met dit onderzoek getoetst worden bij een ZBO. De onderzochte ZBO heeft een Informatiebeleid die deels is afgeleid van de Baseline Informatiebeveiliging Rijksdienst (BIR) wat aansluit op de voorgaande onderzoeken.

3.2.3. Ethische aspecten

Omdat dit onderzoek tot de categorie security behoort en uitgevoerd zal worden bij een ZBO dat belast is met beheer van een voor Nederland vitale infrastructuur zijn ethische aspecten zoals anonimiteit van groot belang. Mogelijkheid bestaat dat met dit onderzoek het reilen en zeilen op gebied van informatiebeveiliging bloot wordt gesteld aan kwaadwillenden met alle gevolgen van dien. Tevens zal er geen sturende invloed op dit rapport komen van de ZBO om de bevindingen rooskleuriger te doen uitkomen. Er is toestemming gevraagd aan de Chief Security Officer (CSO) van de onderzochte ZBO om dit onderzoek uit te kunnen voeren. Wens was dat het rapport doorgenomen kon worden om gevoelige informatie niet openbaar bekend te maken, deze informatie dient dan gecensureerd te worden.

Het volgende aspect waar rekening mee werd gehouden is het vrijwillige karakter. De medewerking van de ondervraagden is volledig op vrijwillige basis. Wel hebben twee IB-functionarissen ervoor gekozen om hier niet aan mee te werken (geen reactie op herhaalde verzoeken) en hun mening werd dan ook gerespecteerd.

Met het aspect privacy is ook rekening gehouden. De enquête is volledig anoniem. Ik werd wel door een medewerker geattendeerd dat iemand die de vragenlijst kritisch bestudeerd, er in sommige

gevallen, achter kan komen wie dit heeft ingevuld. Dat kan uiteraard alleen door iemand die daadwerkelijk werkzaam is binnen deze ZBO en zal nogal wat moeite kosten. Het complete databestand van de enquête echter wordt niet openbaar gepubliceerd alleen de samengestelde cijfers en daar is geen enkel manier mogelijk om dit te kunnen herleiden tot één persoon.

Als onderzoeker was ik bewust van het aspect objectiviteit en heb me tijdens de onderzoeken zoveel mogelijk naar gehandeld.

Ook was ik ervan bewust dat bepaalde vragen reacties kunnen opwekken als schaamte, stress en ongemakkelijkheden (Saunders et al., 2015). Of het aan de vragen, de ondervraagden of aan mezelf lag kan ik niet met zekerheid zeggen maar hier heb ik niets van gemerkt.

Bij het plaatsen van mijn oproep om mee te doen aan de enquête heb ik weliswaar niet duidelijk genoeg het onderzoeksonderwerp en doel bekend gemaakt. Dat heeft geleid dat de CSO wat vragen binnen kreeg over dit onderzoek. Ik had duidelijk aan moeten geven dat dit onderzoek voor mijn studie is en het waarom, dit heb ik snel op de intranetpagina gecorrigeerd.

3.2.4. Beantwoording van de deelvragen

Voor dit onderzoek zijn een aantal deelvragen gesteld waar antwoord op gezocht zal worden. Voor de leesbaarheid zijn deze samen met de te gebruiken methoden weergegeven in de volgende tabel.

Deelvraag	Interview	Enquête	Archiefonderzoek
DV1: Wat is social engineering?			X
DV2: Wat zijn ZBO's?			X
DV3: Welke informatiebeveiligingsdocumenten zijn leidend binnen de Nederlandse Rijksoverheid en dienen ZBO's hieraan te houden?	X		X
DV4: Wat is er in de literatuur bekend over social engineering binnen overheidsorganen?			X
DV 5: Hoe wordt met het social engineering problematiek omgegaan bij Zelfstandig Bestuursorganen (ZBO's)?	X	X	X
DV 6: Zijn de medewerkers binnen ZBO's inhoudelijk bekend met deze informatiebeveiligingsdocumenten?	X	X	
DV 7: Zijn de medewerkers binnen ZBO bekend met de terminologie van social engineering?	X	X	
DV8: Welke social engineering maatregelen worden op beleidsniveau direct of indirect afgedekt door het aanwezige informatiebeveiligingsbeleid binnen de ZBO's?	X	X	X
DV9: Wat is de mate van awareness van de medewerkers binnen de ZBO's van het informatiebeveiligingsbeleid met betrekking tot social engineering?		X	
DV10: Is er een verschil waarneembaar tussen de interne en externe (inhuur) medewerkers, qua bekendheid met het informatiebeveiligingsbeleid en de kennis over social engineering?	X	X	
DV11: Is er een verband tussen het aantal dienstjaren met awareness van SE en beleid hieromtrent binnen de ZBO?		X	
DV12: In hoeverre zijn de ZBO's zelf het doelwit of slachtoffer van social engineering aanvallen?	X	X	

Tabel 3 Onderzoekvragen en onderzoekmethoden

3.3. Databronnen

Om de doelstellingen van dit onderzoek te kunnen realiseren zijn verschillende databronnen nodig die geanalyseerd moeten worden.

3.3.1. Secundaire data

Als eerste moet de informatiebeveiliging dat voor de Rijksoverheid van toepassing is in kaart gebracht en in het bijzonder het gedeelte dat de social engineering lading dekt. Dit wordt gebruikt als basis waarmee de informatiebeveiliging van de onderzochte ZBO wordt vergeleken. Zowel de verschillen als de overeenkomsten moeten in kaart gebracht worden. Hier zal er gebruik worden gemaakt van secundaire data. Dit is data van de voorgaande onderzoeken bij rijksoverheden en ook informatiebeleidsstukken van de onderzochte ZBO samen met intranetinformatie, flyers, hand-outs en andere interne en publieke publicaties. Onderzoeksmethode die hier gebruikt wordt valt onder de categorie archiefonderzoek.

Om het informatiebeleid van de onderzochte ZBO in kaart te brengen zijn deze bronnen gebruikt:

Code	Document	Versie	Datum	Verkregen van
IB1	Cybersecurity v1.0	1.0	Jun-18	Intranet
IB2	Informatiebeveiliging beleid ZBO	1.0	Dec-15	Intranet
IB3	Information security checklist	1.1	Jan-15	Intranet
IB4	Leidraad rubricering informatie	2.0	Apr-14	Intranet
IB5	Security risk assessment methodology	1.0	Dec-15	Intranet
IB6	VIRBI Flyer	nvt	nvt	Intranet
IB7	Wachtwoordbeleid	1.0	Oct-15	Intranet
IB8	Flyer usb encryptie	nvt	nvt	Intranet
IB9	Regeling gebruik bedrijfsmiddelen, internetprotocol en gedragscode social media	2.5	Apr-18	Intranet

Tabel 4 Interne informatiebeveiligingsdocumenten onderzochte ZBO

De hierboven genoemde documenten hebben minimaal een classificatie van “Intern”. Hierdoor zijn deze niet als bijlage of welke manier dan ook beschikbaar gesteld. Dit is dan ook in lijn met de voorgaande onderzoeken bij rijksoverheidsinstellingen.

In deze tabel staan alleen de documenten die van toepassing zijn op informatiebeveiliging. Maatregelen die bij de fysieke beveilig van kracht zijn (bijv. AIVD-scanning, VOG, referentie aanvraag, toegangspasjes, camera beveiliging, biometrische maatregelen etc.) staan hier niet uitgebreid in. Beveiliging (Security) bestaat bij dit ZBO uit:

a. Information security
b. Staff security
c. Physical security

In deze onderzoek ligt de focus alleen op Information security. De interne information security-documenten zijn door mij gerubriceerd om ze tegen de mitigerende maatregelen uit het raamwerk, de BIR en ISO2007 aan te houden. Dat levert de volgende tabel op:

Maatregel	ISO 27001	BIR2017	ZBO IB Publicatie
Screening CV, Referenties	8.12	7.1.1	IB2
Arbeidsvoorwaarden	8.1.3	7.1.2	IB2,IB9
Opleiding en bewustwording	8.2.2	7.2.2	IB1,IB2,IB3,IB4,IB5,IB6,IB7,IB8,IB9
Disciplinaire maatregelen	8.2.3	7.2.3	IB2,IB9
Retourneren bedrijfsmiddelen	8.3.2	8.2.1	IB2,IB6,IB9
Blockering Toegangsrechten	8.3.3	9.2.6	IB2,IB9
Beveilingscamera's	9.1.1	nvt	IB2
Aanmeldprocedure bezoekers	9.1.2	nvt	
Bezoekerspas	9.1.2	nvt	
Foto-identificatiepasjes	9.1.2	nvt	
Toegangsdeuren	9.1.3	nvt	IB2
Informatie classificatie	7.2.1	8.2.1	IB1,IB2,IB3,IB4,IB6,IB8,IB9
Document afhandeling/vernietiging	10.7.3	nvt	IB1,IB2,IB4,IB6
Beperken publieke informatie	10.9.3	9.4.1	IB1,IB2,IB3,IB4,IB6,IB9
Wachtwoordmanagement	11.3.1	9.4.3	IB1,IB2,IB3,IB4,IB8,IB7,IB9
Locken van computer	11.3.2	11.2.9	IB2,IB3,IB4
Clean Desk	11.3.3	11.2.9	IB1,IB2,IB4,IB6
Antivirus/antiphishing	10.4.1	12.2.1	IB2,IB3,IB9
Email filtering	10.8.4	13.2.3	IB2,IB3,IB9
Incident Afhandeling	13.1.1	16.1	IB2,IB4,IB5,IB9
Auditbeleid/Audit controles	15.2.1	18.2	IB2,IB3,IB9
Mobiele apparatuur en telewerken beleid	11.7	6.2	IB1,IB2,IB4,IB7,IB9

Tabel 5 Kruisverwijzing mitigerende maatregelen en informatiebeleidsdocumenten

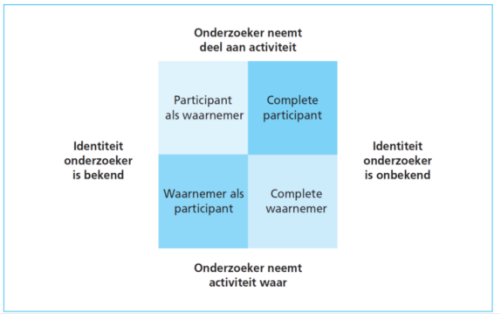
De meeste fysieke beveiligingsmaatregelen worden afgevangen door staff en physical security, dat maakt geen onderdeel van het informatiebeveiligingsbeleid maar zijn aparte onderdelen bij de onderzochte ZBO. De genoemde raamwerk-maatregelen zijn vrij basaal als het gaat om instanties die (deels) verantwoordelijk zijn voor (Europese) vitale Infrastructuren.

3.3.2. Primaire data

Als tweede zal de kennis van de medewerkers van de onderzochte ZBO in kaart gebracht moeten worden. Hun kennis op het gebied van social engineering en hun kennis van het ZBO specifieke informatiebeleid is wat gemeten moet worden om hun awareness te kunnen bepalen. Dit wordt vergeleken met de resultaten van de eerdere onderzoeken. Data over social engineering awareness van hun personeel zal verzameld moeten worden, dit is dan primaire data. Deze data wordt door middel van een enquête verzamelt zodat er een zo groot mogelijke populatie betrokken kan worden. Gestructureerde interviews zullen gebruikt worden bij de informatiebeleidsfunctionarissen om een beter beeld te kunnen krijgen van het informatiebeveiligingsbeleid.

3.3.3. Medewerker-onderzoeker

Voor het verzamelen van de benodigde data heb ik de rol van “medewerk-onderzoeker” dan wel “waarnemer als participant” genomen (Gill & Johnson, 2002). Deze rol houdt in dat ik bekend ben bij iedereen die aan dit onderzoek deelneemt en weten van het doel van dit onderzoek en zijn bewust dat ik ook, net als zij, participeer als werknemer bij deze ZBO. Figuur 1 geeft aan de typologie, hier is de aangenomen rol en de criteria die gebruikt worden binnen het kwadrant weergegeven.



Figuur 1 Typologie van de rol als participerend waarnemer. Overgenomen van Saunders et al., 2015

Ik ben sinds begin 2016 ingehuurd door een ZBO. Dit is één van de belangrijkste redenen dat dit onderzoek afgerond kon worden. De insteek was meer dan één ZBO te onderzoeken echter heeft geen andere instelling, anders dan de instelling waar ik werkzaam ben, mee willen werken. Reden voor het niet mee willen werken, wanneer er überhaupt moeite wordt gedaan om een terugkoppeling te geven, is dat er geen tijd voor is. Onderhandelen over toegang voor onderzoek is dan ook gekenmerkt als een van de moeilijkste horde voor een participerend waarnemer (Saunders et al., 2015).

Het praktische probleem van tijd dat bij deze rol vaak aanwezig is heb ik ook moeten ervaren. Gegevens die je op je werk of via je werk moet verzamelen kan je niet zelf op je werk verwerken. Bij mij kwam het dan ook op een ongelukkig moment gezien ik een aantal migraties moest uitvoeren waar harde deadlines waren gesteld en ik de materiedeskundige was binnen dit migratieteam. Elke migratiefase gaat weken tot soms een maand aan voorbereidingen in zitten. Hierdoor zijn er grote gaten ontstaan in mijn studievorderingen die pas in de vakantieperiode “dichtgelopen” konden worden. Onderhandelen om een deel van mijn werktijd aan het onderzoek te kunnen besteden (Robson, 2002) had in mijn geval geen zin omdat er gewoon de ruimte niet was. Dit was aangepakt door elke ochtend om vier uur te beginnen met onderzoekstaken waardoor ik nagenoeg geen distracties heb en flink door kan werken en later dan normaal te beginnen op mijn werk. Als je geen ochtendmens bent word je dat gewoon.

4. Uitvoering

In dit hoofdstuk wordt besproken hoe dit onderzoek daadwerkelijk is verlopen. Dit is de eerste keer dat ik daadwerkelijk een empirisch onderzoek heb uitgevoerd. Een mini (lees micro) onderzoek heb ik tijdens het schakelprogramma van de Open Universiteit gedaan en dat is zes jaar geleden. In het hoofdstuk reflectie zal ik uitgebreid mijn mening aan bod laten komen.

Scope en toestemming van deelnemende organisaties

Allereerst was uitgezocht wat het aantal ZBO's in Nederland is om de scope van het onderzoek hierop aan te passen indien nodig. De huidige lijst aan ZBO's is te vinden via het ZBO-register (https://almanak.zboregister.overheid.nl/zoeken?keyword=&submit=zoek) en ook als bijlage bij dit onderzoek. Het was meteen duidelijk dat er een afbakening plaats moet vinden om binnen het tijdsbestek van dit onderzoek te blijven. Als eerste poging is geprobeerd om ZBO's die bij een ministerie horen in kaart te brengen via rijksoverheid.nl (https://www.rijksoverheid.nl/ministeries). Deze ZBO's bleken lastig te herkennen vanuit desbetreffende ministerie homepagina's omdat niet alle ministeries aangeven welke onderdelen ZBO's zijn. Ministerie-van-infrastructuur-en-waterstaat is hier een uitzondering, op hun pagina staan alle ZBO's die onder dit ministerie vallen op een rij. Voor de andere ministeries was een kruisverwijzing met het ZBO-register nodig om dit te achterhalen. Een constatering is dat ZBO's nagenoeg nooit op hun eigen publieke pagina het logo van het desbetreffende ministerie waaronder ze vallen gebruiken. Voor dit onderzoek is gekozen voor ZBO's die onder Ministerie-van-infrastructuur-en-waterstaat vallen omdat die voldoende diverse diensten leveren en zo voldoende verschillend zijn dat dit de generaliseerbaarheid ten goede zou beïnvloeden. Tevens heeft de CSO goede contacten met een aantal en zal mij introduceren. Dit maak de kans dat ze mee willen doen met het onderzoek wat beter. Initieel was dit, op papier, een haalbare keuze.

De volgende stap was de andere ZBO's waar de CSO geen ingang voor mij had te benaderen. Twee ZBO's werden benaderd via "Cold Call". Door de telefoniste/receptioniste van de eerste is mij gevraagd een mail te sturen naar hun info mailadres. Bij de tweede heb ik mijn bedoelingen en het onderzoek uitgelegd aan de telefoniste/receptioniste waarna ik een ticketnummer kreeg en mijn email en telefoon heb achtergelaten. Ik werd een week daarna door een persoon gebeld om meer informatie te geven over het onderzoek. Achteraf zou wederom contact met mij gezocht worden. Dit is sindsdien niet meer gebeurd. Van de andere ZBO kreeg ik een email van de directeur dat het bij hen nu de drukste periode van het jaar is en dat hij zelf bereid is de enquête in te willen vullen, mits het niet veel tijd kost. De enquête door de medewerkers te laten invullen zou niet mogelijk zijn. Ik heb hem voor de zekerheid zowel de vragenlijst voor het interview als een aparte link voor de enquête gestuurd. De enquête was door hem ingevuld maar niet meegenomen in deze onderzoek.

Als "contingency plan" heb ik ook KvK (Kamer van Koophandel) en SvB (Sociale verzekeringsbank) benaderd om aan dit onderzoek mee te werken. Van KvK kreeg ik twee weken daarna een mail die mij verwees naar de HRM-beleidsadviseur die mogelijk geanonimiseerde data kon leveren maar echter wegens hun eigen planning een enquête onder de medewerkers er niet in zit. Van SvB geen enkel bericht op mijn verzoek gekregen.

Gezien de vrij teleurstellende berichten van de gevraagde ZBO's om hieraan mee te werken heb ik een beroep tot hulp gedaan bij de CSO van de ZBO die mij inhuurt. Deze heeft me in contact gebracht, via email waarbij ik in de cc stond, met twee ZBO-instellingen. Een daarvan heeft positief

gereageerd echter is het niet gelukt met hem in contact te komen (niet via email of telefonisch) voor verdere acties. De CSO van de andere organisatie heeft erg laat gereageerd met een contactpersoon die benaderd kan worden. De interviewvragen en een aparte enquête-link is verstuurd naar deze contactpersoon echter laat een reactie weer op zich wachten. Wel is de enquête ingevuld. Al met al zeer teleurstellend. Uiteindelijk bleek dat voor dit onderzoek één ZBO haalbaar is. Of dit aan het gekozen thema ligt is niet helemaal duidelijk.

Interview

Voornaamste bijdrage van de interviews voor mij was ontbrekende informatie uit de nog uit te zetten enquêtes te verkrijgen. Hoe precies de informatiebeveiliging bij de ZBO zit, waar ik informatie hiervan kan vinden en ook informatie dat alleen bij de informatiebeveiligingsfunctionarissen te krijgen is was de doelstelling. Na de interviewvragen van de voorgaande onderzoeken (Spijker, 2017) te hebben doorgenomen had ik geen behoefte om hiervan af te wijken.

Het eerste interview werd gehouden met de “Chief Security Officer” (vaak afgekort CSO of CISO) waar ik momenteel werkzaam ben. Dit interview is in een vrij vroeg stadium van het onderzoek gemaakt, dat is dan ook bewust zo gekozen om deze functionaris de eerste indruk te geven hoe dit in zijn werk gaat. Hij is de persoon die verantwoordelijk is voor het aanmaken en bijhouden van het huidige informatiebeveiligingsbeleid en het verspreiden van informatie hieromtrent. In de bijlage zijn alle interviews vastgelegd.

Tijdens het interview kreeg ik veel informatie over het informatiebeveiligingsbeleid die voor mij helemaal nieuw was ondanks dat ik al meer dan twee jaar meedraai. Vanwege de functie die ik vervul bij deze organisatie ben ik bekend met de social engineering problematiek en ben vaak ook betrokken bij het inzetten van mitigerende maatregelen op technisch vlak (antispam, deep-packet inspection etc.). Ook ben ik getuige van campagnes die gebruikt worden om bewustwording te wekken bij de medewerkers. Echter wordt er veel meer gedaan op dit gebied. In mijn geval word ik ingehuurd voor bepaalde expertise die niet aanwezig is bij organisaties, het informatiebeveiligingsbeleid dat bij deze organisaties wordt gehanteerd is niet altijd even goed bekend bij externen. Dit is dan ook één van de vraagstukken van dit onderzoek, of dat bij de meeste externen (inhuur) ook het geval is.

Bij de eerste sessie kwamen we tot de helft van de interviewvragen. Reden hiervoor was dat we tijdens deze sessie bij bepaalde thema’s bleven hangen en afdwaalden. De CSO is vrij gepassioneerd over zijn beroep en dit was mijn eerste sessie. Dit had het effect dat ik andere vragen heb gesteld om het informatiebeleid te kunnen begrijpen. Ik had helaas niet een recorder bij me op dat moment, dit was een gemiste kans om de opnames weer terug te luisteren. Maar dan had ik ook niet het nadeel dat een recorder geeft bij een interview (Saunders et al., 2015) zoals remmend effect op de antwoorden en daardoor vermindering van betrouwbaarheid.

Bij de tweede sessie heb ik me beter gehouden aan de interview-structuur en pas achteraf gingen we in op andere zaken die wel en niet gerelateerd zijn aan mijn onderzoek. De informatiebeveiligingsfunctionarissen komen wekelijks bij elkaar, dit was dan ook de doelgroep van mijn interviews. Op twee na heb ik hun input mogen innen voor dit onderzoek en strikt gehouden aan de interview vragenlijst.

Enquête

Voor de enquête heb ik Google docs gebuikt. Deze bleek alles te kunnen wat ik nodig had dus de keuze was snel gemaakt. Bij internet vragenlijsten heb je weinig controle wie dat invult en of die persoon meer dan één keer dat invult en verlaagt dus de betrouwbaarheid. Er is de mogelijkheid dit te koppelen aan een uniek veld, bijvoorbeeld emailadres van de respondent, echter maakt dit niet meer anoniem.

Ik moest er ook voor zorgen dat de manier van meten compatibel is met de manier die in de andere onderzoeken zijn gebruikt (Saunders et al., 2015). Hierdoor ben ik zoveel mogelijk bij de vorige enquête ontwerp gebleven. Immers voor content validiteit van dit onderzoek, ZBO tegen rijksoverheidsoverheidsinstelling afzetten, moet minimaal dezelfde data aanwezig zijn. Ik had achteraf gezien betrouwbaarheidstestvragen in de vorm van controlevragen in de enquête moeten toevoegen. Dit en andere wensen zullen in het hoofdstuk reflectie verder worden besproken.

Data verzameling bij deze ZBO in de vorm van een enquête kan door middel van een beroep op de gebruikers te doen via de intranetpagina. Actief iedereen benaderen via email kan alleen via de afdeling communicatie. Deze afdeling is echter lastig bereikbaar. In overleg met de CSO zijn de enquêtevragen doorlopen om het één en ander begrijpelijker te maken en samen de tekst voor op de intranetpagina af te stemmen met de link naar de enquête dat via google docs werd gepubliceerd. Er waren initieel twijfels of hier ook General Data Protection Regulation (GDPR) eisen van toepassing zijn echter heeft de CSO mij geattendeerd op het feit dat de enquête anoniem (niet herleidbaar tot een persoon) is waardoor dit niet van toepassing is.

Ook aan de CSO gevraagd wat voor informatie hij zelf wilde weten op dit thema zodat hij zijn informatiebeleid en bekendheid binnen deze organisatie zelf kan verbeteren. Hij had zelf geen eigen vragen die bij de enquête gevoegd moesten worden. Wel had hij de wens om informatie van zijn eigen organisatie uit te kunnen filteren. (In deze stadia gingen we ervan uit dat we alsnog meerdere ZBO's zouden meekrijgen voor het onderzoek). Dit bleek initieel alleen mogelijk door de gebruiker zelf aan te laten geven bij welke organisatie deze werkt gezien de enquête voor meerdere ZBO's bestemd was. We kwamen er al brainstormend achter dat als we een kopie maken van de google form en deze bij elk aparte ZBO zouden publiceren dat we de resultaten apart konden krijgen zonder interventie van de deelnemers. De resultaten van alle ZBO's konden dan achteraf samengevoegd worden om het complete beeld te krijgen.

Archiefonderzoek

De meeste informatie uit archiefonderzoek heb ik uit kunnen voeren via deskresearch. De informatiebeleidsdocumenten van de onderzochte ZBO zijn allemaal via intranet te downloaden. Het zijn wel, zoals eerder vermeld, allemaal interne documenten en kunnen helaas niet beschikbaar gesteld worden. Referentie documenten zoals BIR en ISO27001 zijn vrij verkrijgbaar via internet.

5. Resultaten

In dit hoofdstuk worden de resultaten van het onderzoek gepresenteerd als antwoorden op de deelvragen. De deelvragen die met archiefstudie werden beantwoorden zullen als eerste aan bod komen. De resterende deelvragen zijn beantwoord met data verkregen uit de enquête in combinatie met de interviews.

5.1. Archiefonderzoek

DV1: Wat is social engineering?

De definitie van social engineering, in de context van informatica, is in jaren niet veranderd. De definities die bij de eerdere onderzoeken gebruikt werden zijn nog steeds van toepassing. Hoewel tegenwoordig iedereen bepaalde social engineering aanvallen kent is de term “social engineering” zelf veel minder bekend. Dat is ook een van de constateringen uit de enquête. De meest genoemde social engineer is nog steeds Kevin Mitnick die ook een boek hierover schreef (Mitnick & Simon, 2011). Er zijn verschillende definities, dit is volgens mij de meest toepasselijke: “The use of deception in order to induce a person to divulge private information or esp. unwittingly provide unauthorized access to a computer system or network.” (OED, 2017) Zoeken naar social engineering via woordenboeken geeft vaak als eerst, en soms alleen, de definitie die gebruikt wordt bij het vakgebied sociologie. Deze term is dan ook als eerste gebruikt binnen sociologie en heeft via phreaking hackers zijn intrede gemaakt in de wereld van informatica en zijn eigen definitie gekregen (Hatfield, 2018).

DV2: Wat zijn ZBO’s?

Een zelfstandig bestuursorgaan (ZBO) is in Nederland een organisatie die overheidstaken uitvoert, maar die niet direct onder het gezag van een ministerie valt, en die als zodanig bij wet is ingesteld of aangewezen. (Wikipedia, 2018). Zelfstandige bestuursorganen behoren weliswaar tot de overheid echter vallen deze niet onder een minister. Voor ZBO’s geldt de Kaderwet Zelfstandige Bestuursorganen (overheid, 2018). Het bestaansrecht van een ZBO, volgens de kaderwet, is een orgaan waarbij deze factoren een rol spelen:
a. er behoefte is aan onafhankelijke oordeelsvorming op grond van specifieke deskundigheid;
b. er sprake is van strikt regel gebonden uitvoering in een groot aantal individuele gevallen;
c. participatie van maatschappelijke organisaties in verband met de aard van de betrokken bestuurstaak bijzonder aangewezen moet worden geacht.

Een ZBO hoeft zijn informatiebeleid niet op de BIR af te stemmen, in praktijk wordt bij de onderzochte ZBO wel degelijk rekening gehouden met de BIR.

DV3: Welke informatiebeveiligingsdocumenten zijn leidend binnen de Nederlandse Rijksoverheid en dienen ZBO’s hieraan houden?

De BIR is voor de Rijksoverheid verplicht, hierbij geldt het principe: pas toe of leg uit. (Van der Laan, 2016) De BIR:2017 is tevens de rijksimplementatie van de informatiebeveiligingsstandaarden NEN-ISO/IEC 27001 en NEN-ISO/IEC 27002. ZBO’s dienen hier niet aan te houden, dat staat vermeld in de BIR 2017.

Echter is in het verleden een taskforce van 2013 tot en met 2015 actief geweest (Taskforce BID) om bestuurders te doordringen van het belang van digitale veiligheid en hebben in 2015 een Handreiking besluitvorming implementatie BIR (CIP, 2018) uitgebracht waarin staat dat ZBO's "zich zullen gaan committeren aan een gemeenschappelijke basis door de adoptie van het VIR en de BIR, al dan niet vertaald naar hun eigen situatie".

DV 4: Wat is er in de literatuur bekend over social engineering binnen Nederlandse overheidsorganen?

Uit empirisch onderzoek is gebleken dat er een wezenlijk verschil is in de mate waarin informatiebeveiligingsbeleid is doorgevoerd binnen de Rijksoverheid en de mate waarin de medewerkers op de hoogte zijn van dit informatiebeveiligingsbeleid. Alle maatregelen waren aanwezig maar het personeel is er onvoldoende van bewust (Van der Laan, 2016). Advies om awareness van het informatiebeleid en social engineering sterk te verbeteren.
Een jaar later is weer een onderzoek naar social engineering binnen de rijksoverheid uitgevoerd, dit keer bij een ander ministerie met nagenoeg dezelfde conclusie dat awareness van eigen informatiebeveiligingsbeleid en van social engineering suboptimaal is (Spijker, 2017).
Deze twee onderzoeken hebben een concept-raamwerk gebruikt om social engineering aanvallen en de benodigde maatregelen om het gevaar van deze aanvallen in te perken gebruikt om het informatiebeveiligingsbeleid in kaart te brengen en de awareness hiervan te meten. Dit raamwerk is ook binnen dit onderzoek gebruikt om het informatiebeveiligingsbeleid en awareness van social engineering van ZBO's te analyseren.

DV8: Welke social engineering maatregelen worden op beleidsniveau direct of indirect afgedekt door het aanwezige informatiebeveiligingsbeleid binnen de ZBO's?

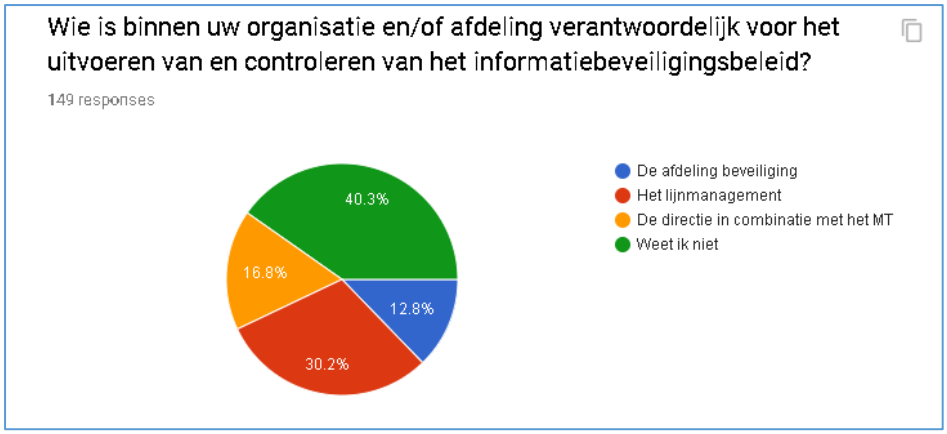
Omdat de scope beperkt bleef tot één ZBO is deze vraag beantwoord in hoofdstuk 3.4.1 waarbij het informatiebeleid samen met de BIR en ISO27001 zijn gekoppeld aan de social engineering aanvallen. Alle maatregelen die uit het raamwerk zijn afgedekt door het informatiebeveiligingsbeleid.

5.2. Enquêtes en Interviews

Van de zes ZBO's die benaderd zijn is alleen van één ZBO voldoende data ontvangen die bruikbaar is voor dit onderzoek. Hiervan zijn vier van de zes informatiebeleidsfunctionarissen geïnterviewd en 149 medewerkers hebben de enquête ingevuld.

De andere vijf ZBO's hebben of niet gereageerd, geweigerd mee te doen of slechts één respondent de enquête ingevuld. Hierdoor is er niet voldoende data om deze organisaties mee te nemen binnen dit onderzoek.

Een van de meest opvallende constateringen uit de enquête bij één ZBO is gebleken dat 40% van de deelnemers niet weet wie verantwoordelijk is voor het uitvoeren en controleren van het informatiebeveiligingsbeleid. Figuur 2 geeft hier de resultaten weer.

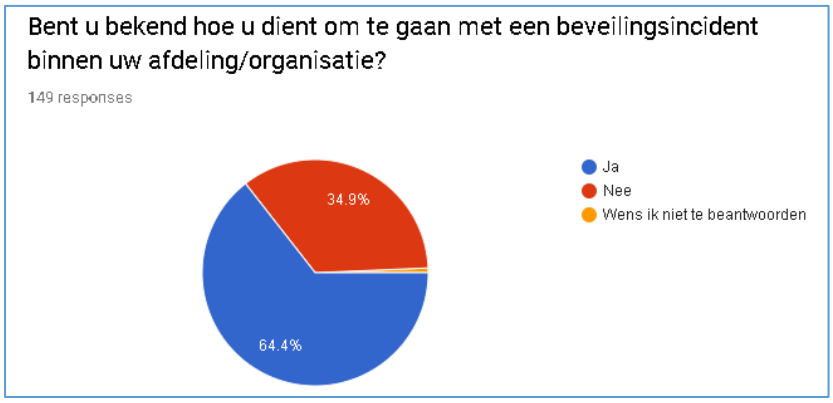


Figuur 2 Antwoord vraag verantwoordelijk IB

Eindverantwoordelijke is de directie in combinatie met het MT, echter is lijnmanagement verantwoordelijk voor het uitvoeren en controleren. Ik moet zelf eerlijk bekennen dat ik voor het starten van dit onderzoek ook niet precies wist wie hiervoor verantwoordelijk was en had wel het vermoeden dat logischerwijs het lijnmanagement hiervoor verantwoordelijk moet zijn gezien de directie en MT wat ver staan om naleving hiervan te kunnen controleren. De afdeling beveiliging bij deze ZBO zorgt voor de fysieke beveiliging echter zijn dit alleen werkzaamheden. De lijnmanager van deze afdeling, net als de andere lijnmanagers, zijn samen verantwoordelijk voor het uitvoeren en controleren van het informatiebeveiligingsbeleid. Een grote groep (bijna een derde) weet dat maar dat is nog niet de meerderheid, die groep weet het dus niet. Ook uit de interviews is gebleken dat niet alle Informatiebeleidsfunctionarissen dit weten.
Deze vraag kan ook als controlevraag gebruikt worden bij bekendheid van het informatiebeveiligingsdocument van de ZBO. Hierin staat duidelijk dat lijnmanagement verantwoordelijk is voor informatiebeveiliging.

Verder heeft meer dan 77% geen cursus/training aangeboden gekregen inzake informatiebeveiliging en 76% zouden die wel willen volgen als ze die aangeboden krijgen. Deze cijfers liggen niet ver van de twee eerdere onderzoeken. Kennelijk zou een cursus bij zowel Rijksoverheidsinstellingen als bij de onderzochte ZBO met open armen worden ontvangen.

Verder weet ongeveer 1 op de 3 deelnemers (34%) niet hoe ze met een beveiligingsincident moeten omgaan. Dit is te zien in figuur 3.

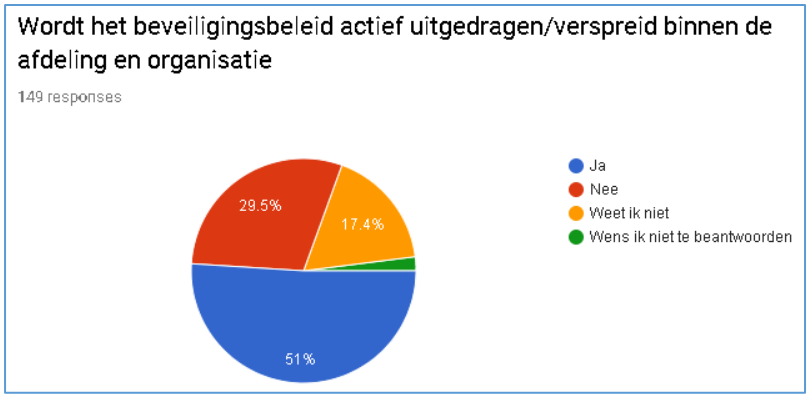


Figuur 3 Antwoord bekend om te gaan met beveiligingsincident

Op zich zou deze uitkomst alarmerend zijn echter ligt dit niet ver van wat bij de Rijksoverheid is gemeten in 2016 (39%). Meting in 2017 ligt wel 15% hoger, dit verschil dient nader onderzocht te worden.

Naar verhouding van populatie weet 45% van de deelnemers die minder dan 2 jaar in dienst zijn niet hoe ze om moeten gaan met een beveiligingsincident. Hier kan focus gelegd worden om nieuwe medewerkers extra bekend te maken met de Informatiebeleidsregels.

Ook vindt bijna één 1 op de 3 deelnemers (29%) dat de beveiligingsbeleid niet actief uitgedragen/verspreid wordt zoals is te zien in figuur 4.



Figuur 4 Antwoord op vraag IB actief uitgedragen/verspreid

Dit ligt een stuk lager dan uit het onderzoek uit 2017 (48%) doch nog steeds substantieel. Ook twee van de 12 managers (16%) die aan dit onderzoek hebben meegedaan vinden dat verspreiding van IB niet actief genoeg is, ook uit de interviews is voortgekomen dat het beter kan. Uit het onderzoek uit 2017 is ook gebleken dat 25% van de managers vinden dat het beter kan. Hier zou de ZBO gehoor aan kunnen geven.

DV 7: Zijn de medewerkers binnen ZBO bekend met de terminologie van social engineering?

DV9: Wat is de mate van awareness van de medewerkers binnen de ZBO's van het informatiebeveiligingsbeleid met betrekking tot social engineering?

DV12: In hoeverre zijn de ZBO's zelf het doelwit of slachtoffer van social engineering aanvallen?

Het begrip "social engineering" zegt bij ongeveer de helft van de medewerkers even niets maar iedereen is bekend met phishing en nagenoeg iedereen met virus en malware.

Vergelijking van het gedeelte social engineering uit de enquête met de onderzoeken van Spijker (2017) en van der Laan (2016) zijn weergegeven in tabel 6.

Social engineering vraagstuk	2018	2017	2016
Awareness			
Begrip social engineering	41%	56%	54%
Aanvalsverloop	37%	39%	39%
Motieven	42%	55%	53%
Awareness aanvaltechnieken/methoden			
Phishing	100%	100%	100%
Dumpster driving	40%	40%	18%
Office snooping	42%	40%	14%
Tailgating	49%	56%	18%
Baiting/ Item dropping	36%	39%	nvt
Malicious software	81%	79%	61%
Reverse social engineering	23%	33%	4%
Genoemde aspecten van misbruik			
Nalatigheid	65%	62%	57%
Slordigheid	71%	67%	68%
Onwetendheid	75%	84%	71%
Naïviteit	81%	79%	71%
Hebzucht	40%	49%	46%
Doelwit afgelopen 6 maanden	25%	49%	61%
Aanvalskanalen			
Email	26%	55%	57%
Telefoon	6%	9%	7%
Fysiek	0%	0%	0%
Social media	2%	13%	7%
Anders	0%	0%	0%
Geschatte kans van slagen			
Phishing Klein	30%	28%	nvt
Phishing middel	49%	59%	nvt
Phishing groot	20%	13%	nvt
Tailgaiting klein	87%	39%	nvt
Tailgaiting middel	12%	39%	nvt
Tailgaiting groot	0%	22%	nvt
Item dropping klein	24%	37%	nvt
Item dropping middel	44%	49%	nvt
Item dropping groot	31%	14%	nvt

Tabel 6 Vergelijking resultaten social engineering

Een directe vergelijking met de enquête uit het onderzoek van Nizami (2017) zoals hierboven te zien in de tabel is niet mogelijk omdat de vragenlijst grote verschillen bevat. Uit de tabel hierboven lijkt het dat SE aanvallen minder populair zijn geworden. Of dit daadwerkelijk zo is kan vervolgonderzoek hier een beter beeld scheppen. Vrijwel iedereen is bekend met phishing, dat is al jaren ook zo, wel is hieruit te lezen dat steeds meer mensen bekend worden met het gevaar van “malicious software” gezien de stijgende cijfers. Kans van tailgaiting bij de onderzochte ZBO is klein omdat er two factor wordt gebruikt, details kunnen hier niet gegeven worden vanwege beveiligingsredenen maar dit reflecteert in de cijfers van de enquête en uit de interviews. Wellicht kunnen andere rijksoverheidsinstellingen een vorm van two factor introduceren. Dat zou de kans van tailgating kunnen halveren volgens de cijfers.

Verdere bekendheid met het label/paraplu begrip “social engineering” is niet echt gestegen sinds 2016, dat is ook verwacht. Dit begrip wordt niet veel gebruikt maar voorbeelden hiervan, bijv. phishing, kent vrijwel iedereen.

DV10: Is er een verschil waarneembaar tussen de interne en externe (inhuur) medewerkers, qua bekendheid met het informatiebeveiligingsbeleid en de kennis over social engineering?

We kijken eerst naar kennis over social engineering tussen deze twee groepen. Bekendheid van het informatiebeleid (Awareness Informatiebeleid) wordt later onderzocht samen met Deelvraag 5. Hier kijken we ook of we hypothese H2 aannemen of verwerpen. We zullen hiervoor gebruik maken van statistiekprogrammatuur.

De verhouding intern en extern uit de enquête ligt niet ver van de twee eerdere onderzoeken, bij de onderzochte ZBO is een kwart van de respondenten extern. De hierboven genoemde resultaten zijn apart bekeken en zijn te lezen uit tabel 7.

Social engineering vraagstuk	Beide groepen	Intern	Extern
Awareness			
Begrip social engineering	41%	33%	64%
Aanvalsverloop	37%	30%	59%
Motieven	42%	38%	54%
Awareness aanvaltechnieken/methoden			
Phishing	100%	100%	100%
Dumpster driving	40%	38%	48%
Office snooping	42%	40%	48%
Tailgating	49%	45%	62%
Baiting/ Item dropping	36%	31%	54%
Malicious software	81%	80%	86%
Reverse social engineering	23%	20%	32%
Genoemde aspecten van misbruik			
Nalatigheid	65%	64%	70%
Slordigheid	71%	72%	67%
Onwetendheid	75%	75%	75%
Naïviteit	81%	80%	83%
Hebzucht	40%	35%	54%
Doelwit afgelopen 6 maanden	25%	9%	43%
Aanvalskanalen			
Email	26%	22%	40%
Telefoon	6%	3%	13%
Fysiek	0%	0%	0%
Social media	2%	2%	2%
Anders	0%	0%	0%
Geschatte kans van slagen			
Phishing Klein	30%	33%	24%
Phishing middel	49%	49%	48%
Phishing groot	20%	18%	29%
Tailgaiting klein	87%	88%	83%
Tailgaiting middel	12%	11%	13%
Tailgaiting groot	0%	0%	0%
Item dropping klein	24%	25%	18%
Item dropping middel	44%	41%	51%
Item dropping groot	31%	33%	32%

Tabel 7 Vergelijking resultaten SE breakdown intern/extern

Zoals hierboven is te zien ligt awareness over social engineering en de technieken bij externe medewerkers hoger dan bij interne medewerkers. Als er naar functieverdeling van internen en externen wordt gekeken zijn 48% van externe IT Specialisten vergeleken met 15% van de internen. IT-specialisten doen het beter op het gebied van social engineering kennis, dit wordt verder in een tabel gepresenteerd.

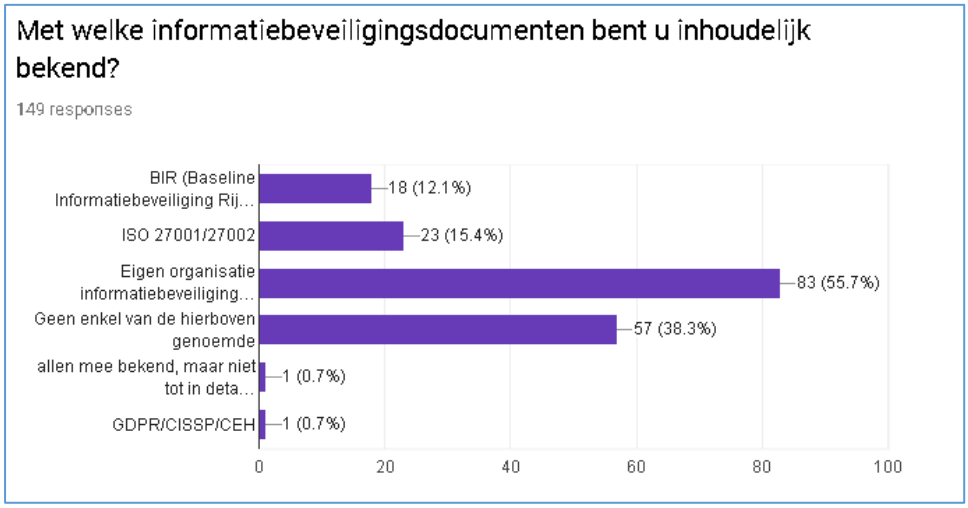
Verder wat uitspringt uit deze vergelijking is dat meer dan een derde van de externen die meededen aan dit onderzoek de afgelopen 6 maanden zelf doelwit waren van SE. Dit in vergelijking 10% minder dan de internen. Mogelijke oorzaak is dat deze specifieke populatie externen die hieraan hebben meegedaan vaker de intranetpagina van deze ZBO bezoeken. Dit is uitsluitend waar de uitnodiging tot deelname aan dit onderzoek is gepubliceerd. En juist deze groep is vaker doelwit van SE vanwege hun sociaal-digitaal gedrag welke als een belangrijke factor beschouwd kan worden bij SE-slachtoffers (Albladi & Weir, 2018). Daarentegen zijn er ook veel externen (en daar reken ik mezelf ook bij) die de intranetpagina van het bedrijf waar ze op dat moment werk voor verrichten weinig in de gaten omdat veel intranet berichten/meldingen gericht zijn aan interne medewerkers. Dit zijn dan de externen die in deze populatie ontbreekt en hebben een ander social-digitaal profiel, bijvoorbeeld hebben geen facebook account etc.

Ik had gehoopt de oproep om mee te doen aan dit onderzoek ook via email te kunnen verspreiden om zo alle type doelgroepen te kunnen bereiken, helaas is dit niet gelukt. Verder ligt het percentage van de typen aanvallen bij internen hoger dan de daadwerkelijke aanvallen, dit duidt aan dat de vraagstelling wellicht niet duidelijk genoeg was voor enkele internen.

Nader onderzoek is hier nodig, het zou interessant zijn deze cijfers met de andere twee onderzoeken te kunnen vergelijken.

DV 6: Zijn de medewerkers binnen ZBO's inhoudelijk bekend met deze informatiebeveiligingsdocumenten?

Bekendheid IB van ZBO



Figuur 5 Antwoord op vraag bekendheid IB documenten

Uit de enquête is gebleken dat meer dan de helft van de deelnemers het interne IB-document kennen zoals te zien is in figuur 5. Dit percentage is weliswaar minder dan het belangrijkste IB-document (BIR) uit het onderzoek uit 2017 maar toch hoger uit het onderzoek van 2016. Er kan gepleit worden dat de "IB-hand-outs" van 2016 een betere vergelijking is met de interne IB-documenten van dit onderzoek, hiervan is de bekendheid 64%.

Wat interessant is, is het percentage externen dat met dit IB-document bekend is. Opvallend genoeg is dit 51%. De verwachting was dat dit percentage lager zou zijn bij externen omdat deze vaak ingehuurd worden voor een bepaalde expertise (in mijn geval is dat netwerk specialisatie) om binnen een project te draaien en na afloop gaan ze naar de volgende organisatie. Hierdoor raken ze minder bekend met het IB van een organisatie en/of houden ze de berichtgeving/campagnes over IB-bekendheid niet nauwlettend in de gaten. Deze hypothese (H2) wordt ontkracht door deze cijfers. Of dit ook bij andere ZBO's of andere Rijksoverheidsinstellingen ook het geval is moet nader onderzocht worden.

DV11: Is er een verband tussen het aantal dienstjaren met awareness van SE en beleid hieromtrent binnen de ZBO?

Van de medewerkers die meer dan 5 jaar in dienst zijn kent 59% het eigen IB-document, die tussen 2 en 5 jaar in dienst zijn is dat ook 59% en bij personeel minder dan 2 jaar in dienst is dat 44%. Verwachting was dat bekendheid van het IB van een organisatie toeneemt met het aantal dienstjaren en de cijfers geven aan dat dit niet meer stijgt na 5 jaar. Tabel 8 geeft de resultaten aan als er gekeken wordt naar awareness voor deze drie groepen.

Social engineering vraagstuk	Minder dan 2 jaar	Tussen 2 en 5 jaar	Meer dan 5 jaar
Awareness			
Begrip social engineering	50%	59%	33%
Aanvalsverloop	44%	50%	31%
Motieven	36%	45%	39%
Awareness aanvaltechnieken/methoden			
Phishing	100%	100%	100%
Dumpster driving	36%	59%	38%
Office snooping	39%	59%	39%
Tailgating	42%	68%	48%
Baiting/ Item dropping	42%	45%	32%
Malicious software	81%	90%	79%
Reverse social engineering	26%	36%	19%
Informatiebeveiliging documentatie bekendheid			
BIR	18%	22%	6%
ISO27001/27002	18%	22%	7%
IB eigen organisatie	44%	59%	59%
Weet hoe om te gaan met IB incident	55%	81%	64%
Wie is verantwoordelijk voor IB			
Afdeling beveiliging	15%	18%	13%
Lijnmanagement	23%	36%	31%
Directie in combinatie met de MT	18%	13%	16%
Weet ik niet	44%	36%	39%

Tabel 8 Awareness dienstjaren breakdown

Wat opvalt is dat SE-awareness hoger ligt bij de groep die tussen 2 en 5 jaar werkt maar juist lager ligt bij de groep van meer dan 5 jaar. Ook is deze groep minder bekend met ISO27001 en BIR. Als er gekeken wordt naar de populatie van de groepen die tussen 2 en 5 jaar en meer dan 5 jaar werkzaam zijn valt het op dat de groep tussen 2 en 5 jaar voor één derde uit IT Specialisten bestaat. Die doen het beter dan de andere groepen op het gebied van SE-awareness en bekendheid van het beleid. Dit heeft een sterke invloed op de resultaten waardoor de groep tussen 2 en 5 jaar beter scoort dan de andere twee groepen. Als er een verdeling gemaakt wordt op basis van functie wordt het duidelijk hoeveel beter de IT Specialisten het doen ten opzichte van de andere groepen. Dat is te zien in tabel 9.

Social engineering vraagstuk	IT Specialist	Medewerker productgroep/ dienstverlening	Ondersteunende groep	Management	Anders
Awareness					
Begrip social engineering	82%	15%	27%	58%	34%
Aanvalsverloop	74%	21%	20%	50%	28%
Motieven	62%	31%	31%	58%	37%
Awareness aanvaltechnieken/methoden					
Phishing	100%	100%	100%	100%	100%
Dumpster driving	62%	31%	31%	50%	34%
Office snooping	62%	21%	31%	66%	45%
Tailgating	77%	28%	24%	83%	54%
Baiting/ Item dropping	62%	23%	13%	58%	37%
Malicious software	97%	78%	68%	100%	74%
Reverse social engineering	97%	7%	10%	25%	22%
Informatiebeveiliging documentatie bekendheid					
BIR	25%	2%	10%	16%	8%
ISO27001/27002	31%	0%	13%	25%	14%
IB eigen organisatie	65%	57%	51%	75%	40%
Weet hoe om te gaan met IB incident	74%	63%	65%	83%	48%
Wie is verantwoordelijk voor IB					
Afdeling beveiliging	20%	21%	10%	33%	0%
Lijnmanagement	28%	18%	34%	41%	37%
Directie in combinatie met de MT	20%	21%	17%	16%	8%
Weet ik niet	31%	42%	41%	16%	54%

Tabel 9 Awareness per functie

Verder één kanttekening bij deze cijfers is dat bij een aantal medewerkers de hoeveelheid dienstjaren minder is dan de aantal jaren die deze actief is in de huidige functie. Dat kan betekenen dat sommige respondenten of een fout hebben gemaakt bij het invullen van de enquête of hebben de vraag anders geïnterpreteerd. Bijvoorbeeld een IT Specialist kan meer dan 5 jaar deze functie hebben maar minder dat 5 jaar actief bij de huidige organisatie.

DV 5: Hoe wordt met het social engineering problematiek omgegaan bij Zelfstandig Bestuursorganen (ZBO's)?

Deze vraag is al deels beantwoord voor de onderzochte ZBO. Het bestaande informatiebeleid dekt alle maatregelen uit het raamwerk die genomen dienen te worden om de risico van social engineering aanvallen te beperken, dat is bij het voorgaande onderzoek ook het geval. Zie hiervoor de tabel in hoofdstuk 3.4.1. Een gedetailleerde uitleg van alle maatregelen en waar deze staan in het informatiebeleid en hoe deze tegenover de regels uit BIR staan voegt niet veel toe aan dit onderzoek omdat de kern van het probleem zit in awareness van deze maatregelen onder de populatie. Met deze enquête is wel vastgesteld dat bekendheid van dit beleid onder de medewerkers beter kan.

Tabel 10 laat zien de resultaten als we de beleidsmaatregelen en de awareness vergelijken met de onderzoeken uit 2016 en 2017.

Maatregel	Beleid aanwezig	Awareness beleid ZBO externen	Awareness beleid ZBO	Awareness rijksoverheid 2017	Awareness rijksoverheid 2016
Opleiding en bewustwording	Ja	29%/67%	19%/76%	16%/84%	17%
Retourneren bedrijfsmiddelen	Ja	91%	83%	73%	77%
Blockering Toegangsrechten	Ja	91%	83%	76%	89%
Informatie classificatie	Ja	67%	57%	37%	42%
Document afhandeling/vernietiging	Ja	59%	59%	51%	50%
Beperken publieke informatie	Ja	59%	73%	92%	57%
Wachtwoordmanagement	Ja	97%	96%	83%	96%
Locken van computer	Ja	75%	71%	81%	92%
Clean Desk	Ja	54%	51%	60%	96%
Antivirus/antiphishing	Ja	72%	80%	72%	71%
Incident Afhandeling	Ja	64%	64%	83%	60%
Gemiddeld 10 punten		72%	71%	70 %	73 %

Tabel 10 Overzicht beleid en awareness

De uitschieter is in geel gearceerd. Awareness onder personeel over informatieclassificatie bij de onderzochte ZBO ligt 20% hoger. Er moet verder uitgezocht worden waar dit aan ligt. Daarentegen scoort de ZBO juist lager als het gaat om beperken publieke informatie met het onderzoek uit 2017 maar toch hoger dan 2016. Data hiervoor is bij de onderzoeken verkregen met de vraag of ze in staat zijn aan te geven welke informatie vertrouwelijk is op hun afdeling. Mogelijk is het niet helemaal duidelijk bij de medewerkers wat nu precies vertrouwelijke informatie is of niet. Dit komt ook naar voren uit de interviews. Op zich hoeft dit niet persé negatief te zijn als de gebruiker bij twijfel of data vertrouwelijk of niet is om deze per definitie als vertrouwelijk te handelen.

Als we de gemiddelde awareness bekijken over de overeenkomende gemeten punten uit de drie onderzoeken, minus “opleiding/bewustwording” want data hiervan is niet geldig, dan komen we tot een gemiddelde van 71% bij de onderzochte ZBO. Hierbij kunnen we concluderen dat awareness, in grote lijnen, vergelijkbaar is tussen de onderzochte ZBO en de eerder onderzochte Rijksoverheidsinstellingen.

Als er alleen naar het deel externen uit de populatie wordt gekeken dan zijn de verschillen, op één maatregel na, maximaal 10%. Grootste verschil is “beperken van publieke informatie” wat bij externen 13% lager is dan het gemiddelde. Samenvattend scoren de externen van de 10 maatregelen die uitgevraagd worden op twee na minder dan de internen en de rest even goed of zelfs beter echter gemiddeld is er weinig verschil. Deze cijfers ontkrachten hypothese 2 dat externen minder bekend zijn met het informatiebeleid dan internen.

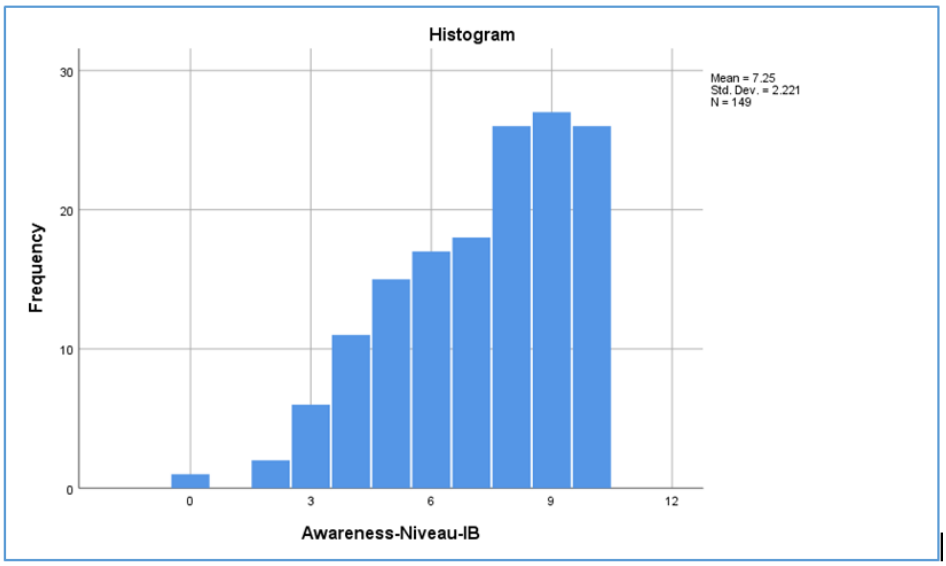
We gaan nu de focus hierop leggen en deze data statistisch analyseren met het applicatie SPSS (Statistical Package for the Social Sciences) met als doel om te kijken of er een verband is tussen type werknemer (Intern of Extern) en awareness. Vooraf is de data opgeschoond waarbij antwoorden als “weet ik niet” (non-response) werden verwijderd waardoor deze niet meetelden. De tien metingen zijn vervolgens opgeteld en dit getal geeft het awareness-niveau van het Informatiebeleid aan van

de respondent. Een “frequentie analyse” was op deze awareness niveau veld uitgevoerd om een beeld van te krijgen en te controleren of er geen fouten zijn gemaakt, dat is te zien in figuur 6.

Statistics

Awareness-Niveau-IB

N	Valid	149
	Missing	0
Mean		7.25
Range		10
Minimum		0
Maximum		10



Figuur 6 Frequentie analyse Awareness

Vervolgens is een independent samples t-test uitgevoerd om Internen en Externen met elkaar te vergelijken met de volgende hypothesen:

H0 (nulhypothese): Het gemiddelde cijfer voor Awareness is gelijk voor Internen en Externen.
HA (alternatieve hypothese): Het gemiddelde cijfer voor Awareness is niet gelijk voor Internen en Externen.

We willen met 95% (standaard bij SPSS) zekerheid kunnen zeggen dat we de nulhypothese moeten verwerpen en de alternatieve hypothese aannemen. De resultaten zijn te zien in figuur 8.

Group Statistics

	Inter-Extern	N	Mean	Std. Deviation	Std. Error Mean
Awareness-Niveau-IB	Intern	112	7.21	2.387	.226
	Extern	37	7.38	1.639	.269

Figuur 7 Group statistics Intern/extern

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means						
									95% Confidence Interval of the Difference	
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
Awareness-Niveau-IB	Equal variances assumed	10.327	.002	-.410	147	.683	-.173	.422	-1.008	.661
	Equal variances not assumed			-.492	89.811	.624	-.173	.351	-.871	.525

Figuur 8 Resultaat Independent-Samples T-Toets

We kijken eerst naar de “Levene’s test”, als de significatie kleiner of gelijk is aan 0.05 wordt ongelijke varianties gekozen. In dit geval is het 0.002, we kijken nu alleen naar de onderste rij. De t-waarde is -.492. Het verschil tussen de gemiddeldes voor Intern en Extern is -.173. We willen nu weten of dit verschil significant is. Dat is zo, als we met minimaal 95% zekerheid kunnen zeggen dat dit verschil bestaat. Dat is het geval als onder sig (2-taled) een waarde staat van .05 (5% foutkans) of lager. De waarde van .624 is veel groter dan .05 (5% kans op een fout) dus mogen we niet zeggen dat het gemiddelde cijfer voor Awareness is niet gelijk voor Internen en Externen. We waren niet voldoende overtuigd (met 95% of meer) om H0 te verwerpen en de HA aan te nemen, ofwel we nemen H0 aan

en verwerpen HA. Resumerend, het gemiddelde cijfer voor Awareness niet onderscheidbaar anders is voor Internen en Externen

We hebben bij deelvraag 11 (Is er een verband tussen het aantal dienstjaren met awareness van SE en beleid hieromtrent binnen de ZBO?) de resultaten van de drie groepen (minder dan 2 jaar, tussen 2 en 5 jaar, meer dan 5 jaar) al op social engineering awareness bekeken. Nu gaan we dat op informatiebeleid doen. Dat is weergegeven in tabel 11.

Maatregel	Awareness beleid < 2 jaar	Awareness beleid 2 -5 jaar	Awareness beleid > 5 jaar
Opleiding en bewustwording	10%/89%	44%/55%	17%/80%
Retourneren bedrijfsmiddelen	75%	94%	84%
Blockering Toegangsrechten	78%	94%	83%
Informatie classificatie	32%	66%	63%
Document afhandeling/vernietiging	50%	55%	62%
Beperken publieke informatie	57%	66%	78%
Wachtwoordmanagement	92%	94%	98%
Locken van computer	71%	83%	68%
Clean Desk	42%	77%	49%
Antivirus/antiphishing	82%	94%	77%
Incident Afhandeling	42%	77%	67%
Gemiddeld 10 punten	62 %	80%	72%

Tabel 11 Breakdown awareness in dienstjaren

Hier zien we wederom, net als bij social engineering awareness dat de populatie die tussen 2 en 5 dienstjaren op hebben het beter doen dan de rest. Bij awareness van social engineering was een groot deel van het verschil te danken aan het percentage IT-specialisten binnen deze doelgroep. Maar doen IT-specialisten het beter bij awareness van het informatiebeveiligingsbeleid? En hoe staat het dan met de andere groepen? Daar kijken we later naar, wat wel opvalt is dat deze groep veel hoger zit als het gaat om informatiebeveiliging of social engineering training die zij aangeboden hebben gekregen. Er kan een aanname gemaakt worden dat ze deze training ook hebben gevolgd. In het onderzoek uit 2017 ontbreekt de vraag of de medewerker daadwerkelijk een cursus heeft gevolgd, deze vraag was wel aanwezig in het onderzoek uit 2016. Dat betekent in feite dat op dit onderdeel zowel data uit 2017 als uit dit onderzoek niet geldig zijn voor deze maatregel, deze zijn daardoor bij berekening van de gemiddelde awareness ook niet meegenomen. Vervolgonderzoek is hiervoor nodig.

De verdeling naar functie is te zien in tabel 12.

Maatregel	IT Specialist	Medewerker productgroep/ dienstverlening	Ondersteunende groep	Management	Anders
Opleiding en bewustwording	34%/62%	7%/92%	13%/86%	33%/66%	17%/74%
Retourneren bedrijfsmiddelen	91%	84%	75%	100%	77%
Blockering Toegangsrechten	88%	84%	79%	83%	82%
Informatie classificatie	80%	50%	55%	66%	42%
Document afhandeling/vernietiging	62%	52%	72%	75%	45%

Beperken publieke informatie	68%	65%	93%	100%	60%
Wachtwoordmanagement	97%	97%	100%	100%	91%
Locken van computer	82%	68%	82%	75%	51%
Clean Desk	62%	44%	72%	66%	25%
Antivirus/antiphishing	80%	78%	82%	91%	77%
Incident Afhandeling	74%	63%	65%	83%	48%
Gemiddeld 10 punten	78%	68%	77%	83%	59%

Tabel 12 Breakdown awareness per functie

Hier zien we dat management het beter doet dan de rest en dat is ook te verwachten, immers lijnmanagent is verantwoordelijk voor het informatiemanagementbeleid in de praktijk. Maar ondanks dat IT-specialisten het beter doen dan de rest is het verschil zeer klein vergeleken met “medewerker productgroep/dienstverlener”. De “overige” groep doet het wel duidelijk slechter dan de rest en in het bijzonder als het gaat om clean desk. Uit deze groep weet slechts 1 op de 4 over deze maatregel.

6. Discussie

In dit hoofdstuk worden de drie limitaties van dit empirisch onderzoek besproken.

De **eerste limitatie** is de **representativiteit** van deze enquête steekproef. Dit onderzoek maakte gebruik van zelf selecterende steekproef (Saunders et al., 2015). Er is geen andere media gebruikt, anders dan een intranetbericht, om de aanwezigheid van de enquête onder de populatie bekend te maken. Minpunt van het benaderen van medewerkers alleen via de intranetpagina is dat je alleen de doelgroep benaderd die daadwerkelijk gebruik maakt van deze dienst. Dat zijn, ben ik bang, niet alle medewerkers maar zeker een grote groep. De enquête was door 149 personen ingevuld, dit is rond de 14% van de populatie. Deze schommelt rond de 1000 medewerkers. Dat betekent dat voor een foutmarge van 5% en een betrouwbaarheidsniveau van 95% ik bijna twee keer zoveel respondenten nodig heb. Er bestaat een kans van non-respons omdat met alleen een intranetbericht ik niet in staat was bepaalde poteniele respondenten te bereiken.

Vermoeden is (eigen ervaring) dat het percentage van externen dat de intranetpagina bezoeken lager is ten opzichte van internen. Dit zou ook een invloed kunnen hebben op de uitkomst van dit onderzoek. Bij een vervolgonderzoek zal er meerdere methodes gebruikt moeten worden zodat er geen twijfel mogelijk is dat alle medewerkers op de hoogte zijn van een enquête, voor de hand liggende methodes zijn email en intranet berichten.

De **tweede limitatie** is **te snel** de enquête uitzetten zonder goed te checken naar wat er precies wordt gevraagd (formulering) en de mogelijk antwoorden. Om het hoogste percentage aan respondenten te krijgen zou het enquêteformulier zo snel mogelijk en dan zo lang mogelijk beschikbaar zijn voor de respondenten. Ook het verwerken van data, het analyseren en presenteren kost veel tijd. Hierdoor is deze enquête, achteraf gezien, niet zorgvuldig genoeg samengesteld. Hierdoor zijn een aantal fouten onopgemerkt in de enquête achtergebleven. Deze worden nu besproken.

a. Vraag over opleiding uit de enquête had anders geformuleerd moeten worden. Er moest gevraagd of er daadwerkelijk een opleiding met betrekking tot social engineering was gevolgd, of er een opleiding werd aangeboden kan ook via interview worden verkregen. Verdere opties als “Wens ik niet te beantwoorden” is niet handig bij enquêtes, dit is equivalent aan een non-respons en moet achteraf weg gefilterd worden. Ik zie weinig toegevoegde waarde aan deze optie.
b. Controlevragen waren niet gesteld. Ik ben bewust dat hoe meer er van de respondenten gevraagd wordt dat deze mogelijk halverwege mee kappen. Echter bestaat met de huidige vraagstelling de kans van “niet-geïnformeerde respons” antwoorden (Saunders et al., 2015) omdat bij social engineering kennis en ervaring van de materie een rol spelen om niet naar antwoorden te raden. Met controlevragen, waarbij hetzelfde wordt gevraagd maar op een andere manier, kan de betrouwbaarheid hiervan verhoogd worden. Dit gaat wel ten koste van het aantal vragen en de tijd die gepaard gaat bij het invullen.

Bij een vervolgonderzoek dient er voldoende tijd aan het controleren van de enquête worden besteed en controlevragen in te bouwen om non-response te kunnen achterhalen.

De **derde limitatie** is **externe validiteit**. Van extrapoleren van dit onderzoek naar andere ZBO’s is bijna geen sprake omdat er slecht één ZBO is onderzocht en de ZBO’s onderling ook zeer divers zijn. Vervolgonderzoek met een vergelijkbaar ZBO (ook belast met beheer vitale infrastructuur en dus

ook vergelijkbaar informatiebeleidsniveau) zou een goede toets zijn en mijn advies als vervolgonderzoek. Begin in een heel vroeg stadia met contacten te leggen met ZBO's die op informatiebeveiliging vergelijkbaar niveau zitten voor een vervolgonderzoek. Externen die bij meerdere ZBO's hebben gezeten en nog contact hebben met deze werkgevers hebben een voordeel. Ervaring is dat het vrij lastig is om toestemming te krijgen van een organisatie als het gaat om informatiebeveiliging, als buitenstaander heb je nagenoeg geen kans.

7. Conclusies en aanbevelingen

In dit hoofdstuk worden de conclusies gepresenteerd waarbij de opdrachtformulering van deze scriptie wordt aangehaald samen met de twee centrale vragen. Per deelvraag wordt vervolgens een antwoord gegeven. Aan het eind van dit document worden een aantal aanbevelingen meegegeven.

7.1. Conclusies

Het doel van dit onderzoek was in kaart brengen van het informatiebeleid omtrent social engineering bij ZBO's alsmede de awareness van social engineering en het informatiebeleid bij de medewerkers. Hierbij zijn twee centrale vragen gesteld:

Hoe gaan ZBO's om met de social engineering problematiek?
Wat zijn de verschillen en overeenkomsten ten opzichte van andere rijksoverheidsinstellingen voor wat betreft het aanpakken van social engineering en awareness?

Eerst kijken we naar de resultaten van het onderzoek ten opzichte van de hypothesen, die waren:

H1: ZBO's scoren hoger qua dekkingsgraad op het gebied van SE met hun Informatiebeveiligingsbeleid vergeleken met andere Rijksoverheidsinstellingen.
H2: Er is een verschil tussen intern en extern personeel bij awareness van het informatiebeleid.

Er is slechts één ZBO onderzocht. Het informatiebeleid van de onderzochte ZBO is afgestemd op de BIR en ISO27001 net als bij de andere rijksoverheidsinstellingen. Omdat deze ZBO belast is met beheer van voor Nederland vitale infrastructuur gelden er andere beveiligingseisen dan bij sommige Rijksoverheidsinstellingen. Als alleen naar deze specifieke ZBO wordt gekeken dan is er geen merkwaardig hogere dekkingsgraad op social engineering met het informatiebeleid ten opzichte van de andere rijksoverheidsinstellingen.

Voor wat betreft hypohese twee is er geen verschil van awareness tussen Internen en externen geconstateerd. Hierbij is statistiek gebruikt om het verschil te bewijzen.

Antwoord op de onderzoeks-deelvragen worden nu gepresenteerd:
Deelvraag 5: Hoe wordt met het social engineering problematiek omgegaan bij Zelfstandig Bestuursorganen (ZBO's)?
Beleid is hierop ingericht, awareness scoort vrij laag. Ongeveer 1 op de 3 deelnemers weten niet hoe ze met een beveiligingsincident moeten omgaan en bijna 30% van de deelnemers vinden dat het beveiligingsbeleid niet actief genoeg wordt verspreid.
Deelvraag 6: Zijn de medewerkers binnen ZBO's inhoudelijk bekend met deze informatiebeveiligingsdocumenten?
Iets meer dan de helft van de medewerkers kent het informatiebeveiligingsbeleid document. Uit de tien social engineering maatregelen uit het informatiebeveiligingsbeleid die onderzocht zijn is gebleken dat bekendheid van vier daarvan onder de maat scoren.

Deelvraag 7: Zijn de medewerkers binnen ZBO bekend met de terminologie van social engineering?
Het begrip “social engineering” zegt bij ongeveer de helft van de medewerkers even niets maar iedereen is bekend met phishing en nagenoeg iedereen met virus en malware.
Deelvraag 8: Welke social engineering maatregelen worden op beleidsniveau direct of indirect afgedekt door het aanwezige informatiebeveiligingsbeleid binnen de ZBO’s?
Het geüpdatet raamwerk telt tweeëntwintig maatregelen die het gevaar van social engineering kunnen inperken. De onderzochte ZBO heeft een informatiebeleid die dit grotendeels dekt en ander beleid (fysiek en personeel) die de rest van deze maatregelen dekt.
Deelvraag 9: Wat is de mate van awareness van de medewerkers binnen de ZBO’s van het informatiebeveiligingsbeleid met betrekking tot social engineering?
Er is getoetst voor awareness op tien maatregelen binnen het informatiebeveiligingsbeleid. Er is slecht gescoord op vier gebieden: Informatie classificatie, Document afhandeling/vernietiging, Clean Desk en Incident Afhandeling.
Deelvraag 10: Is er een verschil waarneembaar tussen de interne en externe (inhuur) medewerkers, qua bekendheid met het informatiebeveiligingsbeleid en de kennis over social engineering?
Voor wat betreft bekendheid van het informatiebeveiligingsbeleid is er geen verschil tussen internen en externen. Bekendheid van social engineering ligt hoger bij externen en is mogelijk te danken aan de hoge percentage IT-specialisten die extern zijn. Hier is kennis op dit gebied hoger vergeleken met andere functies.
Deelvraag 11: Is er een verband tussen het aantal dienstjaren met awareness van SE en beleid hieromtrent binnen de ZBO?
Bij awareness van het informatiebeleid, getest op tien maatregelen, is te zien dat de awareness een fractie hoger ligt bij gebruikers die tussen twee en vijf jaar in dienst zijn en een fractie lager bij meer dan vijf jaar. Als er een verband zou zijn moeten de cijfers van de groep van vijf jaar of meer het hoogste zijn. De cijfers voor bekendheid van social engineering liggen ook hoger voor de doelgroep die werkzaam zijn tussen twee en vijf jaar en lager voor de twee andere doelgroepen.
Deelvraag 12: In hoeverre zijn de ZBO’s zelf het doelwit of slachtoffer van social engineering aanvallen?
De cijfers van social engineering aanvallen voor de laatste 6 maanden is 25%, dat is bijna de helft minder dan uit het onderzoek uit 2017. Dit is een moment opname waar niet direct een conclusie verbonden kan worden.

En de antwoorden op de twee hoofdvragen:
Hoe gaan ZBO’s om met het social engineering problematiek?
Gezien de antwoorden op de hierboven gestelde deelvragen is de conclusie dat meer aandacht besteedt moet worden aan awareness, ZBO’s doen het even slecht als rijksoverheidsdiensten.

Wat zijn de verschillen en overeenkomsten ten opzichte van andere rijksoverheidsinstellingen voor wat betreft het aanpakken van social engineering en awareness?
Er zijn nagenoeg geen verschillen, beide hebben hun informatiebeleid afgestemd op de BIR en de awareness cijfers liggen niet ver uit elkaar.

Het raamwerk dat voor de andere twee onderzoeken bij de rijksoverheid is gebruikt en de onderzoekmethodes hebben nagenoeg dezelfde resultaten opgeleverd. Ondanks dat ZBO ’s enorm kunnen verschillen heeft de onderzochte ZBO een informatiebeveiligingsbeleid dat overeenkomt

met de rijksoverheid op gebied van social engineering. Ook awareness van dit beleid en social engineering bij de medewerkers is op vergelijkbaar niveau als rijksoverheidsmedewerkers.

7.2. Aanbevelingen

7.2.1. Wetenschappelijk

Vervolgonderzoek is nodig om te kunnen achterhalen of ZBO's grote verschillen vertonen op het gebied van social engineering awareness en awareness van hun eigen informatiebeleid hieromtrent. Er is met dit onderzoek slechts één ZBO onderzocht. Advies is een andere (liefst meerdere) ZBO, die ook belast is met beheer van voor Nederland vitale infrastructuur, te onderzoeken waardoor de vergelijking met dit onderzoek eerder gemaakt kan worden.

Advies bij vervolgonderzoek is weer kritisch naar de social engineering aanvalstechnieken te kijken, social engineering problematiek blijft ontwikkelen en ook zo de methodes die kwaadwillenden gebruiken. Raamwerk dient uitgebreid te worden waar nodig om deze nieuwe aanvalstechnieken ook mee te nemen.

7.3. Praktijk

In het algemeen scoort de onderzochte ZBO op de 10 maatregelen tegen social engineering vergelijkbaar met de eerdere onderzoeken. Er zijn maatregelen die goed bekend zijn onder de medewerkers, de maatregelen die voor meer dan een derde van de medewerkers niet of niet goed bekend zijn verdienen acuut aandacht. Dit zijn:

- Informatie classificatie
- Document afhandeling/vernietiging
- Clean Desk
- Incident Afhandeling

Een awareness campagne gericht op de hierboven genoemde aspecten is een stap in de goede richting. Dit kan door middel van extra berichten te plaatsen op intranet in combinatie met hand-outs/flyers om de gebruikers hierop attent te maken.

Intranetberichten ten behoeve van informatiebeveiliging worden bij de onderzochte ZBO met regelmaat geplaatst, met de resultaten uit dit onderzoek kan er nu de focus gelegd worden op de onderdelen die het minst bekend zijn onder de werknemers. Hoe deze maatregelen toegepast worden en hoe de gebruikers hiernaar moeten handelen is beschreven in verschillende beleidsdocumenten, ervoor zorgen dat dit onder de werknemers leeft is de uitdaging.

Ook bij social engineering awareness liggen de cijfers van de ZBO niet ver van de resultaten uit de voorgaande onderzoeken. Hier dient aandacht aan besteed te worden en met name om de onderdelen waar extreem laag op wordt gescoord:

- Begrip social engineering
- Motieven
- Reverse social engineering

Hier geldt ook bekendheid van deze aspecten door middel van intranetberichten, hand-outs/flyers bij de werknemers te promoten. Ook lezingen specifiek op social engineering kan een bijdrage leveren, de onderzochte ZBO heeft dit ook al eerder georganiseerd. Advies is dit met zekere

regelmaat te doen en blijven doen. Na deze enquête is weer een campagne op het gebied van informatiebeveiliging (en dus ook social engineering) gelanceerd met een bijbehorend boekje. Het zou interessant zijn om deze enquête nog een keer te publiceren en de resultaten met een “Paired Samples T-Test” in SPSS te analyseren. Dit geeft dan inzicht in de effectiviteit van de uitgevoerde campagne.

8. Reflectie

8.1. Uitzetten onderzoek

Bij de onderzochte ZBO kon ik als enige methode een oproep doen via intranet, hierdoor heb ik mogelijk hele doelgroepen gemist. Wat ik opmerkte is dat het bericht op intranet met de vraag om hieraan mee te doen bijna meteen werd gezien door een aantal medewerkers en deze hebben binnen het uur de vragenlijst ingevuld en zelfs bericht achtergelaten dat ze naar de resultaten uitkijken. Ook spelfouten werden genoteerd en als bericht geplaatst waarna deze fouten gelijk waren hersteld. De berichten die op intranet geplaatst zijn door de gebruikers (waaronder mijn bericht) komen te staan in de volgorde van plaatsing. Na de plaatsing van mijn bericht zijn er twee andere berichten geplaatst waarna mijn bericht steeds meer naar beneden werd geschoven. Dat betekent dat de gebruikers een stukje naar beneden moet “scrollen” om deze te zien. Als tegenmaatregel kan ik dit bericht verwijderen en opnieuw plaatsen om deze weer boven aan de pagina te krijgen. Echter met deze actie worden alle reacties hierop verwijderd wat als vervelend ervaren kan worden door de medewerkers die dit met alle goede bedoelingen hebben geplaatst. Maar “het doel heiligt de middelen”. Dus om optimaal gebruik van dit medium te kunnen maken moet deze actie uitgevoerd worden als de reacties op de enquête uitdrogen. Bij elk keer dat de enquête wordt ingevuld krijg ik een mail, hierdoor is het makkelijk dit in de gaten te houden.

Waar ik als onderzoeker geen rekening mee heb gehouden is de vakantieperiode. Deze periode gaat gepaard met enorm drukte binnen het bedrijf en begint al in mei. Veel medewerkers die geen kinderen hebben, of hun kinderen al volwassen zijn, gaan al in mei op vakantie en dit gebeurt tot en met de “zomervakantie” periode waarna het alleen maar erger wordt met de bezetting omdat dan de rest van de medewerkers ook met vakantie gaan. Optimaal moet een onderzoeker al niet later dan maart beginnen met dataverzameling of pas maanden na de zomervakantie om de beste kans te maken dat bedrijven aan het onderzoek meedoen.

De situaties die de auteurs van de voorgaande onderzoeken hebben ervaren waarbij de organisaties niet gretig waren aan zo’n gevoelig onderwerp als security mee te willen werken was bij dit onderzoek ook aanwezig. De onderzochte ZBO is belast met beheer van één van de vitale infrastructuren van Nederland (Wikipedia, 2018), hierdoor is het uiterst belangrijk dat er secuur met informatie wordt omgegaan om dit niet in gevaar te brengen. Bijna elke spoor dat specifiek naar deze ZBO kan wijzen in opdracht verwijderd, ook informatie uit de interviews die naar een persoon te herleiden zijn is gecensureerd.

8.2. Analyse onderzoek

Omdat dit onderzoek een vervolgonderzoek is zou het interessant zijn om statische significaties uit te zoeken met data uit de voorgaande onderzoeken. Wellicht zijn er andere factoren die invloed hebben op zowel social engineering als informatiebeveiliging awareness. Deze data is helaas niet beschikbaar. Mijn SPSS-kennis weer op niveau brengen heeft ook wat tijd gekost, zelfs mijn Excel kennis is een beetje achteruit gegaan. Zal proberen deze twee gereedschappen wat vaker te gebruiken.

8.3. Social engineering problematiek

Het is een nobel streven om te proberen de hardnekkige problematiek van social engineering de kop in te drukken. Het is een soort van eeuwige strijd tussen materiedeskundigen/specialisten (de social engineers) en rest. Dat onbalans blijf je houden, om dit recht te trekken moet iedereen op het niveau van een social engineer gebracht worden en dat is niet te doen. Gelukkig zijn er maatregelen die ons helpen, het raamwerk gebruikt bij dit en voorgaande onderzoeken draagt een steentje bij. Echter bewustwording bij de mensen is al een uitdaging. Zowel dit onderzoek als de eerdere onderzoeken dienen als bewijs dat bewustwording niet optimaal is en ben bang dat het nooit zal worden. Ben benieuwd wat de resultaten zouden zijn als we dit onderzoek breder trekken en ook commerciële bedrijven onderzoeken. Voor de vergelijking dan wel de bedrijven meenemen die conform ISO27001 hun informatiebeleid hebben ingericht.

Een groot gemis bij dit onderzoek vind ik persoonlijk het gebrek aan betrouwbare data over opleiding die gevolgd is. Daar vallen meters te maken voor wat betreft bewustwording, effectiviteit hiervan dient gemeten te worden om de trainingen hierop aan te passen. Ik heb deze fout pas ontdekt nadat de enquête al gepubliceerd was. Ik had meer tijd moeten nemen bij voorbereiding van de enquête echter zat ik in tijdsdruk en deze kreeg een hogere prioriteit.

8.4. Opleiding

Wegens persoonlijke omstandigheden is de doorlooptijd van deze opleiding voor mij vrij lang geweest. Ik ben begonnen toen deze opleiding volledig zelfstudie was, naderhand is er een begeleide variant in het leven geroepen en ben ik daar ingestroomd. Ondanks dat er verschillende modules afgelegd moesten worden, individueel of in groepsverband, waar rapporten samengesteld moesten worden valt het niet mee om een empirisch onderzoeksrapport te schrijven. Het schakelprogramma zorgt dat studenten de nodige bagage krijgen om zo'n rapport te maken maar dat was bij mij zes jaar geleden dat ik dit programma had voltooid. Om uit te zoeken "hoe het nou precies zat" heeft me heel veel tijd gekost. Ik had veel eerder met de voorbereiden moeten starten. Verder heb ik veel respect voor onderzoekers, dit is officieel mijn eerste empirisch onderzoek en heb enorm veel geleerd.

Referenties

Schoofs, P. (2014). Phishing bij de overheid in België (Master's thesis, Open Universiteit Nederland).

Spijker, D. (2017). Social engineering binnen de Nederlandse Rijksoverheid (Master's thesis, Open Universiteit Nederland).

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

BIR. (2017). Baseline Informatiebeveiliging Rijksdienst Opgehaald van https://www.earonline.nl/images/earpub/d/d3/BIR2017_definitief_20171130.pdf

Saunders, L. T. (2015). Methoden en technieken van onderzoek, 7e Editie. Amsterdam: Pearson.
Robson, C. (2002). Real world research (Vol. 2). Malden, MA: Blackwell.

Wikipedia. (2018). Social engineering.
Opgehaald van https://nl.wikipedia.org/wiki/Social_engineering_(informatica)

Wikipedia (2018). Vitale infrastructuur.
Opgehaald van https://nl.wikipedia.org/wiki/Vitale_infrastructuur

Wikipedia (2018). Zelfstandig bestuursorgaan
Opgehaald van https://nl.wikipedia.org/wiki/Zelfstandig_bestuursorgaan

Overheid (2018) Kaderwet zelfstandige bestuursorganen
Opgehaald van http://wetten.overheid.nl/BWBR0020495/2015-01-01

Gill, J., & Johnson, P. (2010). Research methods for managers. Sage.

Chiew, K. L., Yong, K. S. C., & Tan, C. L. (2018). A survey of phishing attacks: their types, vectors and technical approaches. Expert Systems with Applications.

Albladi, S. M., & Weir, G. R. (2018). User characteristics that influence judgment of social engineering attacks in social networks. Human-centric Computing and Information Sciences, 8(1), 5.

Ohaya, C. (2006, September). Managing phishing threats in an organization. In Proceedings of the 3rd annual conference on Information security curriculum development (pp. 159-161). ACM.

Heartfield, R., & Loukas, G. (2016). A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks. ACM Computing Surveys (CSUR), 48(3), 37.

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

Social engineering OED Online. (2017). Oxford University Opgehaald van: http://www.oed.com/view/Entry/272695?redirectedFrom=social+engineering

Hatfield, J. M. (2018). Social engineering in cybersecurity: The evolution of a concept. Computers & Security, 73, 102-113.

CIP (2018) Handreiking besluitvorming implementatie BIR Opgehaald van: https://www.cip-overheid.nl/wp-content/uploads/2018/01/Handreiking-besluitvorming-implementatie-BIR-voor-ZBOs-1.0.pdf

2018 Data Breach Investigations Report | Verizon Enterprise Solutions. (z.d.). Geraadpleegd van https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf

Bijlage 1 Interview vragen

Interview m.b.t social engineering binnen ZBO's

Algemene vragen

1. *Wat is uw rol als IB functionaris (IBF) en kunt u deze in het kort omschrijven?*
   Gecensureerd
2. *Hoeveel jaar bent u in dienst en hoeveel jaar vervult u de IBF rol voor uw afdeling?*
   5 jaar
3. *Hoeveel medewerkers telt uw afdeling?*
   Gecensureerd
4. *Bent u een interne medewerker of externe?*
   Intern

Informatiebeveiligingsbeleid

5. *Hoe wordt binnen deze organisatie omgegaan met informatiebeveiliging. Hoe wordt dit vastgelegd?*
   Dit is procedureel vastgelegd.
6. *Hoe verhoudt het informatiebeveiligingsbeleid zich tot de BIR / ISO 27001 normering?*
   BIR is geschreven volgens ISO 27001 (PDCA) en ISO 27002 (controls), daar is IB van deze organisatie op gebaseerd.
7. *Zijn er directe of indirecte informatiebeveiligingsmaatregelen tegen social engineering vastgelegd in het huidige informatiebeleid van uw organisatie? Kunt u hiervan een voorbeeld geven?*
   IB staat bewustwording bij mensen, en er wordt actief geacteerd op spam/phishing. Zie beleid hoofdstuk 12.2
8. *Wat is waardevolle informatie voor uw organisatie? Weten uw manager en de medewerkers dat? Is er binnen de organisatie bekend welke informatie het belangrijkst is?*
   In principe is alle informatie waardevol
   Zie over dataprivacy en informatiebeveiliging op intranet. Hier staat dit beschreven.

9. *Hoe gaat men binnen de organisatie om met het verwijderen van vertrouwelijke gegevens en/of documenten?*
   Deze organisatie heeft een gesloten container op elk verdieping. Er is afgesproken hoe lang Elektronisch data bewaard moet worden en wanneer dit vernietigd moet worden.

10. *Worden medewerkers gescreend voordat deze aangenomen, op welke zaken?*
    Ja, screening B. Minimaal VOG, medewerkers die op het platform op <gecensureerd>l werken hebben een BL screening van AIVD. <gecensureerd> of andere medewerkers die zelfstandig bepaalde ruimtes in moeten (hw zaal, operationeel zal) hebben een B screening. 4 mensen hebben een A screening, omdat deze in aanraking kunnen komen met staatsgeheim.

11. *Is er bij het beëindigen van een dienstverband controle op het retourneren van bedrijfsapparatuur, toegangspassen en het afsluiten van voorzieningen?*
    Ja, procedureel is dit vastgelegd.

12. *Hoe wordt omgegaan met een beveiligingsincident binnen uw afdeling/organisatie? Hoe worden incidenten afgewikkeld? Wordt er een incidentrapport opgemaakt na een beveiligingsinbreuk?*
    Dit is ook procedureel vastgelegd.

13. *Wie is binnen uw organisatie en/of afdelingen verantwoordelijk voor het uitvoeren en controleren van het informatiebeveiligingsbeleid?*
    Lijnmanager is verantwoordelijk voor het uitvoeren, CSO is voor het opstellen en up to date houden van het beleid, bestuur is eindverantwoordelijk.

14. *In hoeverre is uw directe lijnverantwoordelijke van uw organisatie betrokken bij het informatiebeveiligingsbeleid?*
    Direct verantwoordelijke heeft het beleid getekend, zie beleidsstuk.

15. *Worden er risico analyses gemaakt op het informatiebeveiligingsbeleid? Wie is hier verantwoordelijk voor? Hoe vaak worden deze gemaakt?*
    Ja, er worden analyses gemaakt volgens het informatiebeveiligingsbeleid, niet op de beleid. Er wordt geacteerd op actuele dreigingen, bijv van bericht uit de media, partners, meldingen van Nationaal Cyber Security Centrum (NCSC). CSO is verantwoordelijk voor. Er is intern een methodiek ontwikkeld om dreigingen te classificeren.

16. *Wordt het beveiligingsbeleid uitgedragen/verspreid binnen de afdeling en organisatie? Wordt op alle afdelingen het beleid op dezelfde manier uitgedragen?*
    Ja, staat op intranet. Maak intranet berichten, spam campagnes, organiseer sprekers, Cybersecurity game, etc. Het is nog niet bekend of elk afdeling ook acties ondernemen.

17. *Is er het afgelopen jaar een controle/audit uitgevoerd op de beveiligingsbeleidspunten?*
    Ja, er is een audit geweest.

Social engineering

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

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

Definitie B: "Social engineering is een aanvalstechniek waarbij de aanvaller probeert informatiesystemen te hacken door de zwakste schakel in de informatiebeveiliging, namelijk de mens, te manipuleren. Hierbij wordt misbruik gemaakt van menselijke eigenschappen als nieuwsgierigheid, vertrouwen en hebzucht, om daarmee het slachtoffer een bepaalde handeling uit

te laten voeren of vertrouwelijke informatie te verkrijgen, waardoor de aanvaller dichter bij het aan te vallen informatiesysteem kan komen."

Social engineering – sociale technieken gebruiken om informatie gewonnen om te hacken of in te breken. Social engineering is breder dan dat, kern is social engineering gericht op personen en niet techniek.

19. *Kunt u beschrijven hoe een social engineeringaanval in zijn werk gaat?*
    Algemene info inwinnen, wat kan ik over de persoon vinden. Eerst doelwit bepalen. Dus wie is de doel,wat kan ik vinden over de persoon en hoe kan ik benaderen. Dan voordoen al een vertrouwd persoon om informatie te krijgen.

20. *Welke motieven zou een social engineer kunnen hebben?*
    Financieel motief, geld
    Kan ook zijn terroristische motieven, bedrijfsgeheim. Motieven zijn legio, dus kan ook social engineering.

21. *Bent u in staat om een aantal verschillende social engineeringsaanvallen te beschrijven?*
    -phisching
    -bellen als iemand van helpdesk
    - tailgaiting
    -voordoen als verkoper om zo binnen te komen
    - onderzoek over persoon (iemand)

22. *Waar maakt een social engineer misbruik van?*
    Vertrouwen en onoplettendheid van de mens. Vertrouwen winnen, dan niet meer opletten. Het feit dat mensen graag wil communiceren en delen.
23. *Ziet u vanuit uw eigen medewerkers en/of externe partijen bedreigingen binnen de organisatie?*
    De mens is altijd de zwaarste schakel. Eigen medewerker -> risico
    Externe partijen -> bedreigingen, bijv nsc geeft aan dat externe partijen op zoek gaan naar data. Nu geen concreet bedreiging.
    CEO fraude, die stuurt een mail uit naam van de ceo om geld over te maken. Mail komt vanaf extern. Spearfishing.

24. *Zijn er recent incidenten geweest rondom social engineeringsaanvallen? Via welk (communicatie)kanaal werd deze poging ondernomen?*
    Ceo fraude via email.

25. *Is naar uw mening uw organisatie voldoende op de hoogte/bewust van social engineering?*
    Kan altijd beter. Maria Genova een lezing laten doen, nog een organiseren binnenkort. Dit komt deels door samenwerking met partners.

26. *Is naar uw mening uw organisatie momenteel voldoende beschermd tegen social engineeringsaanvallen? Welke verbeteringen kunnen worden doorgevoerd?*
    Op technisch doel wel, bewustwording kan beter.

27. *Wat zijn de mogelijke gevolgen voor de organisatie als vertrouwelijke informatie op straat komt te liggen?*
    Met name reputatieschade

Financiële schade door boetes als persoonsgegeven op straat komt te liggen
De operatie kan verstoren als met de gegevens schade aangericht kunnen worden.

28. *Hoe groot is de kans dat een medewerker in een phishing mailt trapt?*
    De kans is aanwezig en naar eigen zegge is een goede spearfishing mail lastig te herkennen bij een doorsnee medewerker. Voorbeeld is verkeersboetes, zie recente berichten.

29. *Hoe groot is de kans dat een persoon het gebouw binnenkomt als deze zelf geen toegang heeft?*
    Nul, dat is een keer geprobeerd zonder succes.

30. *Hoe groot is de kans dat wanneer een medewerker een data medium (USB stick, cdrom) vindt, deze ook daadwerkelijk bekijkt?*
    Nooit geprobeerd, dit moeten we een keer doen. Fishme tool uitzoeken.

31. *Weet je welke trends er spelen op het gebied van social engineering?*
    Verkeersboetes, ceo fraude, admin fraude -> gebeld door iemand die zich als een " collega" zich voordoet en vragen om een poortje open te zetten op de firewall naar buiten en dat het snel moet omdat het dringend is, procedure komt later nog. Bij een partner is dat gebeurd. (dus Firewall hacking via social engineering)

32. *Reageert de organisatie snel genoeg op nieuwe ontwikkelingen, in dit geval social engineering. Is het een nieuwe ontwikkeling?*
    Nee de organisatie reageert niet snel genoeg maar is wel snel genoeg in geval van nood.

Algemene vragen

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

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

3. *Hoeveel medewerkers telt uw afdeling?*
   Gecensureerd

4. Bent u een interne medewerker of externe?
   Extern

Informatiebeveiligingsbeleid

5. *Hoe wordt binnen deze organisatie omgegaan met informatiebeveiliging. Hoe wordt dit vastgelegd?*
   Er zijn verschillende processen en richtlijnen en er wordt met regelmaat gecommuniceerd op intranet. Daarnaast is er iedere 2 weken een securityoverleg.

6. *Hoe verhoudt het informatiebeveiligingsbeleid zich tot de BIR / ISO 27001 normering?*
   Geen idee

7. *Zijn er directe of indirecte informatiebeveiligingsmaatregelen tegen social engineering vastgelegd in het huidige informatiebeleid van uw organisatie? Kunt u hiervan een voorbeeld geven?*
   Communicatie en awareness. Er worden regelmatig kennissessies gegeven over verschillende onderwerpen.

8. *Wat is waardevolle informatie voor uw organisatie? Weten uw manager en de medewerkers dat? Is er binnen de organisatie bekend welke informatie het belangrijkst is?*
   Er zijn altijd documenten die niet op straat mogen belanden. Tekeningen, ontwerpen en processen over de netwerkinfrastructuur. Alle medewerkers binnen het team zijn bijzonder "aware" van de situatie.

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

10. *Worden medewerkers gescreend voordat deze aangenomen, op welke zaken?*
    Ja, AIVD B-Screening

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

12. *Hoe wordt omgegaan met een beveiligingsincident binnen uw afdeling/organisatie? Hoe worden incidenten afgewikkeld? Wordt er een incidentrapport opgemaakt na een beveiligingsinbreuk?*
    Er moet direct een melding gedaan worden bij de manager en de security officer. Ernstige voorvallen worden achteraf besproken in het security overleg

13. *Wie is binnen uw organisatie en/of afdelingen verantwoordelijk voor het uitvoeren en controleren van het informatiebeveiligingsbeleid?*
    Formeel iedereen, in de praktijk is het vaak toch vooral de security officer

14. *In hoeverre is uw directe lijnverantwoordelijke van uw organisatie betrokken bij het informatiebeveiligingsbeleid?*
    Goede netwerkbeveiliging draagt bij aan informatiebeveiliging in het geheel. Als lijnverantwoordelijke zie ik er op toe dat veiligheid geborgd blijft. Verder zit in 2 wekelijks securityoverleg

15. *Worden er risico analyses gemaakt op het informatiebeveiligingsbeleid? Wie is hier verantwoordelijk voor? Hoe vaak worden deze gemaakt?*
    Er worden regelmatig audits gedaan door externe partijen. Maar de analyses kunnen ook komen vanuit de werkvloer zelf.

16. *Wordt het beveiligingsbeleid uitgedragen/verspreid binnen de afdeling en organisatie? Wordt op alle afdelingen het beleid op dezelfde manier uitgedragen?*
    Er wordt veel gebruik gemaakt van het Intranet voor het delen van het beveiligingsbeleid.

17. *Is er het afgelopen jaar een controle/audit uitgevoerd op de beveiligingsbeleidspunten?*
    Ja, er is een audit geweest op diverse onderdelen binnen de netwerkinfrastructuur

Social engineering

18. *Wat verstaat u onder social engineering? Wat is de kern hiervan? Kunt u zich vinden in de volgende definities van social engineering?*
    Ja, Definitie A sluit goed aan bij mijn beeld.

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

Definitie B: "Social engineering is een aanvalstechniek waarbij de aanvaller probeert informatiesystemen te hacken door de zwakste schakel in de informatiebeveiliging, namelijk de mens, te manipuleren. Hierbij wordt misbruik gemaakt van menselijke eigenschappen als nieuwsgierigheid, vertrouwen en hebzucht, om daarmee het slachtoffer een bepaalde handeling uit

te laten voeren of vertrouwelijke informatie te verkrijgen, waardoor de aanvaller dichter bij het aan te vallen informatiesysteem kan komen."

19. *Kunt u beschrijven hoe een social engineeringaanval in zijn werk gaat?*
    Aanval op personen, in alle lagen van de organisatie, om informatie los te krijgen.

20. *Welke motieven zou een social engineer kunnen hebben?*
    Motieven kan van alles zijn. Van een beroepshacker tot een scriptkiddie. Andere motivatie zou een penetratietest / audit kunnen zijn

21. *Bent u in staat om een aantal verschillende social engineeringsaanvallen te beschrijven?*
    Per telefoon, per mail, face-2-face, social media.

22. *Waar maakt een social engineer misbruik van?*
    Alles wat binnen zijn of haar bereik ligt. Per telefoon, per mail, face-2-face, social media

23. *Ziet u vanuit uw eigen medewerkers en/of externe partijen bedreigingen binnen de organisatie?*
    Binnen eigen afdeling niet, binnen de organisatie misschien. Maar niet waarschijnlijk.

24. *Zijn er recent incidenten geweest rondom social engineeringsaanvallen? Via welk (communicatie)kanaal werd deze poging ondernomen?*
    Buiten de standaard mailtjes en telefoontjes geen bijzondere incidenten

25. *Is naar uw mening uw organisatie voldoende op de hoogte/bewust van social engineering?*
    Zeker, er wordt regelmatig informatie geplaatst op intranet. Tevens de kennissessie dragen bij aan de awareness

26. *Is naar uw mening uw organisatie momenteel voldoende beschermd tegen social engineeringsaanvallen? Welke verbeteringen kunnen worden doorgevoerd?*
    100% sluitend krijg je het nooit, er zijn altijd mensen binnen een organisatie die a-technisch zijn of gewoon naïef. Als verbetering zou ik vooral nog meer blijven communiceren en zorgdragen voor steeds meer bewustwording.

27. *Wat zijn de mogelijke gevolgen voor de organisatie als vertrouwelijke informatie op straat komt te liggen?*
    Moeilijk te overzien, afhankelijk van welke informatie op straat komt. Reputatieschade is denk ik wel een belangrijke.

28. *Hoe groot is de kans dat een medewerker in een phishing mailt trapt?*
    Binnen de afdeling 0%, binnen de organisatie hopelijk kleiner dan 20%

29. *Hoe groot is de kans dat een persoon het gebouw binnenkomt als deze zelf geen toegang heeft?*
    Zeer klein i.v.m. biometrische beveiliging

30. *Hoe groot is de kans dat wanneer een medewerker een data medium (USB stick, cdrom) vindt, deze ook daadwerkelijk bekijkt?*
    Binnen de afdeling 0%, binnen de organisatie hopelijk kleiner 20%

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

32. *Reageert de organisatie snel genoeg op nieuwe ontwikkelingen, in dit geval social engineering. Is het een nieuwe ontwikkeling?*
    De afdelingen security en architectuur zijn goed op de hoogte echter is het binnen de organisatie erg moeilijk om veranderingen door te voeren. Dit kan ver gaan en soms zelfs ten koste van de veiligheid.

Algemene vragen

1. *Wat is uw rol als IB functionaris (IBF) en kunt u deze in het kort omschrijven?*
   Gecensureerd
2. *Hoeveel jaar bent u in dienst en hoeveel jaar vervult u de IBF rol voor uw afdeling?*
   Gecensureerd
3. *Hoeveel medewerkers telt uw afdeling?*
   Gecensureerd
4. Bent u een interne medewerker of externe?
   intern

Informatiebeveiligingsbeleid

5. *Hoe wordt binnen deze organisatie omgegaan met informatiebeveiliging. Hoe wordt dit vastgelegd?*
   Informatie beveiligingsbeleid is de basis
6. *Hoe verhoudt het informatiebeveiligingsbeleid zich tot de BIR / ISO 27001 normering?*
   Deze is afgeleid van de ISO 270001
7. *Zijn er directe of indirecte informatiebeveiligingsmaatregelen tegen social engineering vastgelegd in het huidige informatiebeleid van uw organisatie? Kunt u hiervan een voorbeeld geven?*
   Volgens mij niet, ken geen voorbeeld
8. *Wat is waardevolle informatie voor uw organisatie? Weten uw manager en de medewerkers dat? Is er binnen de organisatie bekend welke informatie het belangrijkst is?*
   Vanuit Gecensureerd is o.a. ontwerpdocumentatie en netwerkinfra belangrijke info, maar ook hoe de beveiliging in elkaar zit
9. *Hoe gaat men binnen de organisatie om met het verwijderen van vertrouwelijke gegevens en/of documenten?*
   N.v.t binnen mijn afdeling
10. *Worden medewerkers gescreend voordat deze aangenomen, op welke zaken?*
    Meestal met een VOG. En in sommige gevallen een AIVD onderzoek
11. *Is er bij het beëindigen van een dienstverband controle op het retourneren van bedrijfsapparatuur, toegangspassen en het afsluiten van voorzieningen?*
    ja
12. *Hoe wordt omgegaan met een beveiligingsincident binnen uw afdeling/organisatie? Hoe worden incidenten afgewikkeld? Wordt er een incidentrapport opgemaakt na een beveiligingsinbreuk?*
    Er is een proces voor. Dat lijkt op het <gecensureerd> ernstige verstoringen
13. *Wie is binnen uw organisatie en/of afdelingen verantwoordelijk voor het uitvoeren en controleren van het informatiebeveiligingsbeleid?*
    De CSO
14. *In hoeverre is uw directe lijnverantwoordelijke van uw organisatie betrokken bij het informatiebeveiligingsbeleid?*
    Ik heb veel contact met de CSO.
15. *Worden er risico analyses gemaakt op het informatiebeveiligingsbeleid? Wie is hier verantwoordelijk voor? Hoe vaak worden deze gemaakt?*
    Op afdelingsniveau vinden deze analyses plaats. Worden een keer gemaakt. Dit omdat ze ook moeten vanwege veiligheidswetgeving. Het is onderzoek naar uitval van functies en het effect op het operationele proces.
16. *Wordt het beveiligingsbeleid uitgedragen/verspreid binnen de afdeling en organisatie? Wordt op alle afdelingen het beleid op dezelfde manier uitgedragen?*

Kan beter

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

Social engineering

18. *Wat verstaat u onder social engineering? Wat is de kern hiervan? Kunt u zich vinden in de volgende definities van social engineering?*
    Iemand die middels contact (email, telefoon) zich voordoet als iemand met enig relevant functie en zich op die manier informatie of zelfs toegang verschaft.

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

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

19. *Kunt u beschrijven hoe een social engineeringaanval in zijn werk gaat?*
    Hallo met Piet van bedrijf X, ik merk dat PC y het niet doet (het nummer is 2435, die Piet heeft gevonden op een foto op de website van deze organisatie). Kunt u de firewal even opzetten dan kan ik kijken wat er aan de hand is (o.i.d).
20. *Welke motieven zou een social engineer kunnen hebben?*
    Hacken of financiële motieven
21. *Bent u in staat om een aantal verschillende social engineeringsaanvallen te beschrijven?*
    nee
22. *Waar maakt een social engineer misbruik van?*
    Geen idee
23. *Ziet u vanuit uw eigen medewerkers en/of externe partijen bedreigingen binnen de organisatie?*
    nee
24. *Zijn er recent incidenten geweest rondom social engineeringsaanvallen? Via welk (communicatie)kanaal werd deze poging ondernomen?*
    Geen idee
25. *Is naar uw mening uw organisatie voldoende op de hoogte/bewust van social engineering?*
    nee
26. *Is naar uw mening uw organisatie momenteel voldoende beschermd tegen social engineeringsaanvallen? Welke verbeteringen kunnen worden doorgevoerd?*
    Nee, Bewustwording verhogen
27. *Wat zijn de mogelijke gevolgen voor de organisatie als vertrouwelijke informatie op straat komt te liggen?*
    Imago schade

28. *Hoe groot is de kans dat een medewerker in een phishing mailt trapt?*
    Kans is aanwezig
29. *Hoe groot is de kans dat een persoon het gebouw binnenkomt als deze zelf geen toegang heeft?*
    klein
30. *Hoe groot is de kans dat wanneer een medewerker een data medium (USB stick, cdrom) vindt, deze ook daadwerkelijk bekijkt?*
    Alles is encrypted tegenwoordig ,dus kans is klein
31. *Weet je welke trends er spelen op het gebied van social engineering?*
    Geen idee
32. *Reageert de organisatie snel genoeg op nieuwe ontwikkelingen, in dit geval social engineering. Is het een nieuwe ontwikkeling?*
    Redelijk

Algemene vragen

1. *Wat is uw rol als IB functionaris (IBF) en kunt u deze in het kort omschrijven?*
   Gecensureerd
2. *Hoeveel jaar bent u in dienst en hoeveel jaar vervult u de IBF rol voor uw afdeling?*
   Gecensureerd
3. *Hoeveel medewerkers telt uw afdeling?*
   Gecensureerd
4. Bent u een interne medewerker of externe?
   Intern.

Informatiebeveiligingsbeleid

5. *Hoe wordt binnen deze ZBO omgegaan met informatiebeveiliging. Hoe wordt dit vastgelegd?*
   Er is beleid en er is een <Branchespecifiek>: het <brachespeciefiek> Security Management Systeem
6. *Hoe verhoudt het informatiebeveiligingsbeleid zich tot de BIR / ISO 27001 normering?*
   Het beleid is gebaseerd op regelgeving vanuit <brancheorganisaie>, Europese en Nederlandse wet- en regelgeving, zoals de BIR en VIR-BI. Het beleid is opgebouwd volgens de ISO27002-norm.
7. *Zijn er directe of indirecte informatiebeveiligingsmaatregelen tegen social engineering vastgelegd in het huidige informatiebeleid van uw organisatie? Kunt u hiervan een voorbeeld geven?*
   Ik weet niet of het vastgelegd is, maar via Intranet en voorlichtingsbijeenkomsten wordt het bij medewerkers onder de aandacht gebracht.
8. *Wat is waardevolle informatie voor uw organisatie? Weten uw manager en de medewerkers dat? Is er binnen de organisatie bekend welke informatie het belangrijkst is?*
   Die informatie die nodig is om "ons werk" (<branche>) uit te kunnen voeren. Daarnaast aanbestedingsdocumenten en natuurlijk (systeem) documentatie. We kennen een Leidraad Rubricering waarin uiteengezet is wat Geheim, Vertrouwelijk, Intern en Publiek is. Binnen de organisatie is, afhankelijk van de plek in de organisatie, een groot verschil in wat daar 'waardevol' wordt genoemd; ik denk niet dat er iemand is die 'waardevol' voor de hele organisatie kan beantwoorden.
9. *Hoe gaat men binnen de organisatie om met het verwijderen van vertrouwelijke gegevens en/of documenten?*
   Documenten worden afgevoerd via afgesloten blauwe bakken van een gecertificeerd bedrijf. Informatiedragers kunnen op deze manier ook afgevoerd worden.
10. *Worden medewerkers gescreend voordat deze aangenomen, op welke zaken?*
    Jazeker. Minimaal een VOG (Verklaring Omtrent Gedrag). Voor personen die een vertrouwensfunctie vervullen is een Verklaring van Geen Bezwaar (VGB) nodig. Om deze te verkrijgen wordt door de AIVD een veiligheidsonderzoek-B voor de <branchespecifiek> uitgevoerd.
11. *Is er bij het beëindigen van een dienstverband controle op het retourneren van bedrijfsapparatuur, toegangspassen en het afsluiten van voorzieningen?*
    Ja.
12. *Hoe wordt omgegaan met een beveiligingsincident binnen uw afdeling/organisatie? Hoe worden incidenten afgewikkeld? Wordt er een incidentrapport opgemaakt na een beveiligingsinbreuk?*
    Binnen Gecensureerd is er een "Werkwijze afhandeling Security incidenten", te vinden bij de Work Instructions in de SSF.

13. *Wie is binnen uw organisatie en/of afdelingen verantwoordelijk voor het uitvoeren en controleren van het informatiebeveiligingsbeleid?*
    De manager van de afdeling is verantwoordelijk. Hij/zij wordt aangestuurd door de CISO en voor Gecensureerd door de Gecensureerd
14. *In hoeverre is uw directe lijnverantwoordelijke van uw organisatie betrokken bij het informatiebeveiligingsbeleid?*
    Hij heeft frequent, regelmatig security-overleg met de CISO.
15. *Worden er risico analyses gemaakt op het informatiebeveiligingsbeleid? Wie is hier verantwoordelijk voor? Hoe vaak worden deze gemaakt?*
    Ja. De CISO en zijn team. Frequentie weet ik niet.
16. *Wordt het beveiligingsbeleid uitgedragen/verspreid binnen de afdeling en organisatie? Wordt op alle afdelingen het beleid op dezelfde manier uitgedragen?*
    Eerst vraag: ja. Tweede vraag: ongetwijfeld niet. Helaas.
17. *Is er het afgelopen jaar een controle/audit uitgevoerd op de beveiligingsbeleidspunten?*
    Ja.

Social engineering

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

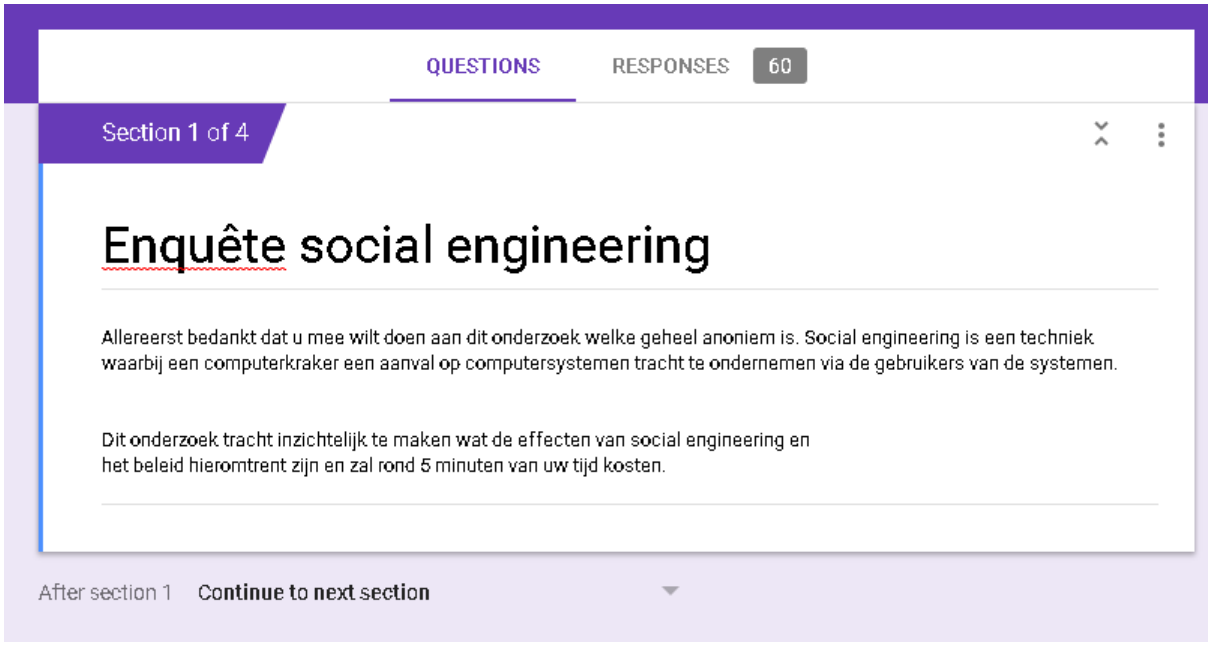
Definitie A: "Social engineering is een set van methoden waarmee het gedrag van een individu of groep individuen wordt gemanipuleerd zodanig dat deze toegang verleent tot bepaalde informatie, met als doel deze informatie te gebruiken om de slachtoffers uit te buiten. Deze techniek maakt gebruik van de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

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

19. *Kunt u beschrijven hoe een social engineeringaanval in zijn werk gaat?*
    Contact zoeken met een slachtoffer, vertrouwen winnen, informatie ontfutselen, manipuleren, etc.
20. *Welke motieven zou een social engineer kunnen hebben?*
    "Gewin" in de breedste zin: soms beperkt het zich tot alleen het achterhalen van (vertrouwelijke) informatie, soms gaat om chantage waarbij de aanvaller uiteindelijk op geldelijk gewin uit is.
21. *Bent u in staat om een aantal verschillende social engineeringsaanvallen te beschrijven?*
    Wellicht.
22. *Waar maakt een social engineer misbruik van?*
    Kwetsbare eigenschappen van de mens: vertrouwen, hulpvaardigheid, aardig gevonden willen worden.

23. *Ziet u vanuit uw eigen medewerkers en/of externe partijen bedreigingen binnen de organisatie?*
    Ja. Eigen medewerkers minder (ze zijn gescreened), maar vanuit externe partijen is het niet uit te sluiten.
24. *Zijn er recent incidenten geweest rondom social engineeringsaanvallen? Via welk (communicatie)kanaal werd deze poging ondernomen?*
    Bij mij niet bekend.
25. *Is naar uw mening uw organisatie voldoende op de hoogte/bewust van social engineering?*
    Op de hoogte wel, bewust is een kwestie van herhalen en herhalen – dus in denk in algemene zin dat er nog sprake is (en zal blijven) van onvoldoende bewustzijn.
26. *Is naar uw mening uw organisatie momenteel voldoende beschermd tegen social engineeringsaanvallen? Welke verbeteringen kunnen worden doorgevoerd?*
    Twijfel. Je kunt de organisatie alleen "voldoende beschermd" kwalificeren als alle medewerkers dat zijn. Moeilijk te realiseren.
27. *Wat zijn de mogelijke gevolgen voor de organisatie als vertrouwelijke informatie op straat komt te liggen?*
    Vele: op de voorpagina van de krant staan, extra kosten moeten maken, aanbestedingstrajecten die ongeldig raken en opnieuw moeten (waardoor vertraging – in ultimo vertraging in de sector met mogelijk economische gevolgen), privacy gevoelige informatie op straat, etc.
28. *Hoe groot is de kans dat een medewerker in een phishing mailt trapt?*
    Groot.
29. *Hoe groot is de kans dat een persoon het gebouw binnenkomt als deze zelf geen toegang heeft?*
    Zeer klein.
30. *Hoe groot is de kans dat wanneer een medewerker een data medium (USB stick, cdrom) vindt, deze ook daadwerkelijk bekijkt?*
    Klein tot gemiddeld. Hieraan is inmiddels zo vaak aandacht gegeven dat men op dit vlak wel beter zou moeten weten.
31. *Weet je welke trends er spelen op het gebied van social engineering?*
    Nee.
32. *Reageert de organisatie snel genoeg op nieuwe ontwikkelingen, in dit geval social engineering. Is het een nieuwe ontwikkeling?*
    Kan beter. Social engineering bestond ook al in het pre-computer tijdperk.

Bijlage 2 enquête vragen



Section 2 of 4

Algemene vragen

Description (optional)

Wat is uw geslacht?

- Man
- Vrouw

Wat is uw leeftijd? *

- <21
- 21 - 30
- 30 - 50
- 50 +

Wat is uw hoogste genoten opleiding? *

- VMBO
- MBO
- HBO
- HBO +
- Universitair
- Other...

Welk categorie beschrijft best uw functie? *

- Management
- IT Specialist
- Medewerker productgroep/dienstverlening
- Ondersteunende groep (bijv HRM, Inkoop, Financien, Relatiebeheer etc)
- Anders

Hoeveel jaar bekleedt u deze functie? *

- minder dan 2 Jaar
- tussen 2 en 5 jaar
- meer dan 5 jaar

Hoeveel jaar in totaal werkt u bij dit bedrijf? *

- minder dan 2 Jaar
- tussen 2 en 5 jaar
- meer dan 5 jaar

Ben u een interne of externe medewerker? *

- Intern
- Extern

Heeft u toegang tot vertrouwelijke informatie vanuit uw functie? *

- Ja
- Nee
- Geen antwoord

After section 2 **Continue to next section**

Section 3 of 4

Vragen informatiebeveiliging

Description (optional)

Met welke informatiebeveiligingsdocumenten bent u inhoudelijk bekend? *

Vink alle toepasselijke opties aan

- [ ] BIR (Baseline Informatiebeveiliging Rijksdienst)
- [ ] ISO 27001/27002
- [ ] Eigen organisatie informatiebeveiligingsdocument
- [ ] Geen enkel van de hierboven genoemde
- [ ] Other...

Voor welke aspecten heeft uw organisatie een beveiligingsbeleid? *

Vink alle toepasselijke opties aan

- [ ] Wachwoordbeleid
- [ ] Antivirus/phishing
- [ ] Change management
- [ ] Informatieclassificatie
- [ ] Documentatieafhandeling/vernietiging
- [ ] Clean desk
- [ ] Locken van computer
- [ ] Weet ik niet

Bent u in staat aan te geven welke informatie vertrouwelijk is op uw afdeling? *

- ( ) Ja
- ( ) Nee
- ( ) Wens ik niet te beantwoorden

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

- ( ) De afdeling beveiliging
- ( ) Het lijnmanagement
- ( ) De directie in combinatie met het MT
- ( ) Weet ik niet

Heeft u ooit vanaf uw organisatie een cursus/training aangeboden gekregen inzage informatiebeveiliging of social engineering? *

- ( ) Ja
- ( ) Nee
- ( ) Wens ik niet te beantwoorden

Als u de kans krijgt een cursus/training met betrekking tot informatiebeveiliging of social engineering te kunnen volgen, zou u dat doen? *

- ( ) Ja
- ( ) Nee
- ( ) Wens ik niet te beantwoorden

Met welke aspecten wordt volgens u rekening gehouden bij beëindigen of wijzigen van het dienstverband? *

Vink alle toepasselijke opties aan

- [ ] Inleveren van bedrijfsmiddelen
- [ ] Blokkering of aanpassen van toegangsrechten
- [ ] Exit gesprek
- [ ] Weet ik niet
- [ ] Wens ik niet te beantwoorden

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

- Ja
- Nee
- Wens ik niet te beantwoorden

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

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

After section 3 **Continue to next section**

Section 4 of 4

Vragen social engineering

Description (optional)

Bent u bekend met het begrip social engineering? *

- Ja
- Nee
- Wens ik niet te beantwoorden

Kunt u beschrijven hoe een social engineeringsaanval wordt uitgevoerd? *

- Ja
- Nee
- Wens ik niet te beantwoorden

Met welke van de onderstaande aanvallen bent u bekend? *

Vink alle toepasselijke opties aan

- [ ] Phishing - Via email, telefoon hengelen naar informatie
- [ ] Dumpster diving - Doorzoeken van de prullenbak / afvalcontainer
- [ ] Office snooping / Desk sniffing - Doorzoeken van een kantoor / werkplekken
- [ ] Piggyback / Tailgaiting - Met een ander persoon meelopen
- [ ] Baiting / Item dropping - Malware geinfecteerd opslagmedium wordt bewust neergelegd/achtergelaten
- [ ] Malicious software - Malware, virus op de werkplek
- [ ] Reverse social engineering -De sympathieke 'collega' die je kan 'helpen' bij een probleem, maar die uiteindelijk een ha...

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

- ( ) Ja
- ( ) Nee
- ( ) Wens ik niet te beantwoorden

Via welke kanalen werd deze poging ondernomen? *

Vink alle toepasselijke opties aan

- [ ] Email
- [ ] Telefoon
- [ ] Fysiek
- [ ] Social media (facebook, linked-in, whatapp etc)
- [ ] Brief
- [ ] Niet benaderd / niet van toepassing
- [ ] Other...

Bent u bekend met de meest voorkomende motieven van social engineers? *

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

Van welke menselijke aspecten maakt een social engineer misbruik? *

Vink alle toepasselijke opties aan

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

Hoe groot schat u de kans in dat één of meerder medewerkers van uw organisatie in een phishing mail trappen? *

- ◯ klein
- ◯ middel
- ◯ groot

Hoe groot schat u de kans in dat een persoon het gebouw van uw organisatie binnenkomt als deze geen toegang heeft? *

- ◯ klein
- ◯ middel
- ◯ groot

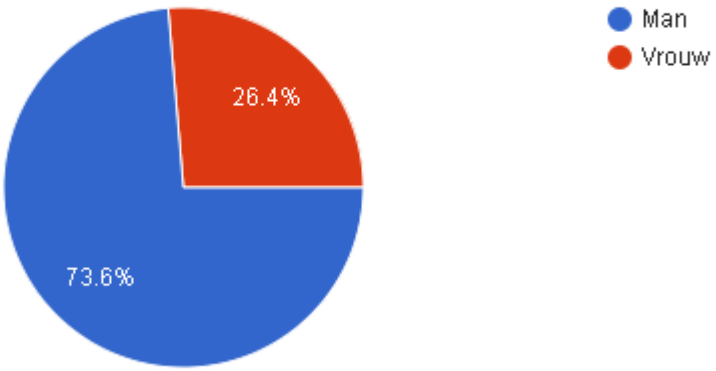
Hoe groot schat u de kans in dat, wanneer een medewerker van uw organisatie een usb stick vindt, hij/zij deze daadwerkelijk probeert te bekijken? *

- ◯ klein
- ◯ middel
- ◯ groot

Bijlage 3 Resultaten enquête

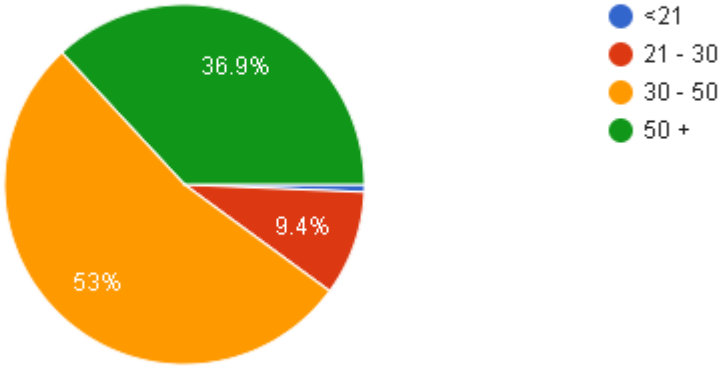
Wat is uw geslacht?

148 responses



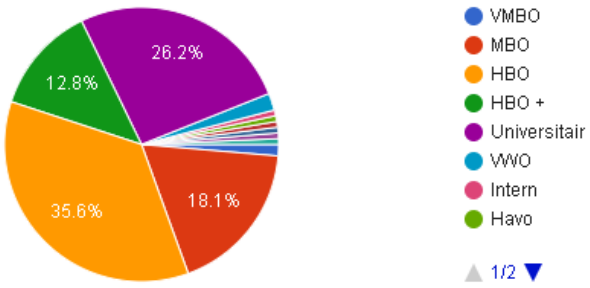
Wat is uw leeftijd?

149 responses



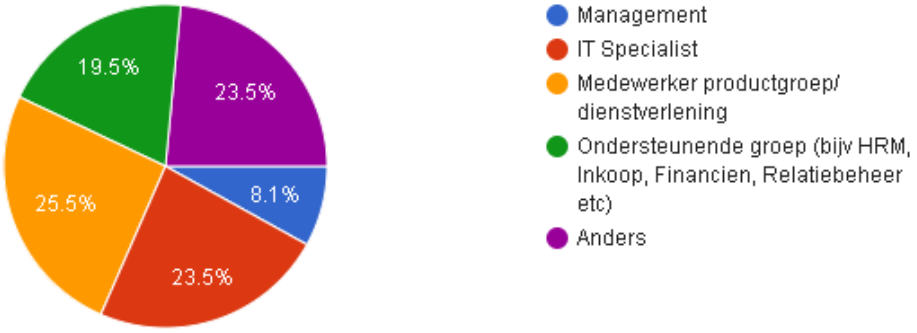
Wat is uw hoogste genoten opleiding?

149 responses



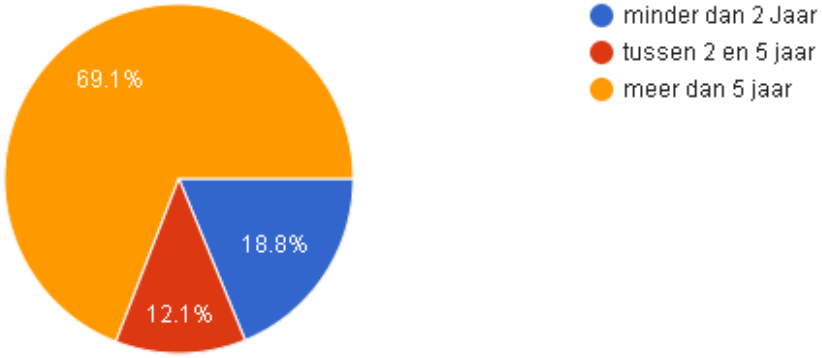
Welk categorie beschrijft best uw functie?

149 responses



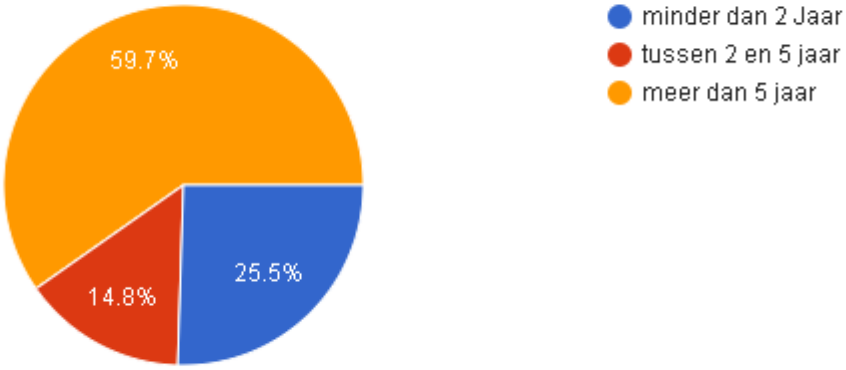
Hoeveel jaar bekleedt u deze functie?

149 responses



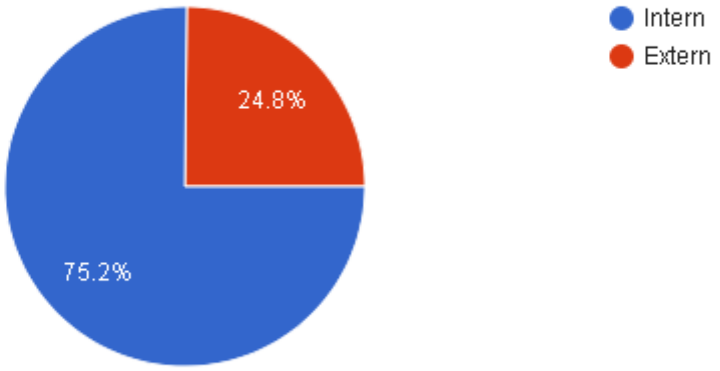
Hoeveel jaar in totaal werkt u bij dit bedrijf?

149 responses



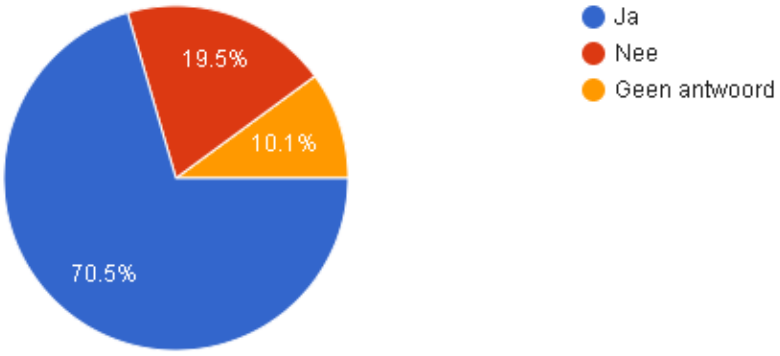
Ben u een interne of externe medewerker?

149 responses



Heeft u toegang tot vertrouwelijke informatie vanuit uw functie?

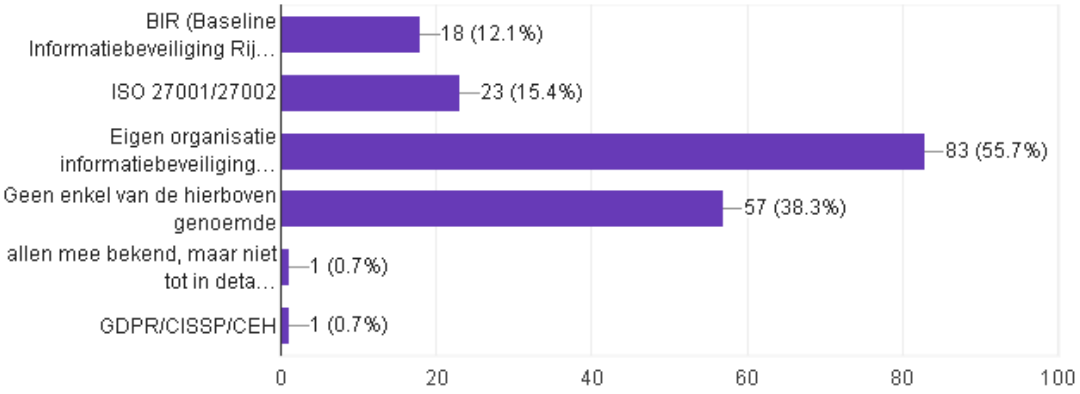
149 responses



Vragen informatiebeveiliging

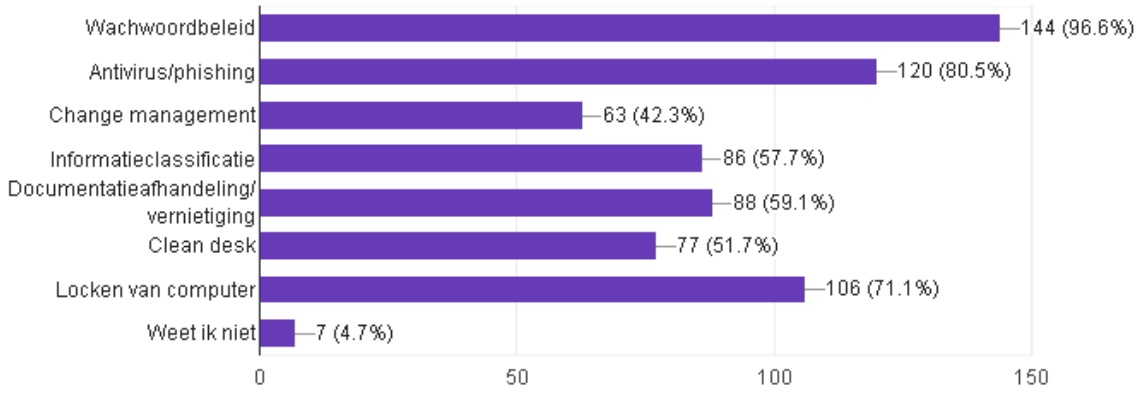
Met welke informatiebeveiligingsdocumenten bent u inhoudelijk bekend?

149 responses



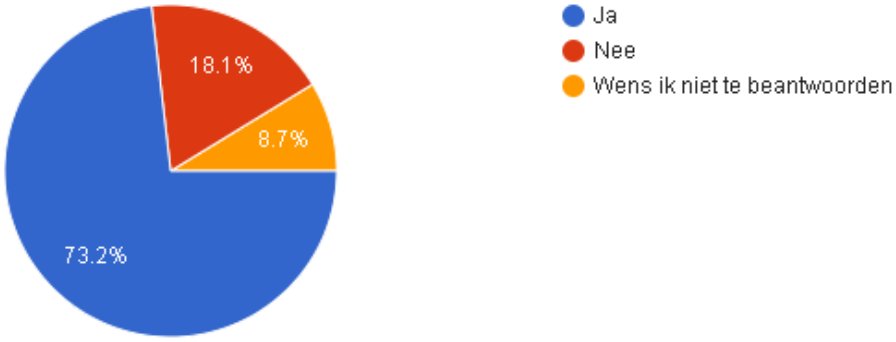
Voor welke aspecten heeft uw organisatie een beveiligingsbeleid?

149 responses



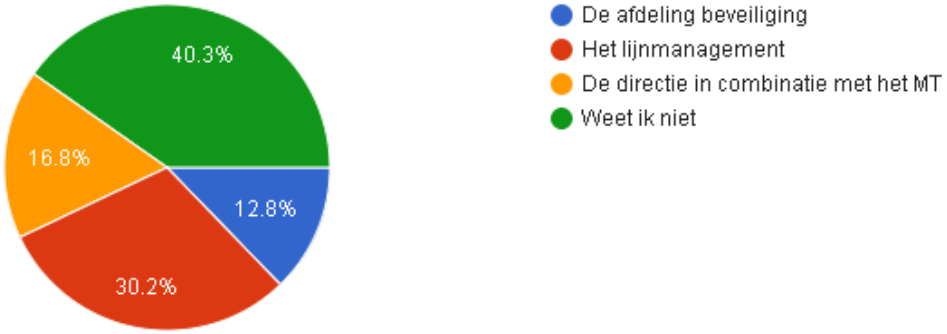
Bent u in staat aan te geven welke informatie vertrouwelijk is op uw afdeling?

149 responses



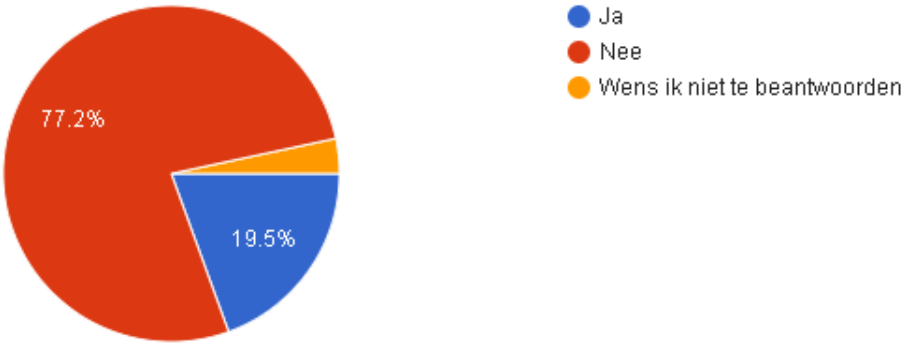
Wie is binnen uw organisatie en/of afdeling verantwoordelijk voor het uitvoeren van en controleren van het informatiebeveiligingsbeleid?

149 responses



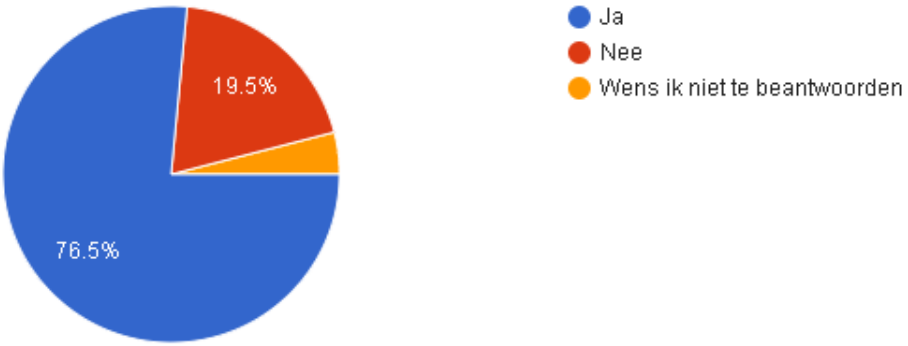
Heeft u ooit vanaf uw organisatie een cursus/training aangeboden gekregen inzage informatiebeveiliging of social engineering?

149 responses



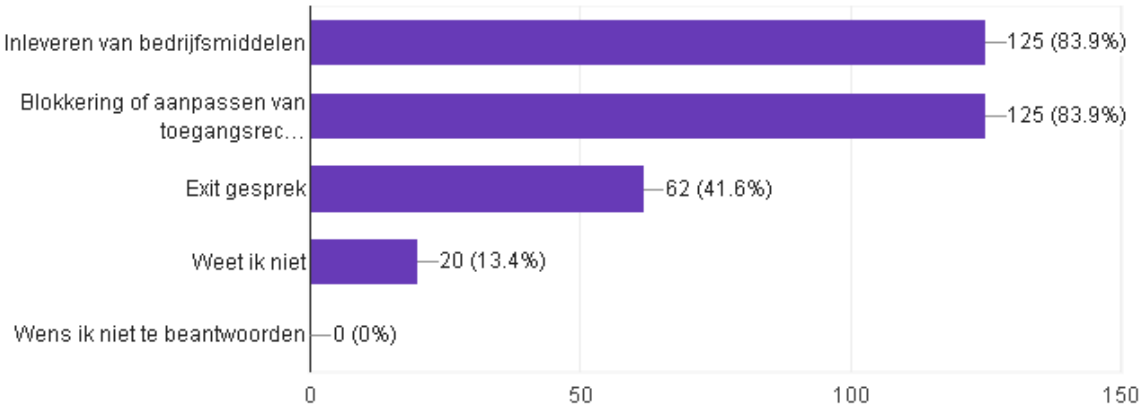
Als u de kans krijgt een cursus/training met betrekking tot informatiebeveiliging of social engineering te kunnen volgen, zou u dat doen?

149 responses



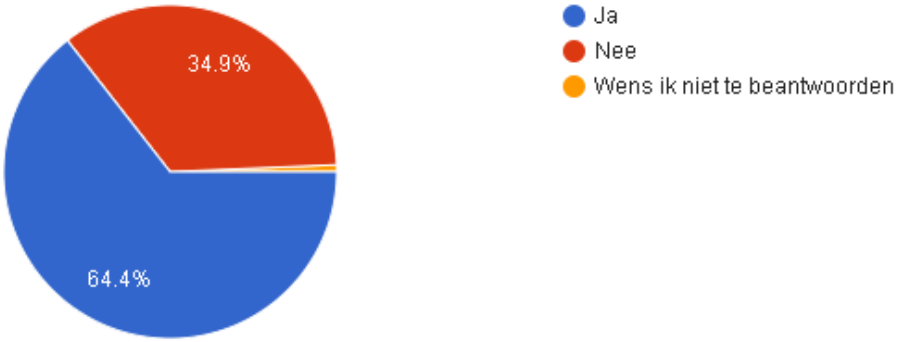
Met welke aspecten wordt volgens u rekening gehouden bij beëindigen of wijzigen van het dienstverband?

149 responses



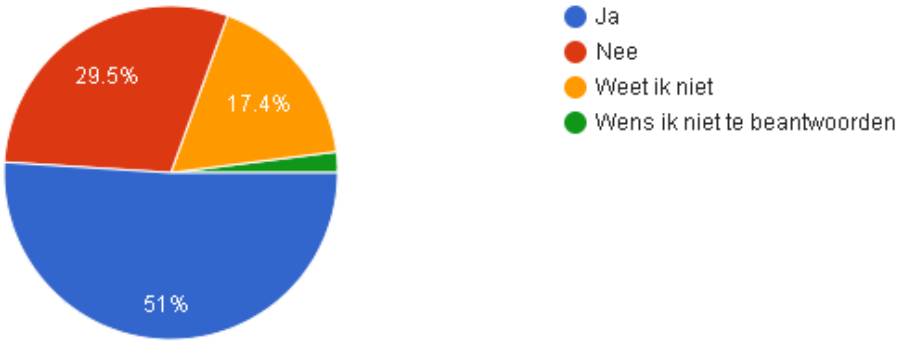
Bent u bekend hoe u dient om te gaan met een beveiligsincident binnen uw afdeling/organisatie?

149 responses



Wordt het beveiligingsbeleid actief uitgedragen/verspreid binnen de afdeling en organisatie

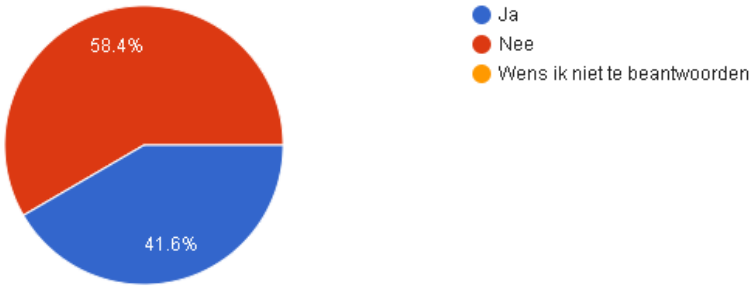
149 responses



Vragen social engineering

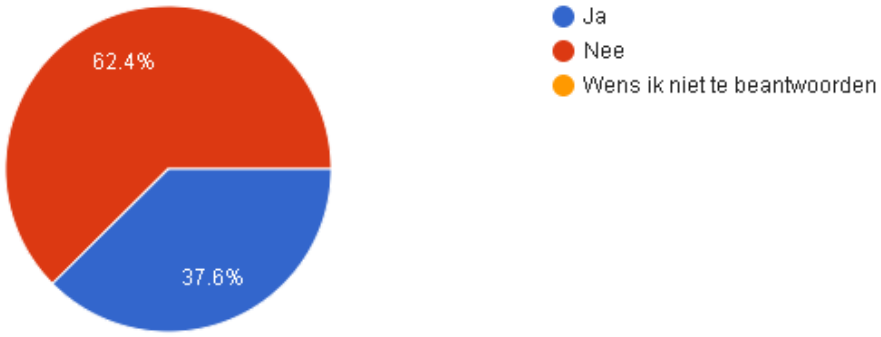
Bent u bekend met het begrip social engineering?

149 responses



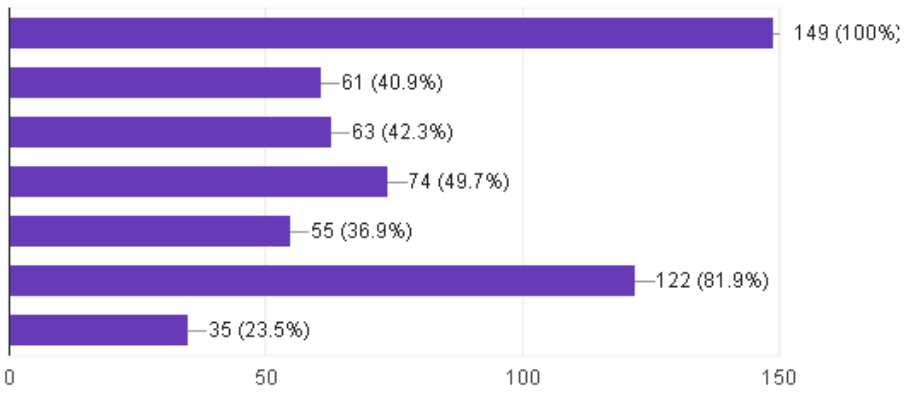
Kunt u beschrijven hoe een social engineeringsaanval wordt uitgevoerd?

149 responses



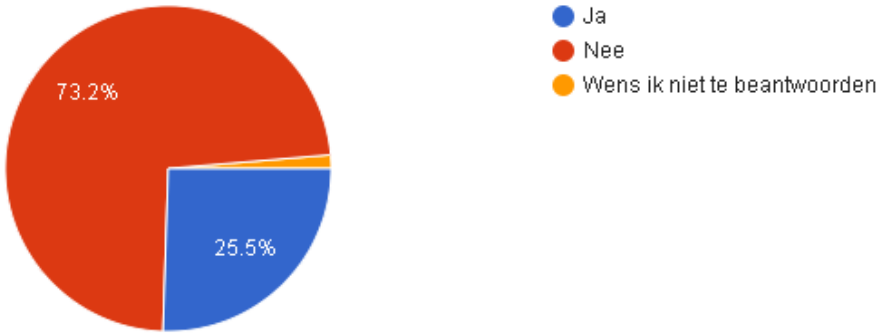
Met welke van de onderstaande aanvallen bent u bekend?

149 responses



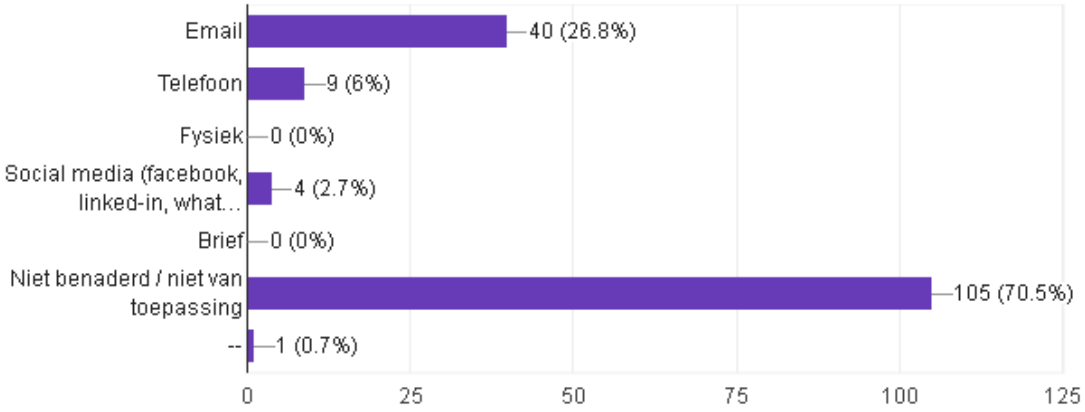
Bent u in de afgelopen 6 maanden benaderd via email, brief, telefoon, social media, dan wel in persoon (fysiek), waarvan u denkt dat dit een poging was tot het verkrijgen van (gevoelige) bedrijfsinformatie?

149 responses



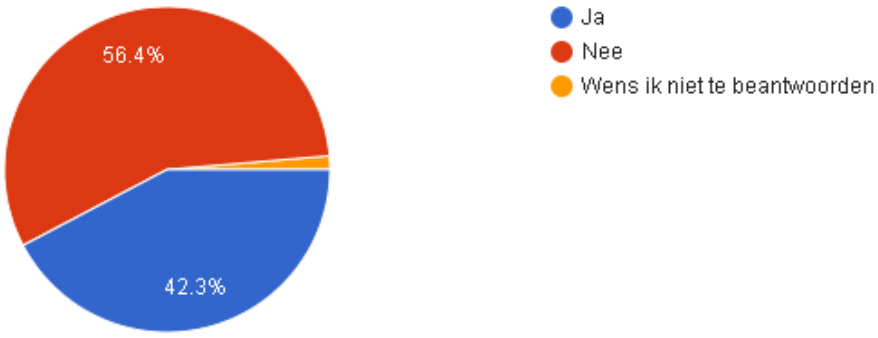
Via welke kanalen werd deze poging ondernomen?

149 responses



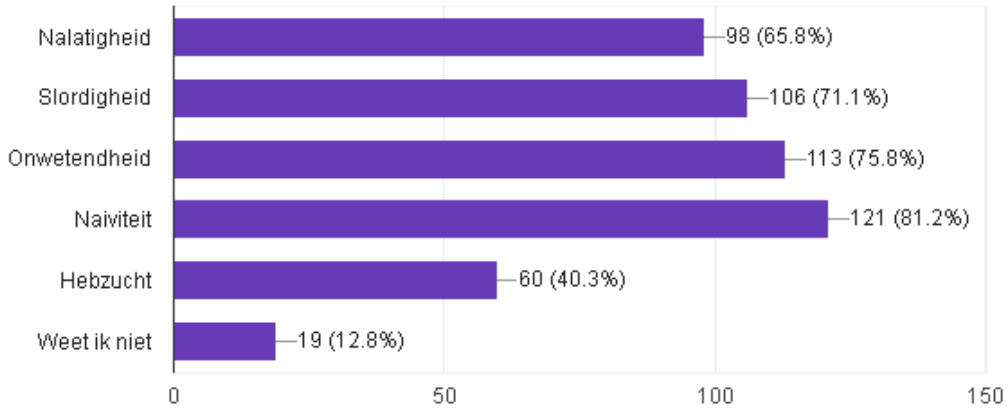
Bent u bekend met de meest voorkomende motieven van social engineers?

149 responses



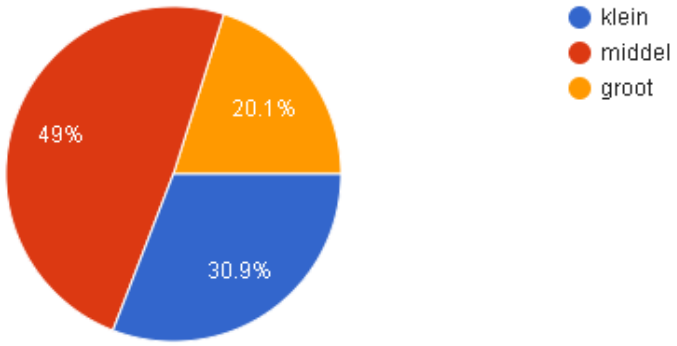
Van welke menselijke aspecten maakt een social engineer misbruik?

149 responses



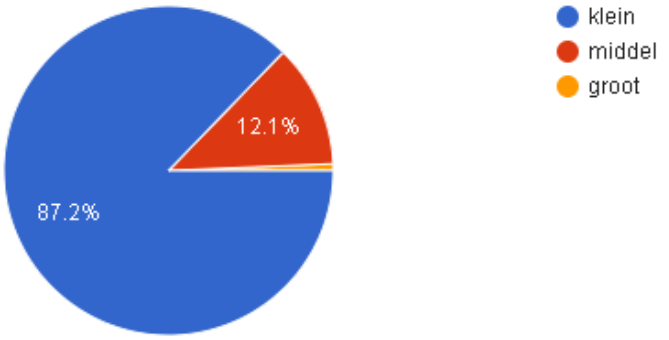
Hoe groot schat u de kans in dat één of meerder medewerkers van uw organisatie in een phishing mail trappen?

149 responses



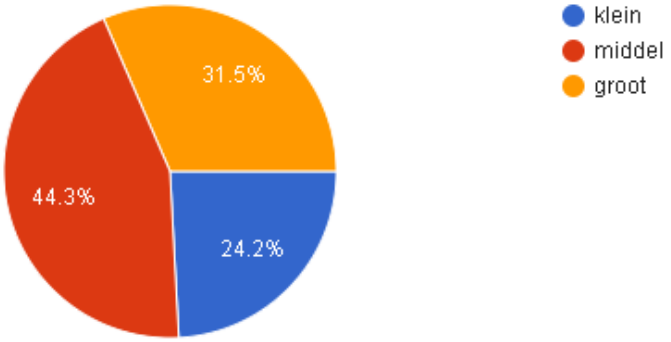
Hoe groot schat u de kans in dat een persoon het gebouw van uw organisatie binnenkomt als deze geen toegang heeft?

149 responses



Hoe groot schat u de kans in dat, wanneer een medewerker van uw organisatie een usb stick vindt, hij/zij deze daadwerkelijk probeert te bekijken?

149 responses



Bijlage 4 lijst Zbo

1. Autoriteit Consument en Markt
2. Autoriteit Financiële Markten
3. Autoriteit Nucleaire Veiligheid en Stralingsbescherming
4. Autoriteit Persoonsgegevens
5. Bevoegde autoriteiten Rijnvaart
6. Bureau Architectenregister
7. Bureau Beheer Landbouwgronden
8. Bureau Financieel Toezicht
9. CAK
10. Centraal Bureau Rijvaardigheidsbewijzen
11. Centraal Orgaan opvang asielzoekers
12. Centrale Commissie Dierproeven
13. Centrale Commissie Mensgebonden Onderzoek
14. CIZ
15. College gerechtelijk deskundigen
16. College sanering zorginstellingen
17. College ter Beoordeling van Geneesmiddelen
18. College van toezicht collectieve beheersorganisaties auteurs- en naburige rechten
19. College voor de Rechten van de Mens
20. College voor de toelating van gewasbeschermingsmiddelen en biociden
21. College voor Toetsen en Examens
22. Commissariaat voor de Media
23. Commissie Eindtermen Accountantsopleiding
24. Commissie schadefonds geweldsmisdrijven
25. De in het kader van Metrologiewet artikel 11 en 12 erkende keurders en aangewezen instanties (Cluster)
26. De Nederlandsche Bank
27. Dienst voor het kadaster en de openbare registers
28. Directeur-generaal van de Statistiek
29. Edelmetaal Waarborg Nederland b.v.
Onderdeel van cluster(s): Waarborginstellingen
30. Erkenninghouders Algemene Periodieke Keuring (Cluster)
31. FGzPt / Registratiecommissie voor gezondheidszorgpsychologen en psychotherapeuten
Onderdeel van cluster(s): Registratiecommissies KNMG, KNMP, KNMT, FGzPt en VenVN
32. FMMU Advies B.V.
33. Gerechtsdeurwaarders (Cluster)
34. Grondkamer Noord
Onderdeel van cluster(s): Grondkamers
35. Grondkamer Noordwest
Onderdeel van cluster(s): Grondkamers
36. Grondkamer Oost
Onderdeel van cluster(s): Grondkamers
37. Grondkamers (Cluster)
38. Grondkamer Zuid
Onderdeel van cluster(s): Grondkamers

39. Grondkamer Zuidwest
Onderdeel van cluster(s): Grondkamers
40. Havenbeheerders (Cluster)
41. Huis voor klokkenluiders
42. Huurcommissie
43. Instituut Fysieke Veiligheid
44. Kamer van Koophandel
45. Kamer voor de Binnenvisserij
46. Kansspelautoriteit
47. Keuringsartsen voor de scheepvaart (Cluster)
48. Keuringsinstanties als bedoeld in artikel 10.3 Telecommunicatiewet (Cluster)
49. Keuringsinstanties bouwproducten (Cluster)
50. Keuringsinstanties geluidshinder (Cluster)
51. Keuringsinstanties Infrastructuur & Milieu overig (Cluster)
52. Keuringsinstanties pleziervaartuigen 2016 (Cluster)
53. Keuringsinstanties uitrusting zeeschepen (Cluster)
54. Keuringsinstanties Volksgezondheid, Welzijn en Sport (Cluster)
55. Keurmerkinstituut jeugdzorg
56. Kiesraad
57. Klassenbureaus Scheepvaart (Cluster)
58. KNMG / Registratiecommissie Geneeskundig Specialisten
Onderdeel van cluster(s): Registratiecommissies KNMG, KNMP, KNMT, FGzPt en VenVN
59. KNMP / Specialisten Registratie Comm, kamers Ziekenhuisfarmacie en Openbare Farmacie (SRC)
Onderdeel van cluster(s): Registratiecommissies KNMG, KNMP, KNMT, FGzPt en VenVN
60. KNMT / Registratiecommissie tandheelkundige Specialismen
Onderdeel van cluster(s): Registratiecommissies KNMG, KNMP, KNMT, FGzPt en VenVN
61. Koninklijke Bibliotheek
62. Koninklijke Nederlandse Akademie van Wetenschappen
63. Landelijk Bureau Inning Onderhoudsbijdragen
64. Luchtverkeersleiding Nederland
65. Medisch-ethische toetsingscommissies (Cluster)
66. Mondriaan Fonds
67. Nationale en Internationale Wegvervoer Organisatie
68. Nederlandse Emissieautoriteit
69. Nederlandse Loodsencorporatie
70. Nederlandse organisatie voor toegepast-natuurwetenschappelijk onderzoek
71. Nederlandse organisatie voor Wetenschappelijk Onderzoek
72. Nederlandse Publieke Omroep
73. Nederlandse Transplantatie Stichting
74. Nederlandse Zorgautoriteit
75. Nederlands-Vlaamse Accreditatieorganisatie
76. Notarissen (Cluster)
77. Onderzoeksraad voor veiligheid
78. Pensioen- en Uitkeringsraad
79. Politieacademie
80. Raad voor Accreditatie
81. Raad voor plantenrassen
82. Raad voor Rechtsbijstand

83. RDW
84. Referendumcommissie
85. Regionale Loodsencorporaties (Cluster)
86. Registratiecommissies KNMG, KNMP, KNMT, FGzPt en VenVN (Cluster)
87. Rijkshavenmeesters (Cluster)
88. Samenwerkingsorganisatie Beroepsonderwijs Bedrijfsleven
89. Sociale Verzekeringsbank
90. Staatsbosbeheer
91. Stichting Administratie Indonesische Pensioenen
92. Stichting Airport Coordination Netherlands
93. Stichting Bloembollenkeuringsdienst
94. Stichting Centraal Orgaan voor Kwaliteitsaangelegenheden in de Zuivel
95. Stichting Donorgegevens Kunstmatige Bevruchting
96. Stichting Fonds voor Cultuurparticipatie
97. Stichting Kwaliteits-Controle-Bureau
98. Stichting Nederlandse Algemene Keuringsdienst voor Zaaizaad en Pootgoed van Landbouwgewassen
99. Stichting Nederlandse Algemene Kwaliteitsdienst voor de Tuinbouw
100. Stichting Nederlands Fonds voor de Film
101. Stichting Nederlands Fonds voor Podiumkunsten
102. Stichting Nederlands Letterenfonds
103. Stichting Nidos
104. Stichting Participatiefonds voor het Onderwijs
105. Stichting Regionale Publieke Omroep
106. Stichting Skal Biocontrole
107. Stichting Stimuleringsfonds Creatieve Industrie
108. Stichting Vaarbewijs- en marifoonexamens
109. Stichting Vakopleiding Automobiel- en Motorrijwielbedrijf
110. Stichting Vervangingsfonds en Bedrijfsgezondheidszorg voor het Onderwijs
111. Stichting Visitatie Woningcorporaties Nederland
112. Stimuleringsfonds Nederlandse Culturele Mediaproducties
113. Stimuleringsfonds voor de Journalistiek
114. Uitvoerders Wlz (Cluster)
115. Uitvoeringsinstituut Werknemersverzekeringen
116. VenVN / Registratiecommissie Specialismen Verpleegkundigen
Onderdeel van cluster(s): Registratiecommissies KNMG, KNMP, KNMT, FGzPt en VenVN
117. WaarborgHolland B.V.
Onderdeel van cluster(s): Waarborginstellingen
118. Waarborginstellingen (Cluster)
119. Waarderingskamer
120. Zorginstituut Nederland
121. Zorgkantoren Wlz (Cluster)
122. ZorgOnderzoek Nederland / Medische Wetenschappen

Bijlage 4 Aanvalstactieken social engineering

Social engineeringstactieken (Granger, 2010; Krombholz et al., 2015; Mitnick & Simon, 2003, Chiew et al, 2018;).

Nr	Aard	Aanvalstechniek	Toelichting
1	P	Dumpser driving	Dumpster diving is het doorzoeken van de prullenbak/afvalcontainer van particulieren of bedrijven met als doel weggegooide items te vinden met gevoelige informatie. Deze informatie kan vervolgens worden gebruikt om toegang tot een systeem of een specifieke gebruikersaccount te bemachtigen.
2	P	People spotting	People spotting is het bestuderen en observeren van een slachtoffer of een groep slachtoffers om na te gaan wat hun gewoontes zijn.
3	P	Physical reconnaissance/shoulder surfing	Shoulder surfing verwijst naar het gebruik van directe-observatietechnieken om informatie te krijgen, zoals meekijken over iemands schouder naar zijn scherm of toetsenbord.
4	P	Pretexting/Profiling	Pretexting is wanneer een social engineer een verhaal ontwikkelt dat hem in staat stelt om zich een beeld te verwerven van de doelgroep. Het biedt de rechtvaardiging voor de vragen die bij de echte aanval gesteld kunnen worden.
5	C	Mail-outs	Er bestaan verschillende soorten mail-outs, bijvoorbeeld in de vorm van enquêtes. Deze worden gebruikt om bedrijfs- en persoonlijke informatie te verzamelen. Deelname aan deze enquêtes wordt verhoogd door het aanbieden van prijzen. Maar mail-outs kunnen ook gebruikt worden om mensen te misleiden voor reverse social engineering of malicious software aanvallen.
6	C	Phishing	Phishing is de poging om gevoelige informatie te verwerven of om iemand te laten handelen op een gewenste manier door zich voor te doen als een betrouwbare entiteit. De aanvallen zijn meestal gericht op grote groepen

			mensen. Phishing-aanvallen kunnen worden uitgevoerd op bijna elk kanaal, van websites, fysieke benadering, sociale netwerken tot zelfs cloud-diensten. Aanvallen gericht op specifieke personen of bedrijven worden aangeduid als spear phishing. Als een phishing-aanval is gericht op high-profile doelen in ondernemingen, wordt de aanval aangeduid als de whale fishing.
7	M	Smishing	Smishing is hetzelfde als Vishing (zie volgende) maar met sms (short message service)
8	M	Phreaking /Vishing	Phreaking of Vishing is het misbruiken van een bedrijfstelefoon of telefooncentrale, zodanig dat iemand intern kan bellen, of gesprekken af kan luisteren. De aanvaller kan daarbij zich voordoen als een collega, belt immers intern en verschaft zich daarmee de legitimiteit om gewenste informatie (uit) te vragen.
9	C	Virtual reconnaissance/Waterholing	Waterholing beschrijft een gerichte aanval waarin de aanvallers een website overnemen die waarschijnlijk bezocht gaat worden door het gekozen slachtoffer. De aanvallers wachten vervolgens „bij de waterpoel" op hun slachtoffer.
10	C	Web Search	Web search is het zoeken naar online informatie over het slachtoffer of de organisatie. Hiermee wordt het voorwerk gedaan voor een verdere aanval.
11	P	Physical Impersonation	Impersonatie is het zich voordoen als een werknemer met als doel de slachtoffers te misleiden. De meeste mensen zijn sneller bereid te helpen of regels te omzeilen als het om een collega gaat.
12	P	Reverse Social engineering	Reverse social engineering is een aanval waarbij eerst een vertrouwensrelatie tot stand wordt gebracht tussen de aanvaller en het slachtoffer. De aanvaller creëert een situatie waarin het slachtoffer hulp nodig heeft waarna hij zichzelf presenteert als de persoon die de situatie kan oplossen. Dit zorgt ervoor dat het slachtoffer hem vertrouwt en

			eerder op zijn verzoeken zal ingaan.
13	C	Virtual Impersonation / Fake profiles	Fake profiles is het opzetten van onechte profielen met het doel informatie van de slachtoffers te bemachtigen.
14	C	Wiphishing	WiPhishing of Evil Twin is een techniek vergelijkbaar met phishing dat gebruik maakt van draadloos netwerk. De phisher gaat tussen de internetgebruiker en een legitime draadloos zender zitten met een rogue AP zodat hij informatie kan aftappen.
15	P	Direct approach	Direct approach is de directe benadering van slachtoffers om informatie te bemachtigen die nodig is voor de daadwerkelijke aanval. Dit kan door simpelweg te bellen en te vragen naar informatie.
16	P	Office Snooping/Desk sniffing	Office snooping/Desk sniffing is het doorzoeken van een kantoor en de werkplekken binnen het kantoor van bedrijven met als doel het vinden van gevoelige informatie. Deze informatie kan vervolgens worden gebruikt om toegang tot een systeem of een specifieke gebruikersaccount te bemachtigen.
17	P	Piggybacking /Tailgating	Piggybacking of tailgating is een aanval waarmee met een andere persoon wordt meegelopen om in een besloten gebied te komen. De persoon met wie wordt meegelopen heeft wel de juiste autorisatie.
18	C	Baiting / Item dropping	Baiting is een aanval waarbij een met malware geïnfecteerd opslagmedium wordt achtergelaten op een plaats waar het beoogde slachtoffer dit zal vinden.
19	C	Data leakage	Data leakage is het met opzet achterlaten van een bestand op een systeem of in de cloud met de bedoeling dat andere individuen dit bestand openen. Op het moment van openen, kan kwaadaardige software worden geïnstalleerd.
20	P/C	Identity theft	Identity theft is het gebruiken van informatie van een persoon zonder diens medeweten, zoals zijn naam, bankrekeningnummer, geboortedatum of zijn BSN-nummer. Dit kan op verschillende wijzen worden

			bewerkstelligd, variërend van het dragen van een uniform, phishing-aanvallen tot het aanpassen van de DNS-setting.
21	C/M	Malicious software	Malicious software is kwaadaardige software die door een social engineer wordt geïnstalleerd of wordt aangeboden. Als de software eenmaal op het systeem van de slachtoffer is geïnstalleerd, kan vaak de controle op het systeem worden overgenomen of wordt bepaalde informatie verzameld en opgehaald.