

Hochschule Darmstadt

- FACHBEREICH INFORMATIK -

Social Engineering Awareness

mittels Serious Games

Abschlussarbeit zur Erlangung des akademischen Grades

Master of Science (M.Sc.)

vorgelegt von

Niklas Bessler und Saed Alavi

Referent: Prof. Dr. Marian Margraf

Korreferent: Prof. Dr. Andreas Heinemann

Erklärung

Wir versichern hiermit, dass wir die vorliegende Arbeit selbstständig verfasst und keine anderen als die im Literaturverzeichnis angegebenen Quellen benutzt haben.

Alle Stellen, die wörtlich oder sinngemäß aus veröffentlichten oder noch nicht veröffentlichten Quellen entnommen sind, sind als solche kenntlich gemacht.

Die Zeichnungen oder Abbildungen in dieser Arbeit sind von uns selbst erstellt worden oder mit einem entsprechenden Quellennachweis versehen.

Die Arbeit ist in gleicher oder ähnlicher Form noch bei keiner anderen Prüfungsbehörde eingereicht worden.

Ort, Datum

Unterschrift

Ort, Datum

Unterschrift

Zusammenfassung

Zielsetzung: Es soll untersucht werden, ob sich eine Sensibilisierung bezüglich des Themenfelds Social Engineering mittels eines Serious Games erzielen lässt. **Methoden:** Um einen möglichen Lerneffekt durch eine spielerische Sensibilisierung zu bestimmen, wurde eine randomisierte kontrollierte Studie durchgeführt. Die Testpersonen ($n=38$) wurden zufällig der Experimental- und Kontrollgruppe zugewiesen. Die vorhandene Sensibilisierung der Probanden (Social Engineering Awareness) wurde jeweils zu Beginn und Ende der Studie mittels standardisiertem Online-Fragebogen bestimmt. Die Experimentalgruppe erhielt nach Bearbeiten des ersten Fragebogens eine Intervention, indem die Teilnehmenden das Serious Game SANIAG spielten. Die Messwerte der Fragebögen wurden automatisiert unter Beachtung der Ratekorrektur in einen numerischen Wert überführt. **Ergebnisse:** Die empirisch erhobenen Daten wurden mittels Varianzanalyse ausgewertet. Eine zweifaktorielle Varianzanalyse mit Messwiederholung mit den Faktoren der Gruppenzugehörigkeit (Stufen: Experimental- und Kontrollgruppe) und der zeitlichen Betrachtung (Stufen: Prä- und Post- Intervention) zeigte signifikante Interaktionseffekte ($F(1, 68) = 5,332$; $p = 0,0239$). Anschließend wurden die Unterschiede innerhalb der Gruppen mittels einfaktorieller Varianzanalyse betrachtet. Die Experimentalgruppe erzielte ein sehr signifikant höheres Ergebnis im Prä-Post-Verlauf ($p < 0,001$). Ein signifikanter Unterschied im Prä-Post-Verlauf der Kontrollgruppe wurde hingegen nicht festgestellt ($p = 0,586$). Der gefundene Interaktionseffekt zeigt eine Effektstärke von 0,27. Dies entspricht einer schwachen Effektstärke nach Cohen. **Interpretation:** Unsere Ergebnisse deuten darauf hin, dass Serious Games eine sinnvolle Methoden sind, um Social Engineering Awareness zu schaffen.

Abstract

Aim: The present study was conducted to investigate the impact of serious games in respect of raising peoples awareness for social engineering. **Methods:** In order to evaluate a potential learning effect caused by a serious game, we conducted a randomized controlled trial. The subjects ($n=38$) were randomly allocated to the experimental group or the control group. The awareness levels (social engineering awareness) were determined both at the onset and at the end of the study using a standardized online questionnaire. The experimental group has the intervention being assessed after completing the first questionnaire by playing the serious game SANIAG. The measured data were then quantified in an automated way negating the effects of random selection using a formula scoring. **Results:** Empirical data were assessed using the statistical test analysis of variance. A two-way ANOVA with repeated measures to evaluate the factors group (categories: experimental and control) and time (categories: pre and post intervention) showed significant interaction effects ($F(1, 68) = 5.332$; $p = 0.0239$). Then, we looked at the difference within the groups by conducting a one-way ANOVA. The experimental group achieved a very significant improvement in the pre-post comparison ($p < 0.001$). There was no statistically significant difference in the pre-post comparison of the control group ($p = 0.586$). The shown interaction effect manifests in an effect size of 0.27. This means a small effect according to Cohen. **Interpretation:** Our results suggests that serious games are a feasible approach to raise social engineering awareness.

Danksagung

Zunächst möchten wir uns an dieser Stelle bei all jenen bedanken, die uns bei der Erstellung dieser Arbeit unterstützt und motiviert haben. Ebenso bedanken wir uns bei allen Teilnehmenden der Studie. Unser besonderer Dank gilt Herrn Prof. Dr. Marian Margraf und Herrn Prof. Dr. Andreas Heinemann für die persönliche Unterstützung und fachliche Betreuung des Themas.

Außerdem bedanken wir uns bei den Psychologinnen Sophie Walter und Ana-Maria Rosca, dass sie uns mit ihrem großen fachlichen Wissen unterstützt haben. Auch gilt unser Dank Loredana Marziano Bento, Bich Ngoc Dao und Kerstin Reuning für die kreative und künstlerische Unterstützung bei der Ausarbeitung des Lernspiels SANIAG. Adrian Muck und Philipp Goldberg danken wir für die Details, die sie zur Entwicklung des Spiels beigetragen haben.

Natürlich möchten wir uns auch bei allen bedanken, die uns während unseres gesamten Studiums begleitet haben. Nicht zuletzt gilt ein herzlicher Dank unseren Familien, die uns überhaupt erst das Informatikstudium ermöglicht und uns während des Studiums unterstützt haben.

Inhaltsverzeichnis

Abbildungsverzeichnis	xi
Tabellenverzeichnis	xiii
Quelltextverzeichnis	xiii
1 Einführung	1
1.1 Motivation	1
1.2 Forschungsfrage und Zielsetzung	3
1.3 Forschungshypothese	4
1.4 Struktur der Arbeit	5
2 Related work	6
3 Grundlagen	8
3.1 Social Engineering	8
3.1.1 Definition	8
3.1.2 Sozialpsychologische Grundlagen	9
3.1.3 Social Engineering Risiken	10
3.1.4 Angriffsvektoren	10
3.1.5 Gegenmaßnahmen	15
3.2 Serious Game	18
3.2.1 Definition	18
3.2.2 Abgrenzung und verwandte Konzepte	19
3.2.3 Design eines Serious Games	23

3.3	Social Engineering Awareness	26
3.3.1	Definition	26
3.3.2	Abgrenzung	27
4	Serious Game SANIAG	29
4.1	Spielprinzip	29
4.2	Spieldidaktische Überlegungen	30
4.2.1	Zielgruppe	30
4.2.2	Spieldesign	31
4.2.3	Spielmechaniken und Ästhetiken	32
4.2.4	Lernziele	33
4.3	Entwicklungsprozess	35
4.4	Finale Spielelemente	37
4.4.1	Spielbrett	37
4.4.2	Spielkarten	39
4.4.3	Weitere Spielbausteine	45
5	Forschungsdesign	47
5.1	Generelles Studiendesign	47
5.2	Rechtliche und ethische Rahmenbedingungen	49
5.2.1	Ethische Aspekte	49
5.2.2	Datenschutz	51
5.3	Stichprobenumfang	52
5.4	Dauer der Studie	55
5.5	Datenerhebungsmethode	55
5.5.1	Auswahl der Datenerhebungsmethode	56
5.5.2	Antwortmodalitäten der Fragebogen	57
5.5.3	Distraktoren	58
5.5.4	Aufbau der Fragebogen	59
5.5.5	Quantitative Gütekriterien der Fragebogen	61
5.5.6	Post-Intervention Fragebogen	62

6	Durchführung der Studie	63
6.1	Pretest	63
6.1.1	Pretest des Spiels SANIAG	63
6.1.2	Pretest des Fragebogens	64
6.2	Generelle Studiendurchführung	65
6.3	Randomisierung	65
6.4	Kohorte THM	66
6.5	Kohorte HDA	67
6.6	Kohorte PRIVSA	69
6.7	Kohorte PRIVNI	70
6.8	Messpunkt nach der Intervention	71
6.9	Quantifizierung und Zuordnung der Datensätze	71
7	Ergebnisse	75
7.1	Einblick in die Daten	75
7.1.1	Rücklaufquote	75
7.1.2	Population	76
7.1.3	Selbsteinschätzung der Testpersonen	76
7.1.4	Vergleich zwischen Primär- und Sekundärgruppe	78
7.1.5	Erzielte Punktwerte der Testpersonen	80
7.2	Statistische Auswertung	81
7.2.1	Prämissen der ANOVA	81
7.2.2	Zweifaktorielle ANOVA mit Messwiederholung	87
7.2.3	Einfaktorielle ANOVA der Experimentalgruppe Prä/Post	90
7.2.4	Einfaktorielle ANOVA der Kontrolle Prä/Post	91
7.2.5	Einfaktorielle ANOVA bezüglich Awareness	92
7.2.6	Berechnung der Effektstärke	93
7.2.7	Überprüfung der Forschungshypothese	93
7.3	Diskussion der Ergebnisse	94
8	Schlusswort	96

Abkürzungsverzeichnis	i
Glossar	ii
Literaturverzeichnis	iv
Anhang	x
A Fragebogen	xii
B VBA-Skript zur Randomisierung	xx
C VBA-Skript zur Quantifizierung der Fragebogen	xxii
D Messwerte	xxix

Abbildungsverzeichnis

1.1	Kosten von Cyberkriminalität	2
3.1	Taxonomie der Angriffsvektoren des Social Engineerings	11
3.2	Einordnung von Spielmodellen nach Deterding	21
3.3	Paradigmen des Edutainments	23
3.4	MDA-Framkework nach Hunicke et al.	23
4.1	SANIAG Spielkarten	30
4.2	Taxonomie von Lernzielen nach Bloom	35
4.3	Bildbearbeitung einer Spielkarte	36
4.4	Zeichnung eines Spielkartenbildes	37
4.5	Saed und Niklas' Awareness Game (SANIAG) Brettspiel	39
4.6	SANIAG Location-Karte	40
4.7	SANIAG Countermeasure-Karte	41
4.8	SANIAG Awareness-Karte	42
4.9	SANIAG Social Hacking-Karte	43
4.10	SANIAG Hacking Gadget-Karte	44
4.11	SANIAG Instant Hacking-Karte	44
4.12	SANIAG Spielfiguren, Würfel und Reputationsmünzen	45
5.1	Studienphasen	48
5.2	Bestimmung des Stichprobenumfangs	53
5.3	Beispielhafte Fragestellung zu einer These	60
5.4	Beispielhafte Fragestellung zu einem Szenario	61

6.1	Pretest des Lernspiels SANIAG	64
6.2	Randomisierung der Testpersonen	65
6.3	Spiele des Lernspiels SANIAG der Kohorte THM	67
6.4	Spiele des Lernspiels SANIAG der Kohorte HDA	68
6.5	Spiele des Lernspiels SANIAG der Kohorte PRIVNI	71
6.6	Fragebogen Hilfstabelle	72
7.1	Beruflicher Status der Testpersonen	76
7.2	Statistiken der Likert-Skala (Experimentalgruppe)	77
7.3	Statistiken der Likert-Skala (Kontrolle)	77
7.4	Messpunkte der Experimentalgruppe	80
7.5	Messpunkte der Kontrolle	80
7.6	Ausreißer-Messwerte der Experimentalgruppe	83
7.7	Ausreißer-Messwerte der Kontrolle	83

Tabellenverzeichnis

3.1	Prinzipien der Beeinflussung nach Cialdini	9
3.2	Beziehung von Spielmechaniken und Spielanreizen	25
5.1	Checkliste des Ethikantrags	50
5.2	Beispielhafte Fragestellungen nach Kruger	62
7.1	Punkteskala der Selbsteinschätzung	79
7.2	Prämissen der ANOVA nach Huber	81
7.3	Varianzgleichheit der Prä-Gruppen	84
7.4	Kolmogorov-Smirnov-Test	86
7.5	Deskriptive Statistiken	88
7.6	Zweifaktorielle ANOVA mit Messwiederholung	88
7.7	Einfaktorielle Varianzanalyse der Experimentalgruppe	90
7.8	Einfaktorielle Varianzanalyse der Kontrollgruppe	91
7.9	Einfaktorielle Varianzanalyse der Prä-Post-Differenz	92
7.10	Effektstärke nach Cohen	93
A.1	Fragebogen mit korrekten Antworten	xix
D.1	Empirisch erhobene und quantifizierte Messwerte	xxix

Quelltextverzeichnis

B.1	VBA-Skript zur Randomisierung	xx
C.1	VBA-Skript zur Quantifizierung der Fragebogen	xxii

Kapitel 1

Einführung

1.1 Motivation

Die Bedrohungslage durch sogenannte Cyberkriminalität wächst zunehmend, während die Aufklärungsrate gering bleibt.[AL19] Cyberangriffe richten sich nicht nur gegen Unternehmen, sondern auch gegen Privatpersonen. Der Schaden durch Cyberangriffe ist dabei vielfältig und reicht vom Produktionsausfall über Know-how Verlust bis hin zu persönlichen Konsequenzen für Führungskräfte, Mitarbeiter oder Privatpersonen. Durch Gesetze und Regularien sind Unternehmen teilweise gezwungen, ihre Systeme abzusichern. Ein Einfallstor bleibt jedoch der Faktor Mensch, der für viele Kriminelle weiterhin ein leichtes Ziel darstellt.

In einer, im Jahr 2019, von Accenture Plc¹ in Auftrag gegebene Studie, wurden in 11 Ländern Unternehmen zu Vorfällen von Cybercrime befragt. Dabei wurden Daten von insgesamt 355 Großunternehmen mittels Befragung erhoben. Ein Gegenstand der jährlich publizierten Studie sind die durch Cyberkriminalität entstandenen Kosten der Unternehmen. Die Aufschlüsselung dieser nach unterschiedlichen Typen von Cyberkriminalität stellt einen Indikator für die Relevanz der verschiedenen Angriffsarten dar. Die genauen Zahlen sind in Abbildung 1.1 als Balkendiagramm grafisch dargestellt.

¹Accenture Plc hat ihren Firmensitz im irischen Dublin und zählt zu den weltweit größten Managementberatungs-, Technologie- und Outsourcing-Dienstleistern.

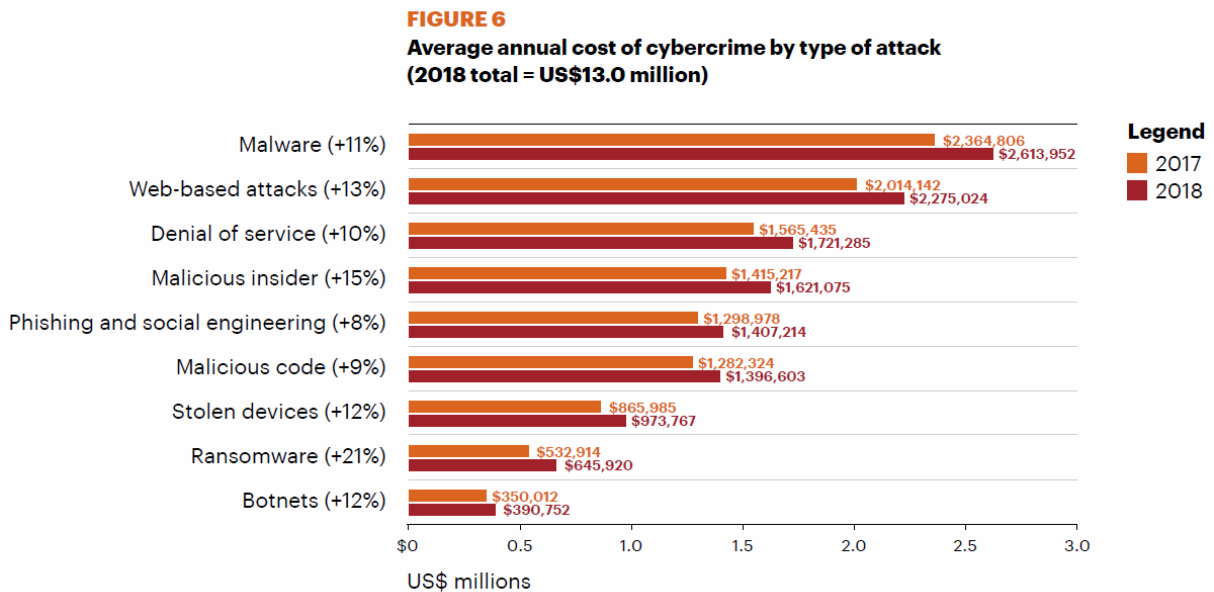


Abbildung 1.1: Kosten von Cyberkriminalität [AL19, Abbildung 6]

Der Abbildung lässt sich entnehmen, dass die Kategorie "Malware" (Schadsoftware) den größten finanziellen Schaden für Unternehmen bedeutet. Dies rückt nicht zuletzt die Techniken des Social Engineerings weiter in den Fokus, da die Verbreitung solcher Malware oftmals auf Phishing oder verwandten Angriffsvektoren des Social Engineerings beruhen. Die Kategorien "Malicious insider" (Böswillige Beschäftigte) und "Stolen devices" (Gestohlene Geräte) haben eine ähnliche Relevanz wie die explizit geschaffene Kategorie für Social Engineering. Hierbei handelt es sich ursächlich jeweils um fahrlässig handelnde bzw. unachtsame Mitarbeiter. Daher lassen sich die beiden Kategorien auch dem Social Engineering zuordnen. Die eigenständige Kategorie "Phishing and social engineering" (Phishing und Social Engineering) ist unter den fünf bedeutsamsten Kategorien vertreten, was für dessen Relevanz spricht.

Die Interpretation, dass Social Engineering eine große Rolle einnimmt, wird darüber hinaus im Fließtext der Studie bekräftigt, in der menschliche Faktoren als schwächstes Glied ausgemacht werden ("Human are still the weakest link" [AL19]). Weiter wird als erste und wichtigste Maßnahme empfohlen, dass Angriffe, die auf menschlichen Faktoren aufbauen, verstärkt Beachtung erhalten sollen ("1. Prioritize protecting people-based attacks" [AL19]). Schulungen seien hierfür essentiell.

Gardner und Thomas widmen in ihrem Buch "Building an Information Security Awareness Program" ein Kapitel der Debatte, wie unwirksam aktuelle Schulungsansätze scheinen.[GT14, Kapitel 6] Dabei referenzieren sich auch aktuellere Forschungsergebnisse. Sie sprechen sich deutlich gegen traditionelle Schulungen im Format einer Vorlesung bzw. Präsentation aus ("In fact, many in higher education say that the lecture, a centuries-old teaching technique, is dead" [GT14]).

Dieser Umstand zeigt auf, dass weitere Forschungsbemühungen zu dem Themenfeld Social Engineering Awareness notwendig und wichtig sind, um weitere Cybercrime-Vorfälle zu minimieren. Diese Arbeit widmet sich daher der Evaluierung einer neuartigen Methode zur Sensibilisierung von Mitarbeitern bezüglich Social Engineering Angriffen.

1.2 Forschungsfrage und Zielsetzung

Der zentrale Gegenstand dieser Arbeit ist die Beantwortung der Forschungsfrage "Lassen sich Personen durch das Spielen eines Lernspiels für Social Engineering Angriffe sensibilisieren?". Die Fragestellung beschränkt sich auf die Sensibilisierung gegenüber Angriffen auf menschliche Faktoren. Insofern findet eine Abgrenzung zu dem übergeordneten Themenfeld der Informationssicherheit statt, welches zusätzlich rein technische Sicherheitslücken beinhaltet. Hierunter fallen etwa Pufferüberläufe, fehlskonfigurierte Firewalls oder das Verwenden von unsicheren kryptografischen Verfahren.

Die Beantwortung der Forschungsfrage soll mittels empirischer Forschung bzw. einem echten Experiment realisiert werden. An dieser Stelle soll ausdrücklich dargelegt werden, dass nicht das Schaffen eines geeigneten Lernspiels, sondern die Beantwortung der Forschungsfrage im Vordergrund steht.

1.3 Forschungshypothese

Um ein echtes Experiment durchführen zu können, ist im Vorfeld eine Hypothesenbildung notwendig. [Dör+15, Kapitel 5.2] In der Regel wird für die spätere statistische Auswertung ein Hypothesenpaar gebildet, die Nullhypothese und die Alternativhypothese. Die Nullhypothese ist falsifizierbar, wohingegen die Alternativhypothese (auch Arbeitshypothese) gegenteilig zur Nullhypothese formuliert ist. Somit kann die Arbeitshypothese als wahr angesehen werden, sofern die Nullhypothese verworfen werden muss.

Nullhypothese (H_0):

Das Spielen eines Lernspiels zu dem Themenfeld Social Engineering hat keinen positiven Einfluss auf die Sensibilisierung bezüglich Social Engineering.

Alternativhypothese (H_1):

Das Spielen eines Lernspiels zu dem Themenfeld Social Engineering hat einen positiven Einfluss auf die Sensibilisierung bezüglich Social Engineering.

Es ist anzumerken, dass die Hypothesen gerichtet sind. D.h. nicht bloß das Vorhandensein eines Effekts ist relevant, sondern ebenso die Richtung des potentiellen Einflusses (etwa positiv, negativ oder nicht vorhanden). Ein Lerneffekt, und damit die Sensibilisierung, kann also auch negativ sein.

Basierend auf der Literatur, welche im Grundlagenkapitel 3 erläutert wird, sowie den Überlegungen bezüglich einer spielerischen Sensibilisierung mittels Serious Games, ist der zu erwartende Effekt grundsätzlich positiv. D.h. es wird von einer Sensibilisierung der Spieler für Social Engineering ausgegangen. Da vergleichbare Erhebungen nicht vorliegen, wird eine mittlere Effektgröße angenommen.

1.4 Struktur der Arbeit

Die vorliegende Arbeit besteht aus insgesamt acht Kapiteln. Das erste Kapitel 1 wird mit einer Motivation eingeleitet und das Ziel des Forschungsvorhabens erläutert. Kapitel 2 gibt einen Überblick über themenverwandte Arbeiten und bisherige Forschungsergebnisse. In Kapitel 3 werden die Grundlagen erläutert und in die Terminologie eingeführt. Das Kapitel 4 beschreibt die Intervention der Studie, welche in Kapitel 5 genauer abgehandelt wird. Im darauffolgenden Kapitel 6 wird die Durchführung des wissenschaftlichen Experimentes dokumentiert. Die Ergebnisse der Studie werden in Kapitel 7 statistisch ausgewertet und interpretiert. Kapitel 8, und damit das letzte Kapitel, bildet den inhaltlichen Schluss mit einem Fazit und einem Ausblick.

Kapitel 2

Related work

Dieser Arbeit ging eine systematische Literaturrecherche voraus. Diese deckt sich mit einer groß angelegten Metaanalyse von Köhler und anderen.[KRW] Eine Auswahl an verwandten Forschungsarbeiten wird nachfolgend vorgestellt.

Beckers et al. haben 2016 das Serious Game¹ HATCH (Akronym für Hack And Trick Capricious Humans) entwickelt, welches als Training für Social Engineering konzipiert ist. [BPF16] Das Spielprinzip beruht darauf, dass Spieler für ein fiktives Szenario Angriffsvektoren des Social Engineerings erörtern sollen. Anschließend wird die Überlegung des Spielers in einer Gruppendiskussion auf ihre Machbarkeit hin diskutiert. Beckers und Pape geben an, dass die Testpersonen im Stande waren plausible Angriffsvektoren zu identifizieren. Von insgesamt 25 Spielern wurde für 14 Testpersonen ein Lerneffekt bestimmt. Hierzu mussten die Probanden ihre Zustimmung gegenüber verschiedenen Aussagen äußern. Dabei wurden 14 Items auf einer Likert-Skala aufgetragen. Diese sind nicht näher beschrieben. Insgesamt wird eine Steigerung der "security awareness" nach dem Spielen von HATCH verzeichnet.[BP16]

Zu den verwandten Arbeiten zählt ebenso das Kartenspiel Control-Alt-Hack aus dem Jahr 2012, welches von Denning und anderen realisiert wurde.[Den+13] Das Spiel soll auf spielerische Art und Weise ein Bewusstsein für IT-Sicherheit schaffen. Im Kon-

¹der Begriff Serious Game ist in Kapitel 3.2 definiert

trast zu dieser Arbeit liegt der Fokus von Control-Alt-Hack also nicht ausschließlich auf dem Themenfeld Social Engineering. Ob ein Lerneffekt ("awareness") geschaffen wird, wurde primär anhand standardisierter Fragenbögen im Rahmen einer Online-Befragung von 22 Pädagogen ("educators") bestimmt. Diese hatten zuvor ein Exemplar des Spiels angefordert. Der überwiegende Teil der Pädagogen gab eine Sensibilisierung der Schüler an. Insgesamt spielten mehr als 450 Schüler das Spiel. Sekundär wurden Ergebnisse einer kleineren Nutzerstudie ausgewertet. Dabei handelt es sich um eine Befragung von 11 Personen, die das Spiel selbst gespielt haben. Hiervon zeigten 8 von 11 Teilnehmenden eine Sensibilisierung.

Newbould und Furnell haben das Brettspiel Playing Safe prototypisch zu Schulungszwecken des Social Engineerings umgesetzt.[NF09] Es wurde durch 21 Spieler evaluiert, von denen 86% der Spieler mittels Selbsteinschätzung angegeben haben, dass ihr Sicherheitsbewusstsein bezüglich Social Engineering gesteigert wurde. Daneben beschreiben die Forscher eine Korrelation: Je mehr Zeit der Spieler online verbringt, desto höher scheint der erreichte Punktwert im Spiel zu sein.

Scholl ist eine Mitautorin von wissenschaftlichen Arbeiten im Rahmen des Projekts SecAware4job.[Sch19] [Sch+17]. Die Forscherin veröffentlichte noch eine Reihe weiterer Publikationen, in denen zur spielerischen Wissensvermittlung von Informationssicherheit geforscht wird.[Sch] SecAware4job macht sich den Game-based-Learning-Ansatz zu Nutze und adressiert vor allem Schüler und Studierende. Inhaltlich werden bereits viele Aspekte des Social Engineerings thematisiert. Ein dediziertes Spiel für Social Engineering ist derzeit in Planung. Der Lerneffekt durch das Projekt wird in der Kombination aus Vorträgen, analogen und digitalen spielebasierten Lernszenarien sowie interaktiven Übungen gesehen. Genaue Angaben über mögliche Lerneffekte sind nicht beschrieben, da die empirische Basis bisher zu gering sei.

Kapitel 3

Grundlagen

3.1 Social Engineering

Dieses Kapitel dient der Vermittlung aller Grundlagen über das Themenfeld Social Engineering im Kontext der Informationssicherheit. Die erläuterten Aspekte stellen die Basis für das geplante Lernspiel dar. Sie führen jedoch zum Teil inhaltlich weiter als das Wissen, das den Spielern durch das Lernspiel vermittelt werden soll.

3.1.1 Definition

Der amerikanische IT-Sicherheitsberater und professionelle Social Engineer Christopher Hadnagy definiert Social Engineering wie folgt:

The act of manipulating a person to take an action that may or may not be in the "target's" best interest. This may include obtaining information, gaining access, or getting the target to take certain action. [HW10]

Die ersten Berührungspunkte mit Social Engineering haben Menschen im Alltag bereits in sehr jungen Jahren. Beispielsweise durch Eltern, die versuchen den Mund ihrer Kinder auf geschickte Art und Weise zu öffnen, um sie zu füttern. Auch Lehrer, Psychologen, Polizisten und viele andere Berufe haben täglich Berührungen mit diesem Gebiet. [HW10]

Im Kontext der Informationssicherheit bedeutet Social Engineering, dass Angreifer den Menschen als Schwachstelle eines Sicherheitskonstruktes ausnutzen, um technische Sicherheitsmechanismen zu umgehen. Nach dieser zugrundeliegenden Definition betrachten wir Social Engineering, nämlich ausschließlich im Kontext der Informationssicherheit.

3.1.2 Sozialpsychologische Grundlagen

Die verschiedenen Angriffsvektoren des Social Engineerings nutzen per Definition stets menschliches Verhalten aus. Dies ist auch im Kontext der IT-Sicherheit der Fall. Wissenschaftliche Erkenntnisse hierzu sind dem Forschungsbereich der Sozialpsychologie zuzuordnen, also den beiden Forschungsdisziplinen Psychologie und Soziologie. Der Psychologe und emeritierte Professor für Psychologie und Marketing der Arizona State University Robert Beno Cialdini hat 7 Prinzipien der Beeinflussung definiert, denen sich die Social Engineering Angriffe zuordnen lassen. Die Prinzipien werden nachfolgend tabellarisch aufgelistet und erläutert:

Prinzip der Beeinflussung	Beschreibung
Reziprozität (Reciprocity)	Menschen tendieren dazu einen Gefallen zu erwidern.
Commitment und Konsistenz (Commitment and consistency)	Eine einmalige Zusage wird eher beibehalten und gewürdigt, um das Selbstbild zu wahren.
Soziale Bewährtheit (Social proof)	Das eigene Verhalten orientiert sich am Verhalten anderer Menschen.
Sympathie (Sympathy)	Menschen lassen sich eher von Personen beeinflussen, die sie mögen.
Autorität (Authority)	Menschen beugen sich eher dem Urteil von Autoritäten.
Knappheit (Scarcity)	Ein scheinbar knappes Gut erscheint wertvoller.
Zusammengehörigkeit (Unity)	Menschen lassen sich eher von etwas überzeugen, wenn sie es zu ihrer Gruppe gehörend ansehen.

Tabelle 3.1: Prinzipien der Beeinflussung nach Cialdini [Cia13]

Ein grundlegendes Verständnis für die beschriebenen Prinzipien ist erforderlich, um Manipulationsversuche oder Einflussnahme anderer aufdecken und hinterfragen zu können.

3.1.3 Social Engineering Risiken

Die potentiellen Risiken von Social Engineering Angriffen sind von hoher Bedeutung. Die Firma Accenture Plc überführt das Risiko, bestehend aus den Faktoren Eintrittswahrscheinlichkeit und potentielltem Schadensausmaß, in eine Geldsumme, wie im Motivationskapitel 1.1 dargelegt. Dabei beziffern sie die wirtschaftlichen Schäden durch Social Engineering als hoch.[AL19] Die Motive der Angreifer umfassen etwa finanzielle Absichten, Wettbewerbsvorteile oder den Zugang zu Firmengeheimnissen [CS16, Abbildung 2].

3.1.4 Angriffsvektoren

Das Social Engineering umfasst eine beträchtliche Anzahl an Angriffsvektoren. [HL15] [CS16] [IJ11] [HW10] [Lon08] Die konkrete Umsetzung der Angriffsvektoren kann sich wiederum in ihrer Ausprägung unterscheiden und verschiedene Spezifika besitzen. Mangels einer akzeptierten Taxonomie wird, basierend auf den in der Literatur beschriebenen Angriffsvektoren, eine eigene Taxonomie erstellt. Diese ist der Abbildung 3.1 in Form eines Dendrogramms zu entnehmen.

Die in dieser Arbeit vorgestellte Kategorisierung der Angriffsvektoren sieht im Wesentlichen eine Unterteilung in Technical-based Social Engineering (TBSE) und Human-based Social Engineering (HBSE) vor. TBSE beschreibt Techniken unter Zuhilfenahme von technischen Hilfsmitteln. HBSE beschreibt Angriffe ohne technische Hilfsmittel. Die vorgestellte Kategorisierung ist inhaltlich sehr nahe zu verschiedenen Klassifikationsschemata anderer Publikationen. So schlagen Foozy et al. [Foo+11] ebenfalls die Unterscheidung von Human-based bzw. Technical-based Social Engineering vor. Marcus Lipski kategorisiert die Angriffsvektoren des Social Engineerings ähnlich, er

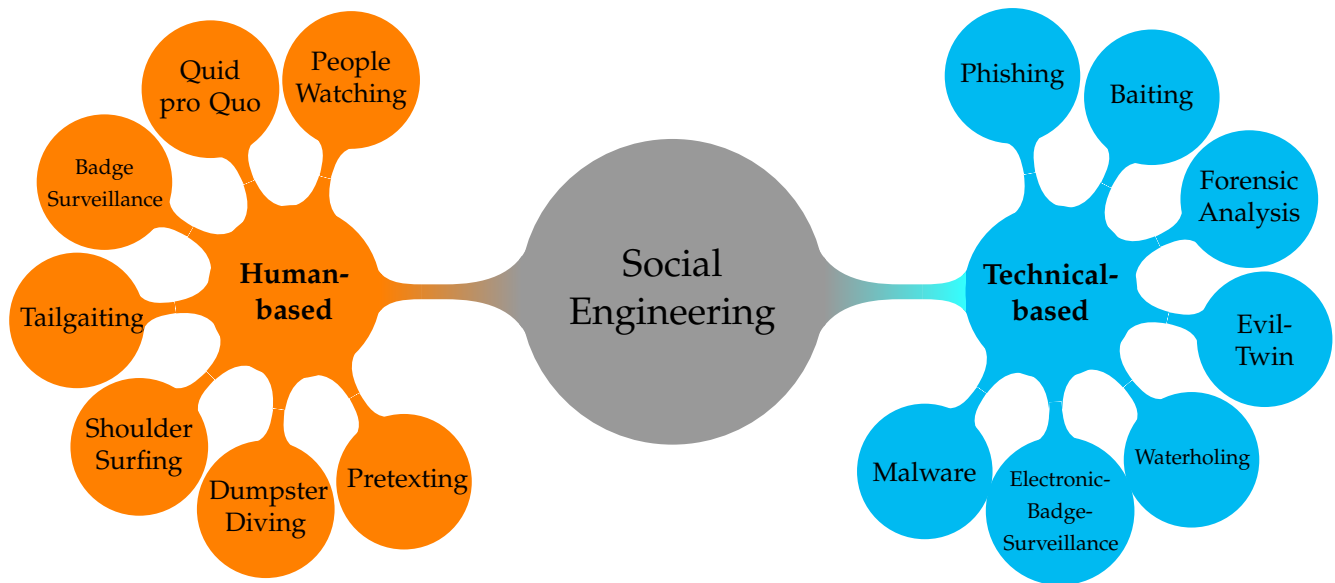


Abbildung 3.1: Taxonomie der Angriffsvektoren des Social Engineerings

führt jedoch eine dritte Kategorie „Reverse Social Engineering“ ein [Lip09, S. 7-9]. Dabei handelt es sich um Angriffe, die das Opfer selbst triggert. Heartfield et al. weichen von den bisher vorgestellten Arbeiten ab und definieren zusätzlich verschiedene Formen der Malware (etwa Virus, Trojaner und Wurm) als Angriffsvektoren des Social Engineerings [HL15].

3.1.4.1 Technical-based Social Engineering

Technical-based Social Engineering beschreibt die Durchführung von Angriffen mit Hilfe von technische Hilfsmittel. Diese werden dazu verwendet Informationen über die Opfer zu sammeln, mit diesen in Kontakt zu treten oder die Opfer anderweitig über technische Hilfsmittel zu manipulieren. In diesem Unterkapitel werden gängige TBSE-Angriffe aufgelistet und beschrieben.

Phishing

Phishing bezeichnet einen Angriff, der sowohl gezielt gegen einzelne Person, aber auch gegen eine Gruppe von Personen erfolgen kann. Der Angriff erfolgt üblicherweise durch Vortäuschung einer falschen Identität bzw. eines falschen Vorwands (Pretext). Die Ziele von Phishing Angriffen können sehr variieren. Im Allgemeinen wird versucht, die Opfer zu Aktionen zum eigenen Vorteil zu bewegen. Beispielsweise das

Herunterladen und Ausführen von schädlichen Dateien, die an eine E-Mail angehängt sind. Es gibt verschiedene Varianten des Phishings. Darunter befinden sich etwa Spear-Phishing (zielgerichtete Phishing-Angriffe auf Einzelpersonen), Whaling (Phishing von hochrangigen Mitarbeitern) und Vishing (Phishing auf telefonischem Wege).[IJ11]

Baiting

Bei einem Baiting Angriff verteilt der Angreifer externe Speichermedien, wie CDs oder USB-Sticks an Orten, an denen diese leicht gefunden werden können. Dabei wird die Neugierde der Menschen ausgenutzt, damit sie über ihre Computer auf diese Speichermedien zugreifen, um den Inhalt abzurufen. Die Computer werden dann durch die vermeintlichen Speichermedien (z.B. Rubber Ducky¹) oder durch den Inhalt auf diesen infiziert.[CS16]

Forensic Analysis

Forensic Analysis kann im Social Engineering Kontext auch als elektronisches Dumpster Diving angesehen werden. Ebenso wie beim Durchsuchen von Müll ist es möglich, entsorgte Speichermedien zu untersuchen. Dabei werden solche Datenträger auf forensische Weise analysiert, um auf diesen vertrauliche Informationen zu finden.[HL15]

Evil-Twin

Ein Evil-Twin ist ein WLAN-Access-Point, welcher einen legitimen Accesspoint nachahmt. Ziel ist es, dass sich Benutzer fälschlicherweise mit diesem verbinden und Angreifer so die Verbindung ausspähen können oder Benutzerdaten abgreifen. Dabei werden der Name (SSID) und möglichst alle anderen Einstellungen des legitimen Accesspoints kopiert bzw. nachgeahmt.[HL15]

¹Der Rubber Ducky ist ein Microcontroller, welcher aussieht wie ein USB-Stick und sich verhält wie ein automatisiertes Eingabegerät.

Waterholing

Waterholing oder Watering-Hole Angriffe werden meist auf Unternehmen mit hohen Sicherheitsstandards ausgeführt. Dabei versucht der Angreifer vorher die Gewohnheiten der Mitarbeiter zu analysieren, primär jedoch die besuchten Webseiten externer Unternehmen (etwa die Website der Kantine). Die Seiten mit geringeren Sicherheitsstandards werden nach Sicherheitslücken durchsucht, um diese mit Schadsoftware zu infizieren. Ziel ist es die Computer der Mitarbeiter des Zielunternehmens mit Schadsoftware zu infizieren, sobald diese die jeweiligen Websites besuchen.[HL15]

Electronic Badge Surveillance

Electronic Badge Surveillance ist das elektronische Gegenstück zum Badge Surveillance. Dabei wird versucht die Funktionsweise und Daten der Chips auszulesen und zu kopieren.[Lon08]

Malware

Malware umfasst sämtliche Arten von Schadprogrammen, wie etwa Viren, Würmer oder Trojaner. Sie wird in der Literatur in der Regel nicht zu den Angriffsvektoren des Social Engineerings gezählt. Jedoch besteht eine starke Assoziation zwischen Malware und Social Engineering. So erfolgt die Verbreitung von Malware oftmals durch Angriffsvektoren des Social Engineerings; etwa durch Phishing. Social Engineering ist jedoch nicht ausschließlich ein unterstützendes Werkzeug in Hinblick auf die Malware. Auch die umgedrehte Kausalität trifft zu. So sind Malware-gestützte Social Engineering Angriffe nicht unüblich. Diese Subkategorie der Malware wird als Scareware² bezeichnet.[HL15]

²Scareware ist ein Schadprogramm (Malware), welches Computerbenutzer verängstigen und so zu bestimmten Handlungen bewegen soll.

3.1.4.2 Human-based Social Engineering

Anders als beim TBSE werden HBSE-Angriffe ohne jegliche technische Hilfsmittel durchgeführt. Der Angreifer nutzt direkt menschliche Eigenschaften aus, um seine Ziele zu erreichen. Bei diesen Angriffen treten die Angreifer meist in direkten Kontakt mit dem Opfer, was jedoch nicht zwingend notwendig ist. Im Folgenden werden gängige HBSE-Angriffe genauer erläutert.

Pretexting

Ein Pretext ist im Social Engineering eine Technik, in der ein Angreifer ein Szenario erfindet, welche es ihm leichter macht, das Opfer zu beeinflussen. Dieser Angriff nutzt primär den Wunsch nach Konsistenz von Menschen aus. Ziel ist es, ein vertrautes Verhältnis zum Opfer aufzubauen, damit dieses die gewollten Aktionen durchführt, ohne diese weiter zu hinterfragen. Typischerweise geben sich Angreifer als Vertrauenspersonen, wie Vorgesetzte oder IT-Support Mitarbeiter aus.[HW10]

Dumpster Diving

Als Dumpster Diving wird das Durchsuchen von Müll nach brauchbaren Informationen bezeichnet. Viele Menschen gehen leichtfertig mit vertraulichem und vermeintlich nicht vertraulichem Papiermüll um und entsorgen diese in einer gewöhnlichen Mülltonne. Somit können beispielsweise Telefonlisten oder Kalender dazu genutzt werden um ein weiteres Vorgehen zu planen.[Lon08]

Shoulder Surfing

Shoulder Surfing ist eine triviale Technik, bei der versucht wird, Passwörter oder andere vertrauliche Informationen vom Opfer zu erspähen. Bei diesem Angriff steht der Angreifer meist direkt hinter dem Opfer und beobachtet den Bildschirm oder die Tastatureingaben. Es ist jedoch auch möglich, diesen Angriff mittels Kameras, Ferngläser oder anderem Werkzeug über Entfernung durchzuführen.[Lon08]

Tailgating

Beim Tailgating bzw. Piggybacking nutzt ein Angreifer die Hilfsbereitschaft oder Unachtsamkeit des Opfers aus, um unautorisierten Zugang zu physisch gesicherten Bereichen zu erlangen. Dies geschieht beispielsweise, indem ein Angreifer mit vollen Händen hinter einer Person herläuft, welche diesem die Tür aufhält.[IJ11]

Badge Surveillance

Dieser Angriff besteht in erster Linie darin, Zugangskarten von Personen zu beobachten, um diese im nächsten Schritt zu fälschen. Ein Angreifer, der eine echt aussehende Zugangskarte bei sich trägt, kann das Risiko eines Fehlschlags minimieren.[Lon08]

Quid pro Quo

Quid pro Quo ist die Ausnutzung des Reziprozitätsverhaltens von Menschen. Dabei fordern Angreifer Informationen vom Opfer im Tausch gegen für das Opfer gleichwertig erscheinende Informationen oder wünschenswerte Gegenstände. Ein einfaches Beispiel hierfür ist die Bestechung eines Mitarbeiters, ihm Geld für sein Passwort anzubieten.[CS16]

People Watching

People Watching ist, wie der Name bereits verrät, die Beobachtung von Menschen. Dabei tritt der Angreifer nicht in direkten Kontakt mit dem Opfer, sondern beobachtet dieses aus der Ferne. Es wird versucht, anhand der Kleidung, dem Verhalten, Umgang mit Menschen oder präferierter Orte, ein genaues Bild vom Opfer zu machen. Erkenntnisse werden dann für weitere Angriffe ausgenutzt.[Lon08]

3.1.5 Gegenmaßnahmen

In der Literatur sind vielfältige Maßnahmen gegen die Angriffsvektoren des Social Engineerings beschrieben.[CS16] [HL15] In den meisten Fällen sind jedoch keine Angaben über die Wirksamkeit der Maßnahmen aufgeführt. Prinzipiell können sie lediglich den Erfolg eines Angriffs minimieren. Die Umsetzung der Maßnahmen garan-

tiert jedoch keinen vollständigen Schutz. In dieser Arbeit werden Gegenmaßnahmen danach unterteilt, ob sie allgemein wirksam sein können oder spezifisch bestimmte Angriffsvektoren adressieren.

3.1.5.1 Allgemeine Gegenmaßnahmen

Allgemeine Gegenmaßnahmen richten sich hauptsächlich an Verhaltensweisen von Menschen und minimieren so den Erfolg eines Angriffs unabhängig vom Angriffsvektor. Dies beinhaltet Richtlinien, Verbote und andere Maßnahmen. Im Folgenden werden einige allgemeine Gegenmaßnahmen erläutert.

Awareness Kampagnen

Ein prominentes Beispiel in der Literatur sind Awareness Kampagnen. Das Ziel solcher Kampagnen ist es, eine langfristige Verhaltensänderung von Mitarbeitern zu erreichen. Inhaltlicher Kern einer solchen Kampagne, welche über einen längeren Zeitraum von bis zu mehreren Jahren verläuft, ist üblicherweise das Regelwerk der Sicherheitsrichtlinien des Unternehmens. Dabei werden verschiedene Methoden angewendet, um die Aufmerksamkeit zu erhöhen und Wissen zu teilen, wodurch die Sensibilität (User-Awareness) erhöht werden soll. Typische Instrumente, die verwendet werden sind etwa Flyer, Plakate, Schulungen und die Evaluierung des Sicherheitsbewusstseins mittels Social Engineering Penetrationstests.[FK05]

Social Engineering Penetrationstests

Ziel eines Social Engineering Penetrationstests ist es, die Sicherheitsstruktur eines Unternehmens hinsichtlich seiner Beständigkeit gegen tägliche, reale Gefahren zu überprüfen. Die Wirksamkeit der implementierten Sicherheitsmaßnahmen gegen potenzielle Bedrohungen wird durch simulierte, strukturierte und systematische Angriffe überprüft. Insbesondere wird dadurch das Sicherheitsbewusstsein der Mitarbeiter und die User-Awareness validiert.[FK05]

Richtlinien

Richtlinien sind im Kontext dieser Arbeit Handlungsanweisungen und Empfehlungen, welche vor dem Schaden von Social Engineering Angriffen schützen sollen. Richtlinien bieten einen übergreifenden Schutz vor verschiedenen Angriffsvektoren, da diese gezielt das Verhalten der Menschen regeln. Einige dieser Richtlinien sind im Folgenden beschrieben.[ANM18]

Passwortrichtlinie: Diese Richtlinie regelt den allgemeinen Umgang mit Zugangsdaten und beinhaltet Empfehlungen zur Wahl eines sicheren Passworts.

Informationsklassifizierung: In dieser Richtlinie werden die Vertraulichkeit und der Umgang mit Informationen geregelt, sodass Mitarbeiter wissen, wie sie mit welchen Informationen umgehen.

Clear Desk Richtlinie: Eine Clear Desk Richtlinie fordert Ordnung auf dem Schreibtisch bei längerer Abwesenheit. Dadurch soll verhindert werden, dass sensible Daten zugänglich rumliegen.

Incident-Response-Plan: Im Falle eines Vorfalls müssen Mitarbeiter wissen, wie sie damit umgehen. Dieser Umgang und jeweilige Kontaktpersonen werden in dieser Richtlinie festgehalten.

Social-Media Policy Es werden häufig Fotos oder Inhalte in sozialen Medien gepostet, welche sensible Informationen beinhalten können. Die Anweisungen in dieser Richtlinie sollen das verhindern.

3.1.5.2 Spezifische Gegenmaßnahmen

Gegenmaßnahmen, die bestimmte Angriffe adressieren, werden im Kontext dieser Arbeit als spezifische Gegenmaßnahmen bezeichnet. Eine solche Gegenmaßnahme kann dabei eine oder mehrere Angriffsvektoren adressieren. Im Folgenden sind beispielhaft für die Angriffsvektoren Phishing und Dumpster Diving gängige spezifische Gegenmaßnahmen erläutert.

Maßnahmen gegen Phishing

Phishing-Angriffe erfolgen in den meisten Fällen mittels E-Mails. Typische Gegenmaßnahmen gegen Phishing sind E-Mail Signaturen, wodurch die Authentizität von E-Mails gewährleistet werden kann. Spamfilter können dabei helfen, die Mehrheit von Phishing E-Mails zu blockieren, bevor sie einen Posteingang erreichen. Eine weitere Gegenmaßnahme ist die Verwendung eines Sender Policy Frameworks (SPF), E-Mail-Authentifizierungsmethode, mit der gefälschte Absenderadressen während der Zustellung von E-Mails erkannt werden.[SK19]

Maßnahmen gegen Dumpster Diving

Wie in Kapitel 3.1.4 beschrieben, wird das Durchsuchen von Müll nach brauchbaren Informationen als Dumpster Diving bezeichnet. Maßnahmen um den Erfolg eines solchen Angriffs zu verringern richtigen sind entsprechend an der Entsorgung und Überwachung von Müll. Eine verschlossene Datentonne und die Vernichtung mittels Aktenvernichter oder durch einen professionellen Dienstleister ist eine gängige Methode, um Papiermüll sicher zu entsorgen. Dies verhindert weitestgehend, dass vertrauliche Informationen im normalen Abfall zu finden sind, vorausgesetzt, dass das Papier auch darin entsorgt wird. Außerdem kann der Zugang zu Abfallbehältern kontrolliert werden, damit Unbefugte sie nicht durchsuchen können, falls doch vertrauliche Informationen in die Abfallentsorgung gelangt sind.[SK19]

3.2 Serious Game

3.2.1 Definition

Der Begriff "Serious Game" kann als Fremdwort sinngemäß in "ernsthaftes Spiel" übersetzt werden und ist sprachlich ein Oxymoron³. Über die Bedeutung des Terminus "Serious Game" herrscht in der Literatur immer wieder Uneinigkeit. Dies ergeben eine Literaturrecherche[Det+11][MHZ16] sowie eine aktuelle Diskussion der

³Ein Oxymoron ist eine Formulierung aus zwei gegensätzlichen oder sich einander widersprechenden Begriffen. Dabei ist der Widerspruch absichtlich gewählt.

Wortherkunft in der Literatur[Dja+11]. Eine passende und klare Definition des Begriffs "Serious Game" postulierte Clark Abt im Jahr 1970 in seinem gleichnamigen Buch "Serious Game":

Games may be played seriously or casually. We are concerned with serious games in the sense that these games have an explicit and carefully thought-out educational purpose and are not intended to be played primarily for amusement. This does not mean that serious games are not, or should not be, entertaining. [Abt70]

Mit dem Aufkommen der Digitalisierung in den 2000er Jahren prägte Sawyer et al. eine neue Definition, die ausschließlich digitale Spiele in die Definition einbezieht:

Any meaningful use of computerized game/game industry resources whose chief mission is not entertainment. [Saw07]

In dieser Arbeit wird Bezug auf die ursprüngliche weitgehendere Definition genommen, wonach Serious Games sowohl digitale als auch nicht-digitale Spiele sind, die nicht in erster Linie der Unterhaltung und zugleich Bildungszwecken dienen. Die Charakteristik eines Spiels wird in der nachfolgenden Sektion beschrieben.

3.2.2 Abgrenzung und verwandte Konzepte

Neben dem Serious Game beschäftigt sich die Spielwissenschaft mit weiteren ähnlichen Konzepten. Im Folgenden soll daher eine Unterscheidung hinsichtlich einem Spiel, Gamification sowie Edutainment beschrieben werden.

Spiel

Das Spiel ist als eine Oberkategorie des Serious Games zu verstehen und hat nicht das primäre Ziel einem Bildungszweck zu genügen. Die Bedeutung des Begriffs Spiel wird hinsichtlich einzelner Aspekte kontrovers diskutiert. Jedoch scheint in der Literatur mehrheitlich eine vorgeschlagene Definition nach Clark C. Abt aus dem Jahr 1968 akzeptiert zu sein. Demnach handelt es sich bei einem Spiel um Folgendes:

Any contest (play) among adversaries (players) operating under constraints (rules) for an objective (winning, victory pay-off). [Ste16]

Bei einem Spiel handelt es sich also um eine Partie, in der Spieler unter Einhaltung eines Regelwerks ein bestimmtes Ziel erreichen wollen.

In der englischen Sprache werden oftmals die Begrifflichkeiten Playing und Gaming unterschieden. So stellen die zwei Begriffe nach Caillois verschiedene Aktivitäten dar.[Cai61] Playing, welches er als "Paidia" bezeichnet, beschreibt frei formulierte, nicht regelbasierte und ausdrucksstarke Handlungen wie etwa das Spielen mit einer Puppe. Gaming wird von Caillois als "Ludus" bezeichnet und stellt eine regelbasierte und zielorientierte Spielform dar. Das Konzept Gaming wird weiter beschrieben als eine Aktivität, die freiwillig und unterhaltsam ist, von der realen Welt getrennt, ungewiss, unproduktiv (da die Aktivität keine Güter von äußerem Wert hervorbringt) und von Regeln regiert wird.

Auch aktuellere Forschungsarbeiten bekräftigen eine Unterscheidung zwischen Playing und Gaming[SZ03]. Nach Juul [Juu05] lässt sich Gaming eindeutig anhand von sechs Merkmalen definieren:

1. Ein regelbasiertes formales System
2. Besteht aus variablen und quantifizierbaren Ergebnissen
3. Unterschiedlichen Ergebnissen werden unterschiedliche Werte zugewiesen
4. Anstrengungen des Spielers können das Ergebnis beeinflussen
5. Der Spieler fühlt sich emotional an das Ergebnis gebunden
6. Spiele können Folgen auf das reale Leben haben

Letztendlich wird diese Definition nach Juul im Rahmen dieser Forschungsarbeit präferiert, da sie den Begriff Spiel bzw. Game eindeutig anhand von Kriterien beschreibt.

Gamification

Der Terminus Gamification ist von seiner Bedeutung her verwandt mit dem Serious Game. Im Gegensatz zu den Serious Games handelt es sich jedoch lediglich um das Ergänzen von einzelnen Spielelementen oder spielerischen Aspekten. D.h. nach erfolgter Gamifizierung entsteht kein Spiel nach der beschriebenen Definition. Ebenso unterscheidet sich Gamification darin, dass Bildungszwecke kein zwingender Bestandteil sind. Eine Definition nach Deterding et al. lautet:

Gamification is defined as the use of game design elements in non-game contexts. [Det+11]

Der Forscher Deterding illustriert die Beziehung von Gamification und Serious Games, wie in Abbildung 3.2 dargestellt.

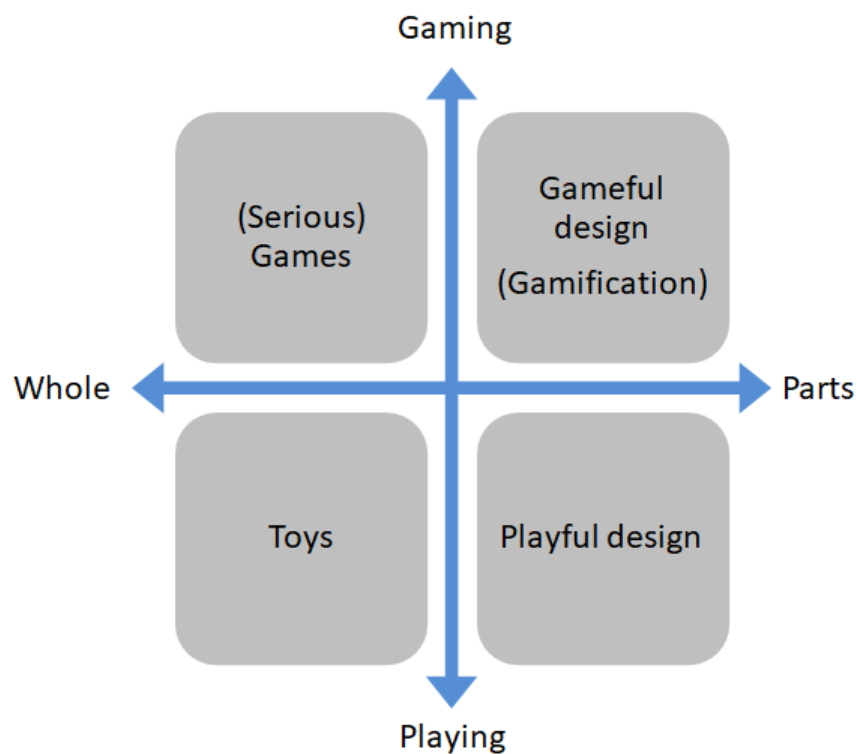


Abbildung 3.2: Einordnung von Spielmodellen nach Deterding[Det+11]

Demnach erfüllen sowohl Gamification als auch das Serious Game Aspekte eines Spiels, jedoch ist nur das Serious Game als ein vollwertiges Spiel zu verstehen.

Toys und Playful design

Deterding et al. grenzen zusätzlich die Begriffe Toys ("Spielzeug") sowie Playful design ("spielerische Gestaltung") von den bereits genannten Begriffen ab. Sie stellen jeweils das Spielen im Sinne des Playings dar und sind somit nicht regelbasiert. Dabei erfüllt das Playful design nur in Teilen die Definition des Playings.

Edutainment

Edutainment setzt sich aus den englischen Wörtern education (Bildung) und entertainment (Unterhaltung) zusammen und beschreibt ein Konzept, das die Verbindung beider Elemente vorsieht. Es handelt sich jedoch um ein rein additives Konzept, bei dem klassische Lernmethoden um eine unterhaltende Komponente zur vermeintlichen Steigerung der Lernmotivation ergänzt werden.[RW06] Die Unterhaltung findet zeitlich separat zur Bildung statt.

Ritterfeld und Weber postulieren drei Paradigmen für das Edutainment. Davon ordnen sie der derzeitigen Umsetzung von Edutainment insbesondere zwei Paradigmen zu. Das Motivationsparadigma ("Motivation Paradigm") beschreibt Unterhaltung als einen "Köder" für unbeliebte Lernmethoden, wie etwa dem Auswendiglernen. Das Belohnungsparadigma ("Reinforcement Paradigm") kehrt die kausale Abfolge um und nutzt Unterhaltung als Belohnung für eine abgeschlossene Lernpassage.[RW06] Dem Lernenden wird dabei meist schnell bewusst, dass die Unterhaltung nur einen Vorwand darstellt. Resultierend daraus sinkt die Motivation zum Lernen. Klopfer et al. bezeichnen das Problem sinnbildlich als "Brokkoli-Schokoladen-Problem"[KOS+09, Seite 18] und sprechen sich gegen das Konzept Edutainment aus.

Abbildung 3.3 illustriert die beschriebenen Paradigmen nach Ritterfeld und Weber. Ein drittes Paradigma stellt das Vermischen der zeitlichen Abfolge dar ("Blending Paradigm"), welches unter Forschern als wesentlich vielversprechender gilt. Es besagt, dass der Lernprozess selbst unterhaltend sein soll. Diesem Paradigma folgen auch die Serious Games und grenzen sich damit von Edutainment ab.

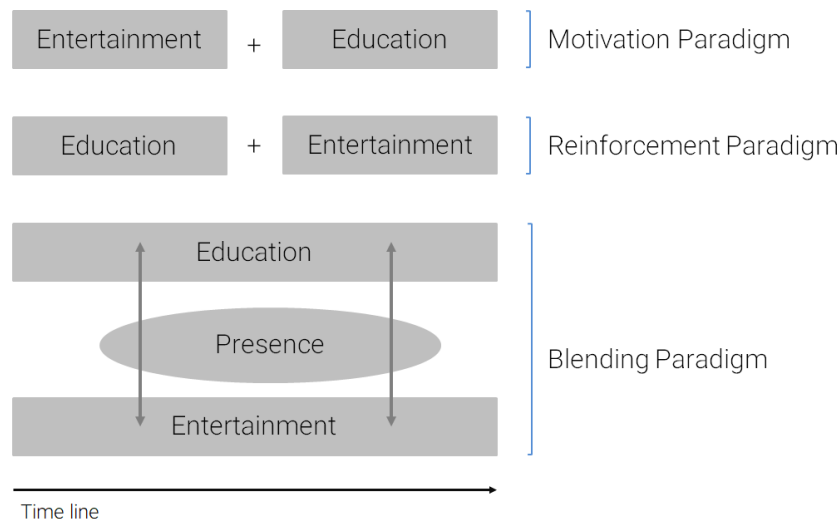


Abbildung 3.3: Paradigmen des Edutainments [RW06, Abbildung 26.2]

3.2.3 Design eines Serious Games

Die Forscher Hunicke et al. postulieren im Jahr 2004 ein formales Modell für das Erstellen von Spielen, welches sie MDA-Framework nennen.[HLZ04] Das Akronym MDA steht dabei für Mechanics, Dynamics und Aesthetics. Das in Abbildung 3.4



Abbildung 3.4: MDA-Framkework nach Hunicke et al.[HLZ04]

illustrierte Modell wird in der aktuellen Literatur häufiger zitiert[MHZ16] und dient in Teilaspekten als Orientierung für die Erstellung des Lernspiels SANIAG. Die drei Bestandteile werden nachfolgend erläutert.

3.2.3.1 Spielmechaniken (Game mechanics)

Spielmechaniken sind Elemente, die ein Spiel nach der Definition von Juul zu einem Spiel machen [Juu05]. Die Spielmechaniken ermöglichen die Quantifizierung von Spielergebnissen und erzeugen Spielanreize. Die Forscher führen beispielhaft verschiedene Spielmechaniken aus. Dabei referenzieren sie ein Whitepaper "Gamification 101"[Bun10] der Firma Bunchball Inc, welche als Unternehmen hauptsächlich Dienstleistungen zu Gamification anbietet. Zu den Spielmechaniken gehören[MHZ16]:

Punkte:	Sie repräsentieren den Erfolg eines Spielers im Spiel und sind zugleich eine Belohnung.
Level:	Level zeigen einem Spieler leicht verständlich dessen Fortschritt an und haben eine Außenwirkung.
Herausforderung:	Das Bewältigen nicht trivialer Aufgaben bedeutet sich von anderen Spielern abheben zu können.
Virtuelle Güter:	Der Besitz drückt Wohlstand und Macht aus.
Ranglisten:	Ranglisten stellen eine hierarchische Auflistung der Spieler dar, welche dazu dient, die Leistungen aller Spieler zu visualisieren.
Wohltätigkeit:	Hierbei steht die soziale Interaktion zwischen den Spielern im Vordergrund.

3.2.3.2 Spielanreize (Game dynamics)

Spielanreize dienen der Abdeckung grundlegender menschlicher Wünsche und Bedürfnisse im Spiel [KKK18]. Sie sind als eine Folge der Spielmechanik zu verstehen und existieren in jedem Menschen, sind jedoch individuell unterschiedlich stark ausgeprägt. Zu den Spielanreizen zählen mitunter [MHZ16]:

Belohnung:	Etwas von Wert, das man für eine Aktion erhält.
Status:	Das Bedürfnis nach Anerkennung und Respekt.
Erfolg:	Aufgaben, die durch Erfüllung bestimmter Anforderungen zum Ziel führen.
Selbstdarstellung:	Das Bedürfnis, sich einzigartig zu fühlen.
Wettbewerb:	Leistungssteigerung im Wettbewerbsumfeld.
Altruismus:	Uneigennützig handeln, um Beziehungen zu pflegen.

Die Beziehung zwischen Spielmechaniken zu Spielanreizen wird in Tabelle 3.2 verdeutlicht. Dabei kennzeichnen die Symbole ● menschliche Bedürfnisse, die eine Spielmechanik primär erfüllt. Das verwendete Symbol ◐ bedeutet ein menschliches Bedürfnis, das eine Spielmechanik nur zum Teil bzw. sekundär erfüllt. Beispielsweise lösen Spiele mit einem Punktesystem das Gefühl der Belohnung bei den Spielern aus.

	Menschliche Bedürfnisse					
Spielmechanik	Belohnung	Status	Erfolg	Selbstdarstellung	Wettbewerb	Altruismus
Punkte	●	◐	◐		◐	◐
Level		●	◐		◐	
Herausforderung	◐	◐	●	◐	◐	◐
Virtuelle Güter	◐	◐	◐	●	◐	
Ranglisten	◐	◐			●	◐
Wohltätigkeit		◐	◐		◐	●

Tabelle 3.2: Beziehung von Spielmechaniken und Spielanreizen [MHZ16]

3.2.3.3 Ästhetik (Aesthetics)

Hunicke et al. erkannten verschiedene Ästhetiken als grundlegende emotionale Beweggründe, ein Spiel zu spielen. Sie spiegeln die Sichtweise des Spielers wider. Insgesamt werden acht verschiedene Ästhetiken identifiziert[HLZ04]:

Sensation: Spiel zum Verwöhnen der Sinne.

Fantasy: Spiel mit surrealen Elementen.

Narrative: Geschichte verkörperndes Spiel.

Challenge: Spiel, bei dem Hindernisse überwunden werden müssen.

Fellowship: Spiel unter sozialen Aspekten.

Discovery: Spiel auf unerforschtem Land.

Expression: Spiel zur Selbstfindung.

Submission: Spiel zum Zeitvertreib.

Ästhetiken sind als eine Folge der Spielmechaniken und Spielanreize zu verstehen. Dabei bedeuten Spielmechaniken die konkrete Umsetzung des Spiels durch den Entwickler. Welche Ästhetiken sich das Serious Game SANIAG zunutze macht, wird im Kapitel 4.2.3 beschrieben.

3.3 Social Engineering Awareness

Der Ausdruck "Social Engineering Awareness" ist in der Literatur nicht einheitlich definiert. So weisen Köhler et al. in ihrer Publikation auf ein mangelndes Bewusstsein für die Bedeutung der verschiedenen Begrifflichkeiten hin.[KRW] Tatsächlich scheint der Terminus in der hohen Anzahl an verwandten Arbeiten eine geringe Verbreitung zu finden. Da es sich bei "Social Engineering Awareness" in Bezug auf diese Arbeit jedoch um einen sehr zutreffenden Begriff handelt, wird dieser eigens definiert.

3.3.1 Definition

Social Engineering Awareness wird in dieser Arbeit wie folgt definiert:

Social Engineering Awareness beschreibt das Wissen, die Einstellung sowie das Verhalten einer Person, welches klar messbar ist, zu dem Themengebiet Social Engineering. Es ermöglicht einer Person Gefahren des Social Engineerings zu erkennen und angemessen darauf zu reagieren. Es handelt sich dabei nicht erforderlicherweise um technisches Expertenwissen.

Diese Definition ist angelehnt an Kruger und Kearney, die die drei zu messenden Merkmale Wissen, Einstellung und Verhalten zur Objektivierung der Awareness postulierten [KK06]. Die Forscher beziehen sich in ihrer Publikation auf die Bestimmung

der "information security awareness". Der Begriff "awareness" wird durch das NIST definiert und ist weitläufig akzeptiert als:

Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly." [WH03]

Dabei definiert das NIST den Begriff im Kontext von "information technology security awareness.

In unserer Definition wird explizit die Notwendigkeit der Messbarkeit gefordert. Dabei kann die Messmethode etwa einen Fragebogen wie in dieser Arbeit einschließen. Auch wird das Themengebiet auf Social Engineering beschränkt. Weshalb eine neue Definition sinnvoll ist. In welcher Hinsicht eine Abgrenzung zugelassen werden kann, wird in der folgenden Sektion erläutert. Im Rahmen dieser Arbeit wird der verkürzte Term Awareness synonym verwendet. Im konkreten Fall der vorliegenden Arbeit leitet sich Awareness von der Messmethode mittels Fragebogen ab. D.h. die Awareness beschreibt objektivierbare Werte, die aus den Fragebogen hervorgehen.

3.3.2 Abgrenzung

3.3.2.1 Themenfeld

In dieser Arbeit wird ein klarer Bezug auf das Themengebiet des Social Engineerings genommen, das sich anhand einer akzeptierten Definition klar abgrenzen lässt. Da Angriffe auf menschliche Faktoren im Vordergrund stehen sollen, wird in dieser Arbeit bewusst nicht von Begriffen wie "information security awareness" gesprochen.

In anderen Arbeiten wird inhaltlich Bezug auf gleiche Fragestellungen genommen. Jedoch werden verschiedene Begriffe wie "information technology security (IT security)", "information security" oder etwa "cyber security" genutzt, um das Themenfeld

zu beschreiben. Keiner dieser Ausdrücke setzt einen Fokus auf menschliche Schwachstellen. Ebenso adressiert das Social Engineering nicht alle Aspekte der Informationssicherheit oder lässt sich mit IT-Sicherheit gleichsetzen.

3.3.2.2 Kontinuum des Lernens

Dem NIST zufolge lässt sich das Lernen im Bereich IT-Sicherheit in einem mehrstufigen Modell klassifizieren.[WH03, Abbildung 2-1] Es werden konkret die drei Begriffe Awareness, Training und Education unterschieden.

Awareness bedeutet dem NIST zufolge:

Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly. [WH03]

Training bedeutet dem NIST zufolge:

Training strives to produce relevant and needed security skills and competencies. [WH03]

Education bedeutet dem NIST zufolge:

Education integrates all of the security skills and competencies of the various functional specialties into a common body of knowledge ... and strives to produce IT security specialists and professionals capable of vision and pro-active response. [WH03]

Awareness vermittelt also lediglich die notwendige Aufmerksamkeit für ein Thema und richtet sich an alle Personengruppen. Training hingegen soll konkrete Fähigkeiten und Kompetenzen vermitteln. Das Training kann mit einem Zertifikat abgeschlossen werden. Den Begriff der Education definiert das NIST als eine Vermittlung von Wissen an Spezialisten und Experten. Für die Zwecke dieser Studie soll daher von (Social Engineering) Awareness gesprochen werden.

Kapitel 4

Serious Game SANIAG

Um eine spielerische Sensibilisierung bezüglich Social Engineering zu ermöglichen, wird das Spiel "Saed und Niklas' Awareness Game (SANIAG)" entwickelt. Bei dem Spiel handelt es sich um ein Serious Game. In dieser Arbeit wird auch synonym die Bezeichnung Lernspiel verwendet.

4.1 Spielprinzip

SANIAG soll den Spieler in die Rolle eines Beraters für Social Engineering versetzen. Das Ziel der Spieler besteht darin, möglichst viele Kunden an sich zu binden und damit einhergehend auch eine bestimmte Menge an Reputation zu erwerben. Ein Kundenverhältnis entsteht dadurch, dass die jeweiligen Sicherheitsmaßnahmen einer Location gehackt werden. Der Berater versucht hierbei alle Sicherheitsmaßnahmen mittels Würfeln oder Frage- und Antwortaktionen zu umgehen. Gelingt ihm das, so gewinnt er diese Location als Kunden und kann weitere Sicherheitsmaßnahmen implementieren. Somit fällt es dem nächsten Berater schwieriger, alle Sicherheitsmaßnahmen zu umgehen. Falls ein Hack fehlschlägt, so verliert der hackende Berater Reputation an den aktuellen Berater der Location. Die Berater können während des Spiels verschiedene Aktionen ausführen, die dabei helfen, das Hacken einer Location zu vereinfachen oder für andere Spieler zu erschweren.

Die einzelnen Bestandteile des Brettspiels werden in Kapitel 4.4 genauer beschrieben. Eine wesentliche Komponente des Spiels stellen die in Abbildung 4.1 dargestellten Spielkarten dar.

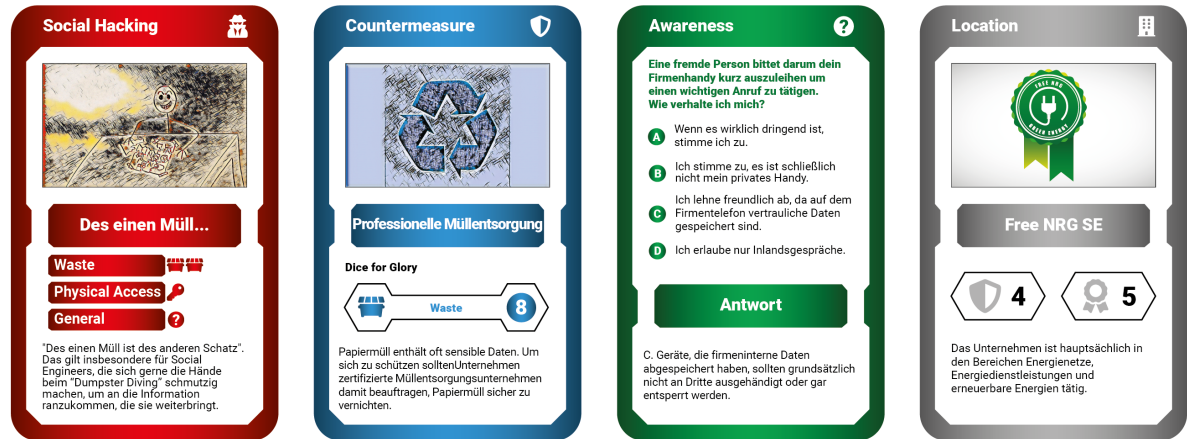


Abbildung 4.1: SANIAG Spielkarten

Rote Hacking-Karten repräsentieren offensive Aktionen, wie das Hacken von Locations. Blaue Countermeasure-Karten spiegeln beratende Tätigkeiten wider und dienen dem Schutz einer Location. Grüne Awareness-Karten beinhalten einen Wissenstest. Graue Location-Karten stellen einen Kunden dar.

4.2 Spieldidaktische Überlegungen

Die Spieldidaktik ist eine Teildisziplin der Spielwissenschaft und befasst sich mit der Bildungswirkung des Spielens, den Zielsetzungen von Spielen sowie Spielmechaniken. Der Umsetzung des Lernspiels SANIAG gingen einige didaktische Überlegungen voraus. Im Vordergrund steht, welche Personengruppen durch welche spezifische Umsetzung des Spiels welche Ziele erreichen sollen.

4.2.1 Zielgruppe

SANIAG soll für Social Engineering Angriffe sensibilisieren. Somit adressiert es alle Personengruppen, die potentiell Opfer von Social Angriffen sein können. Da jede Person das Ziel von Social Engineering sein kann, wird die Zielgruppe in eine Primär-

und Sekundärgruppe unterteilt. Um Begrifflichkeiten und ein gewisses Niveau von Spielmechaniken nutzen zu können, richtet sich das Spiel nur an Personen ab einem Alter von zwölf Jahren oder höher.

4.2.1.1 Primärgruppe

Die Primärgruppe umfasst Menschen mit einem geringen Wissen über die Vorgehensweise des Social Engineerings. Dies umfasst überwiegend Arbeitnehmer, die keine Ausbildung in dem Themenkomplex IT-Sicherheit erhalten haben. Aber auch zukünftige Arbeitnehmer, wie Studierende und Schüler, gehören der primären Zielgruppe an. Die Primärgruppe hat durch die geringen Berührungspunkte und das meist kaum vorhandene Wissen über die IT-Sicherheit den größten Bedarf an einer Sensibilisierung.

4.2.1.2 Sekundärgruppe

Die Sekundärgruppe schließt Personen mit ein, die sich in ihrem Alltag bereits mit der IT-Sicherheit beschäftigen und Social Engineering Angriffe in Ansätzen kennen. Hierzu zählen beispielsweise Studierende in den Bereichen IT-Sicherheit oder Psychologie, Systemadministratoren oder IT-Sicherheitsbeauftragte. Diese Gruppe hat ein geringes bis hohes Wissen über das Themenfeld Social Engineering. Der Bedarf an Sensibilisierung ist daher nicht sehr hoch. Dennoch soll das Lernspiel dazu führen, dass weiteres Wissen erlangt wird, da das Spiel bezogen auf die Thematik Social Engineering sehr umfangreich gestaltet ist.

4.2.2 Spieldesign

Bedingt durch die große Zielgruppe soll das Spiel möglichst eigenständig und unabhängig von Ressourcen wie einem Computer sein. Sowohl in der durchzuführenden Studie als auch in üblichen Schulungsszenarien kann nicht stets der Zugang zu einem Computer für alle Teilnehmenden garantiert werden. Das Spiel soll daher als physisches Brettspiel umgesetzt werden. Weitere Überlegungen, welche bereits didaktische

Elemente aufgreifen, unterstützen die Entscheidung:

1. Alle benötigten Materialien sind im Spiel beinhaltet und es gibt keine Abhängigkeiten zu anderen Materialien oder Geräten.
2. Die Spieler sitzen beieinander und interagieren untereinander, wodurch die Teambildung gefördert werden soll.
3. Es sollen Diskussionen angeregt werden, wodurch sich Lerninhalte besser einprägen lassen.

Um ein geeignetes physisches Spielmodell zu finden, werden vor Beginn der Spielentwicklung diverse verfügbare Spiele evaluiert. Dabei werden insbesondere beliebte Gesellschaftsspiele[Stab] sowie erfolgreiche Kickstarter-Spiele[Staa] betrachtet.

Letztendlich orientiert sich das Serious Game SANIAG an verschiedenen Spielen. Das entworfene Spielbrett zeigt Ähnlichkeiten zu dem Brettspiel des Spieleklassikers Monopoly¹. Die Awareness-Karten orientieren sich am Frageformat der mobilen App Quizduell². Die Reputationsmünzen sowie die Gestaltung der Spielkarten weisen Ähnlichkeiten zu dem Brettspiel Control-Alt-Hack³ auf. Der Mechanismus der Instant-Hacking-Karten ist im Kartenspiel Exploding Kittens⁴ zu finden.

4.2.3 Spielmechaniken und Ästhetiken

Zunächst soll SANIAG den Spieler in eine neue Rolle schlüpfen lassen, die interessant und aufregend erscheinen kann. Der Spieler wird in seiner Rolle nicht nur mit vielen Begrifflichkeiten und Vorgehensweisen zu dem Themenfeld Social Engineering konfrontiert, sondern muss sich auch mit Kundenverhältnissen und seinen Konkurrenten auseinandersetzen, wie dies im realen Leben der Fall ist. Dabei können sich Spieler an vielen Stellen entscheiden, ob sie eine eher offensive oder defensive Strategie verfolgen. Das Hacken soll als spannende Aktivität verstanden werden und ist

¹<https://monopoly.hasbro.com/de-de>, abgerufen am 01.11.2019

²<http://www.quizduell-game.de/>, abgerufen am 01.11.2019

³<http://www.controlalthack.com/>, abgerufen am 01.11.2019

⁴<https://explodingkittens.com/>, abgerufen am 01.11.2019

im normalen Sprachgebrauch oftmals als illegale, reizvolle Tätigkeit konnotiert. Aus Sicht der Spielentwicklung handelt es sich hierbei um einen explorativen Ansatz, der die Neugierde des Spielers anspricht.

Neben der ästhetischen Einordnung des Spiels werden bewusst die im Grundlagenkapitel 4.2.3 thematisierten Spielmechaniken umgesetzt. Die Spielmechaniken führen dazu, dass das Spiel Spaß bereitet, ungeachtet des thematischen Hintergrunds. Alle Spieler befinden sich grundsätzlich im Wettbewerb untereinander. Sie können aber auch Teams ausbilden. Die zu sammelnden Reputationsmünzen sowie der Besitz von Location-Karten stellen eine klare Belohnung dar und sind zugleich ein virtuelles Gut. Welche Countermeasure-Karten zu einer Location gehören ist zunächst unklar und dient damit dem Erzeugen von Spannung. Insbesondere gut gesicherte Lokationen, wie etwa eine Bank, stellen eine besondere Herausforderung dar, an denen sich Spieler messen wollen. Instant Hacking-Karten bringen eine hohe Dynamik in das Spielgeschehen.

4.2.4 Lernziele

Die Spieler sollen während des Spiels für Social Engineering sensibilisiert werden. Sie sollen typische Vorgehensweisen eines Angreifers kennenlernen, deren psychologischen Grundlagen verstehen und eine Akzeptanz für umgesetzte Sicherheitsmaßnahmen entwickeln. Der Lernvorgang soll dabei automatisch und freiwillig durch das Spielen erfolgen. Die Spielmechaniken sind so konstruiert, dass sowohl explizites Lernen als auch implizites Lernen ermöglicht wird.

4.2.4.1 Implizites Lernen

Durch die Kategorisierung der Hacking- und Countermeasure-Karten sollen die Spieler die Zuweisung von Gegenmaßnahmen zu Angriffsvektoren verstehen. Die Gegenmaßnahmen sollen dadurch akzeptiert und im Alltag berücksichtigt werden. Es ist im Spiel nicht möglich, sich gänzlich vor einer Kategorie zu schützen, was ebenso der Realität entspricht. Es ist möglich, die Wahrscheinlichkeit eines erfolgreichen Angriffs

zu minimieren, diesen jedoch nicht zu verhindern. Die Hacking- und Countermeasure-Karten besitzen auf der unteren Hälfte eine Beschreibung, welche den Titel der Karte kurz erläutert. Die Beschreibungen können den Spielern im Spielablauf dazu verhelfen, Awareness-Karten zu beantworten. Dies kann die Spieler dazu motivieren sich die Texte durchzulesen und zu merken. Es ist für den Spielverlauf jedoch nicht zwingend erforderlich. Durch das umfangreiche Thematisieren von Angriffsvektoren und Gegenmaßnahmen, beschränkt sich der Lernfaktor nicht nur auf unwissende Spieler. Experten im IT-Sicherheitsbereich haben ebenfalls die Möglichkeit dazuzulernen.

4.2.4.2 Explizites Lernen

Den expliziten Lerninhalt beinhalten die Awareness-Karten. Ein hackender Spieler muss zur Überwindung der allgemeinen Countermeasures (Kategorie "General") eine bestimmte Anzahl Awareness-Karten korrekt beantworten. Es gibt im Spiel verhältnismäßig wenige Awareness-Karten, sodass diese wiederholt in das Spielgeschehen einbezogen werden. Durch die Wiederholung der Fragen sollen sich die Spieler die korrekten Antworten besser einprägen können.

4.2.4.3 Taxonomiestufen nach Bloom

Lernziele können nach Bloom et al. verschiedenen Taxonomiestufen zugeordnet werden. [BKM84]⁵ Durch die hierarchisch aufgebauten Lernstufen sollen Lernende alle Lernaspekte, über das reine Wissen hinaus, erreichen. Jede Stufe baut auf der vorangehenden Stufe auf und beinhaltet diese. Eine Veranschaulichung der Lernzieltaxonomie zeigt die Abbildung 4.2. Inwieweit das Lernspiel SANIAG mit dem Ziel der Sensibilisierung von Social Engineering den Taxonomiestufen entspricht, wird nun begründet. Hierbei wird auf Beobachtungen aus dem Kapitel 6 vorgegriffen.

Die erste Stufe ist gegeben, da Spieler Faktenwissen erlernen und beibehalten. Das Verständnis und damit die zweite Stufe wird als gegeben angesehen, da Testpersonen

⁵Bloom hat inzwischen eine überarbeitete Taxonomie publiziert. Sie beinhaltet keine relevante Unterscheidung in Hinblick auf diese Arbeit.

Sachverhalte in eigenen Worten wiedergeben und die Korrektheit der Awareness-Karten nachvollziehen können. Die dritte Stufe ist durch die Beantwortung bestimmter Frageformulierungen im Spiel gegeben, wie sich die Spieler in bestimmten Situationen verhalten. Die Spieler analysieren die Situationen, welche in den Awareness-Karten geschildert sind und leiten sich somit die korrekte Antwort her, wodurch auch die vierte Stufe gegeben ist. Durch SANIAG können die Spieler darauf vorbereitet werden, das im Spiel erworbene Wissen langfristig mit dem Arbeitsalltag zu vernetzen. Daraufhin soll das Social Engineering Risiko des eigenen Arbeitsplatzes beurteilt werden können. Hiermit sind auch die fünfte und sechste Stufe der Taxonomie gegeben.

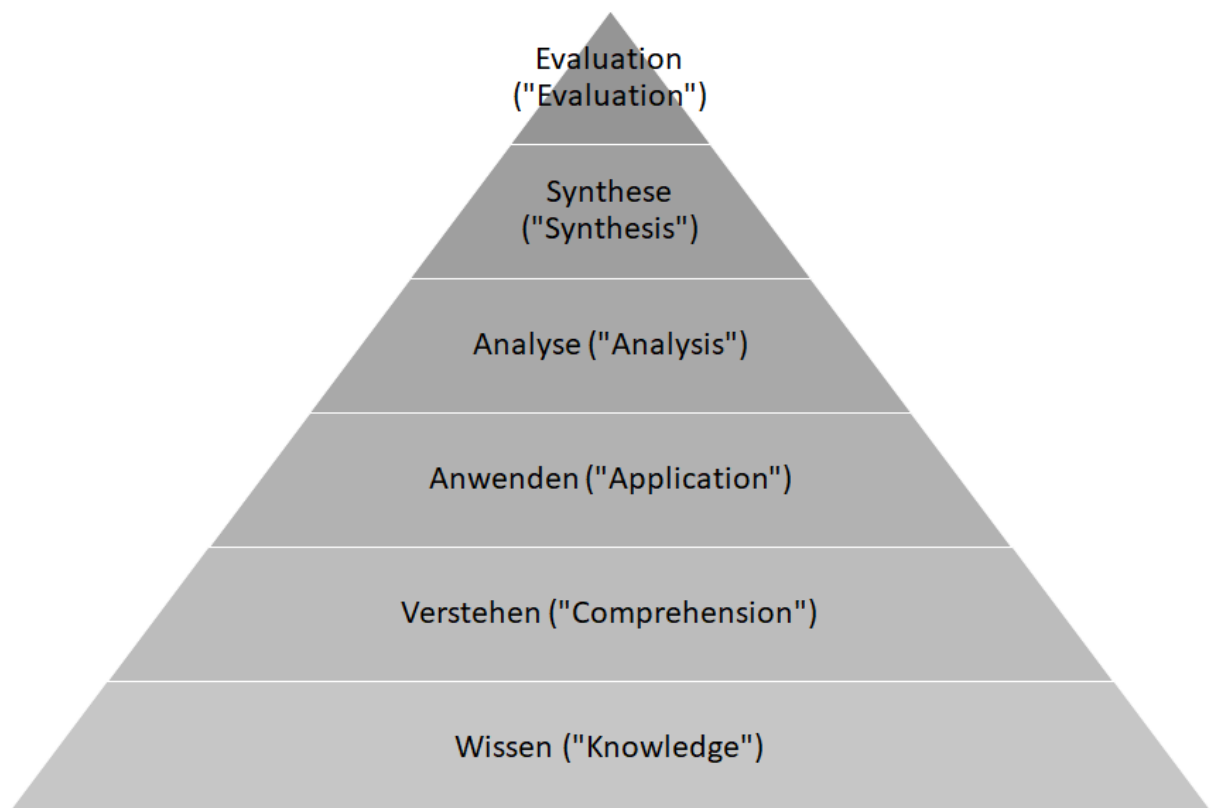


Abbildung 4.2: Taxonomie von Lernzielen nach Bloom [BKM84]

4.3 Entwicklungsprozess

Die Entwicklung des Serious Games SANIAG spiegelt nur einen von vielen Teilspekten der wissenschaftlichen Studie wider. Tatsächlich sind drei Monate des veranschlagten Zeitraums, somit die Hälfte der Zeit, ausschließlich in die Entwicklung

des Spiels investiert worden. Hierunter fallen etwa Arbeiten zu den Spielmechaniken, Spielinhalten und dem Design.

Ein großes Arbeitspaket stellt die Recherche der Spielinhalte dar, welche sich in 274 individuellen Spielkarten widerspiegelt. Die inhaltliche Ausprägung der Karten leitet sich von den beschriebenen Erkenntnissen des Grundlagenkapitels 3.1 ab. Die Inhalte wurden zunächst in Excel Arbeitsmappen gesammelt. Das Spielbrett und die Spielkarten wurden zunächst mit der freien Software Gimp⁶ erstellt. Nachträglich wurden die Spielelemente mit dem kostenpflichtigen Programm Adobe Illustrator⁷ ein weiteres Mal erstellt, um eine höhere Qualität zu erzielen. Das Bearbeiten einer Spielkarte wird in Abbildung 4.3 illustriert. In der Abbildung lässt sich im rechten Bildbereich die Komplexität der verschiedenen Ebenen einer einzelnen Karte einsehen.



Abbildung 4.3: Bildbearbeitung einer Spielkarte

Die Grafiken, die im oberen Bereich der Spielkarten zu finden sind, werden extra zum Zwecke des Spiels händisch gezeichnet. Abbildung 4.4 zeigt beispielhaft eine Zeichnung. Neben den größtenteils eigens angefertigten Grafiken gibt es Ausnahmen bezüglich der verwendeten Bilder. Die Quellen befinden sich dann auf der beiliegenden CD. Die Grafiken durchlaufen anschließend einen Filter, der mit der Software

⁶<https://www.gimp.org/> abgerufen am 08.03.2020

⁷<https://www.adobe.com/de/products/illustrator.html> abgerufen am 08.03.2020

Deep Art Effects⁸ realisiert wird. Die verschiedenen verwendeten Symbole stammen von Font Awesome⁹ und sind frei verfügbar.

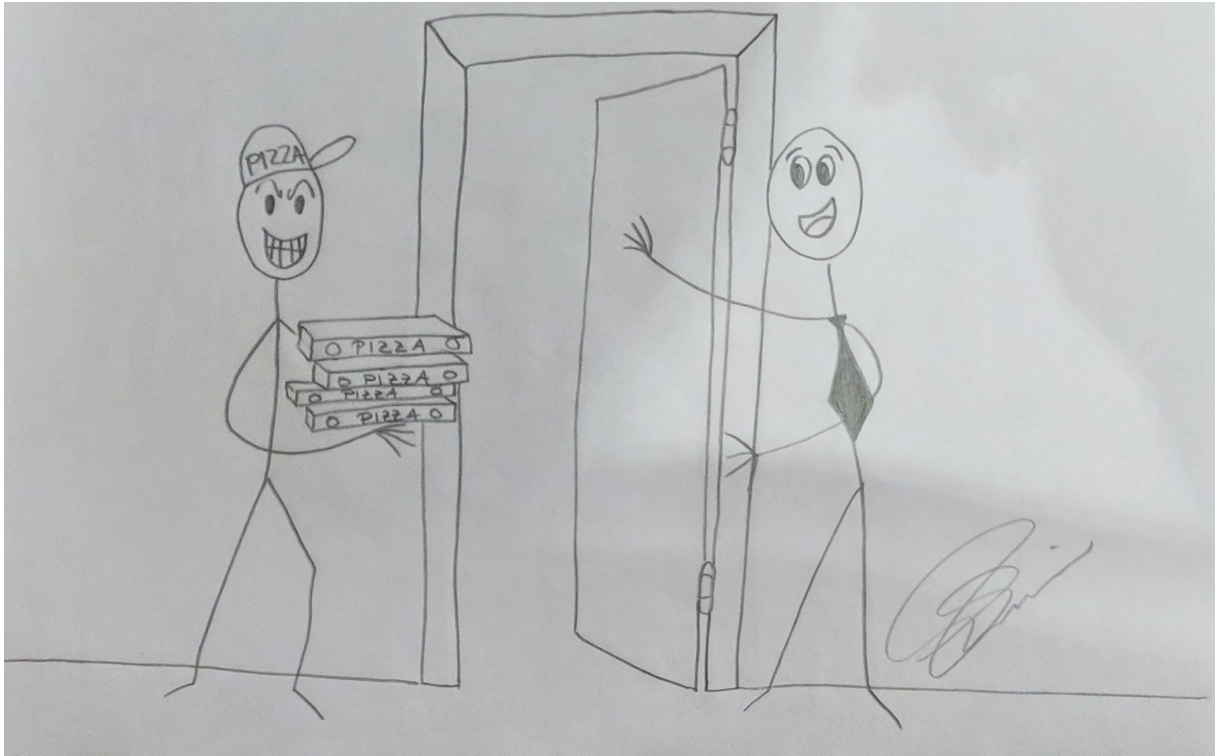


Abbildung 4.4: Zeichnung eines Spielkartenbildes

4.4 Finale Spielelemente

4.4.1 Spielbrett

Die Grundlage des Spiels ist das in Abbildung 4.5 gezeigte Spielbrett. Auf diesem sind die Locations abgebildet, auf welchen sich die Spieler mittels Spielfiguren im Uhrzeigersinn fortbewegen können. Das Spielbrett besteht aus insgesamt 30 Spielfeldern, welche sich wie folgt aufteilen:

2x Payday:

Die Payday-Felder befinden sich an der unteren linken bzw. der oberen rechten Ecke. Die Felder sind sowohl die Startfelder des Spiels als auch die Reputations-Felder. Jeder Spieler kann sich zu Spielbeginn aussuchen, auf welchem dieser Felder er be-

⁸<https://www.deeparteffects.com/> abgerufen am 08.03.2020

⁹<https://fontawesome.com> abgerufen am 08.03.2020

ginnen möchte. Wenn ein Spieler eine der beiden Locations überquert, so erhält er Reputation in Höhe der aufsummierten Reputations-Werte seiner Kunden.

1x Red Team:

Das Red Team-Feld¹⁰ befindet sich auf der oberen linken Ecke des Spielbretts. Ein Spieler, der diese Location überquert, darf sich eine Hacking-Karte (siehe Kapitel 4.4.2) vom Stapel ziehen. Wenn der Spieler direkt auf dem Feld landet, darf dieser zwei Hacking-Karten ziehen.

1x Blue Team:

Das Blue Team-Feld¹¹ befindet sich auf der unteren rechten Ecke des Spielbretts. Ein Spieler, der diese Location überquert, darf sich eine Countermeasure-Karte (siehe Kapitel 4.4.2) vom Stapel ziehen. Wenn der Spieler direkt auf dem Feld landet, darf dieser zwei Countermeasure-Karten ziehen.

26x Location:

Alle weiteren Spielfelder sind als Locations gekennzeichnet (Symbol auf der oberen rechten Ecke des Feldes). Es gibt 24 normale Locations mit einem Countermeasure- und Reputations-Wert und zwei Instituten, welche einen Countermeasure-Wert und ein Countermeasure oder Hacking Symbol besitzen. Zu jedem Location-Feld gibt es eine Location-Karte, welche im Kapitel 4.4.2 genauer beschrieben sind. Es wurde darauf geachtet, dass die Werte einer jeden Location und der diagonal gegenüberliegenden Location gleich sind.

3x Kartenstapel-Felder:

In der Mitte des Spielbretts sind drei Felder für die Kartenstapel gekennzeichnet, auf welchen die Countermeasure-, Awareness- und Hacking-Karten abgelegt werden.

¹⁰Ein Red Team ist eine Gruppe, welche aus der Perspektive eines Angreifers agiert, um Schwachstellen unter realen Bedingungen aufzudecken.

¹¹Ein Blue Team besteht aus internen Mitarbeitern eines Unternehmens und ist durchgängig für die Sicherheit zuständig. Es versucht vorausschauend Angriffe zu erkennen und abzuwehren.



Abbildung 4.5: SANIAG Brettspiel

4.4.2 Spielkarten

SANIAG beinhaltet Karten, welche Dynamik in das Spiel bringen und den didaktischen Teil beinhalten. Es gibt insgesamt vier Kategorien, die sich in ihrer Farbe und wie sie im Spiel verwendet werden können, unterscheiden. Die Countermeasure und Social Hacking-Karten besitzen außerdem mindestens eine von sieben Social Engineering Typen, die in den Kapiteln 4.4.2 und 4.4.2 beschrieben werden. Die Countermeasure, Hacking und Location-Karten besitzen im unteren Teil der Karte einen kurzen Text, welcher entweder die Karte beschreibt oder eine lehrende Information zu Social Engineering beinhaltet. Außerdem ist auf der oberen Hälfte ein Bild, welches den Namen der Karte veranschaulicht.

Location-Karten

Jede auf dem Spielbrett abgebildete Location hat eine zugehörige Location-Karte. Die Karten sind zu Beginn des Spiels neutral, also in keinem Besitz eines Spielers. Sie werden nach einem erfolgreichen Hack in den Besitz eines Spielers übergeben. Die Location ist dann in einem Kundenverhältnis mit dem Spieler bzw. Berater. Eine Location besitzt zwei Kartenwerte. In der Abbildung 4.6 stellt der linke Wert den für Countermeasure dar. Der rechte Wert bestimmt die Reputation. Der Countermeasure-Wert gibt die Anzahl der Countermeasure-Karten vor, durch welche die Location von Beginn an geschützt ist. Der Berater einer Location kann weitere Countermeasures hinzufügen und diese damit sicherer vor Hacks machen. Die Anzahl der Countermeasures, die eine Location besitzen darf, ist unbegrenzt. Der Reputation-Wert gibt die Anzahl der Reputationspunkte an der Location an. So erhält der Spieler beim Überqueren der Payday-Felder Reputationsmünzen in Höhe des Reputation-Wertes seiner Locations. Bei einem fehlgeschlagenen Hack auf seine Location erhält der Spieler ebenso Reputationsmünzen in dieser Höhe vom gegnerischen Spieler.

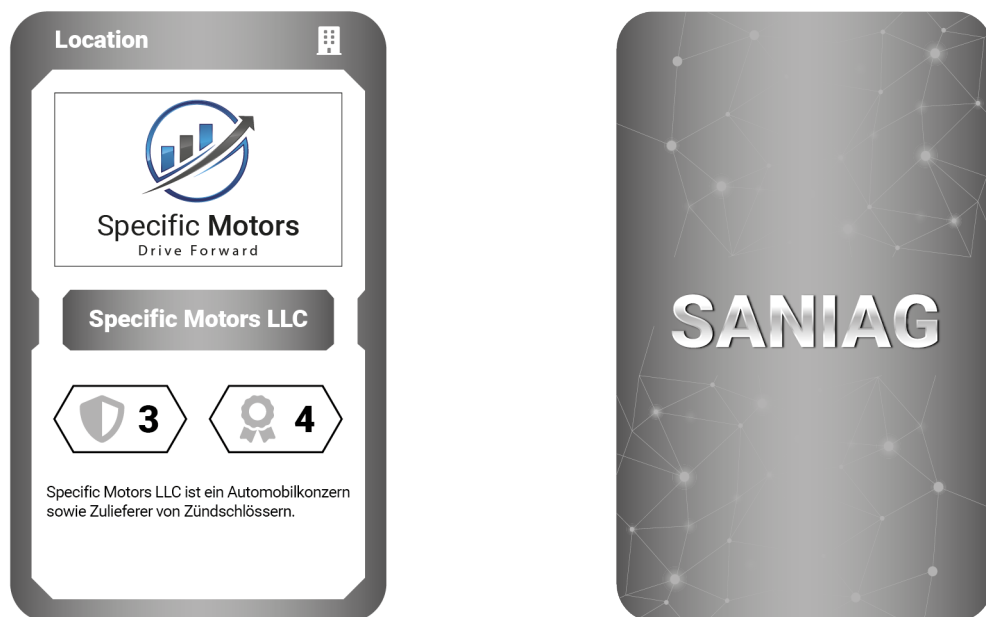


Abbildung 4.6: SANIAG Location-Karte

Es gibt zwei besondere Locations, welche als Institut bezeichnet werden. Diese besitzen keinen Reputation-Wert. Stattdessen belohnen sie den Berater des Instituts in jeder Spielrunde mit einer Countermeasure- oder Hacking-Karte.

Countermeasure-Karten

Countermeasure-Karten sind blau und schützen vor genau einer der sieben Social Engineering Kategorien im Spiel. Die Countermeasures werden auf Locations platziert und sollen diese vor erfolgreichen Hacks schützen. Ein Berater muss während eines Hacks jede Countermeasure einer Location überwinden. Die jeweiligen Typen fordern entweder das Würfelglück eines Spielers heraus oder fragen das Wissen mittels Awareness-Karten (siehe Kapitel 4.4.2) ab. Der Wert der Countermeasure-Karte bestimmt, wie hoch der hackende Spieler würfeln muss, bzw. wie viele Awareness-Karten korrekt beantwortet werden müssen, damit der Hack erfolgreich ist und die Location in ein Kundenverhältnis mit dem neuen Berater übergeht. Eine der Countermeasure-Karten wird beispielhaft in Abbildung 4.7 dargestellt.



Abbildung 4.7: SANIAG Countermeasure-Karte

Awareness-Karten

Awareness-Karten haben eine grüne Farbgebung und stellen den Hauptlernerfolg des Spiels dar. Die Awareness-Karten beinhalten eine Fragestellung mit vier Antwortmöglichkeiten im oberen Teil und den korrekten Antwortbuchstaben samt Antworttext im unteren Teil. Eine Spielkarte für Awareness wird mittels Abbildung 4.8 veranschaulicht. Die korrekte Antwort ist kurz und gehaltvoll erklärt, um so den Spielern Wissen zu vermitteln. Die Anzahl der verschiedenen Awareness-Karten ist absichtlich auf 60 Stück limitiert, sodass deren Inhalte wiederholt im Laufe einer Partie vorkommen und dadurch eingeprägt werden. Während eines Hacks im Spiel gibt eine Countermeasure-Karte der Kategorie "General" vor, wie viele Awareness-Karten der Spieler korrekt beantworten muss. Diese werden vom nachfolgenden Spieler gezogen und vorgelesen. Die Awareness-Karten behandeln Themengebiete im Social-Engineering Bereich, die typischerweise in Awareness-Schulungen adressiert werden. Sie decken damit die Inhalte des Grundlagenkapitels 3.1 weitestgehend ab.



Abbildung 4.8: SANIAG Awareness-Karte

Hacking-Karten

Hacking-Karten sind rot und in den drei Unterkategorien "Social Hacking", "Hacking Gadget" und "Instant Hacking" vertreten. Sie können die Chance für einen erfolgreichen Hack steigern oder Spielern Vor- oder Nachteile im Spielverlauf verschaffen.

Social Hacking-Karten

Social Hacking-Karten sind das Gegenstück zu den Countermeasure-Karten. Jede Social Hacking-Karte besitzt bis zu drei der sieben Social Engineering Kategorien. Jeder Typ besitzt einen Wert zwischen eins und vier, wie beispielhaft eine Spielkarte in der Abbildung 4.9 zeigt. Vor einem Hack kann der Berater am Zug entscheiden, ob und welche Social Hacking-Karten er während des Hacks nutzt. Die Werte derselben Typen werden summiert und von jeder Countermeasure-Karte des selben Typs abgezogen. Dadurch muss der hackende Spieler eine geringere Augenzahl würfeln oder weniger Awareness-Karten überwinden. Diese Spielmechanik veranschaulicht die Effektivität von verschiedenen Sicherheitsmaßnahmen. Den Spielern soll außerdem vermittelt werden, welche Angriffe es im Social Engineering Bereich gibt und der Sinn und Zweck hinter Sicherheitsmaßnahmen verdeutlichen.



Abbildung 4.9: SANIAG Social Hacking-Karte

Hacking Gadget-Karten

Hacking-Gadgets haben einen Effekt und können von den Spielern während ihrer Aktionen ausgespielt werden. Sie besitzen eine strategische Komponente und bringen dem Spieler Vorteile oder den gegnerischen Spielern Nachteile.



Abbildung 4.10: SANIAG Hacking Gadget-Karte

Instant Hacking-Karten

Instant Hacking-Karten können jederzeit ausgespielt werden und sollen die Dynamik und den Spielspaß von SANIAG erhöhen. Ebenso wie die Hacking Gadget-Karten bringen sie den Spielern verschiedene Vor- und Nachteile.



Abbildung 4.11: SANIAG Instant Hacking-Karte

4.4.3 Weitere Spielbausteine

Spielfiguren

Jeder Spieler wählt sich zu Beginn des Spiels eine von acht Spielfiguren aus, welche dazu verwendet wird, sich auf dem Spielfeld fortzubewegen. Die Spielfiguren sind 3D-Varianten der Social Engineering Kategorien sowie der Countermeasure- und Hacking-Karten.

Würfel

Im Spiel enthalten sind außerdem zwei Würfel. Diese werden sowohl für die Fortbewegung auf dem Spielbrett genutzt als auch beim Hacken von Locations zur Überwindung der sechs spezifischen Countermeasure-Kategorien.



Abbildung 4.12: SANIAG Spielfiguren, Würfel und Reputationsmünzen

Reputationsmünzen

Die Reputationsmünzen stellen die Währung bzw. das Punktesystem des Spiels dar. Sie werden von den Spielern benötigt, um das Spiel zu gewinnen. Die Reputation soll den Spielern vermitteln, dass erfolgreiche Projekte und zufriedene Kunden für ein höheres Ansehen sorgen können. Der Verlust von Kunden kann ebenso mit dem Verlust von Reputation einhergehen. Solange eine Location im Spiel Kunde eines Beraters ist, erhält dieser Reputation. Bei Verlust der Location verliert dieser Berater jedoch langfristig Reputation und das Ansehen sinkt.

Spielanleitung

Um einen einfachen Einstieg in das Spiel SANIAG zu ermöglichen, ist dem Spiel eine vierseitige Anleitung beigelegt. In dieser sind die Spielmaterialien aufgezählt und die Spielregeln beschrieben. Am Ende der Spielanleitung befinden sich zwei Beispielrunden eines Spielers, welche einen Großteil der vorher beschriebenen Regeln exemplarisch veranschaulichen. Das Design der Anleitung richtet sich nach den anderen Elementen des Spiels.

Kapitel 5

Forschungsdesign

Bei dem gewählten Untersuchungsdesign handelt es sich um eine randomisierte kontrollierte Studie. Genauer gesagt wird die Methode des experimentellen Ansatzes verfolgt. Mittels der Studie soll untersucht werden, ob bzw. in welchem Maße Probanden durch ein Social Engineering Lernspiel sensibilisiert werden. Dabei gilt das Spielen bzw. Nicht-Spielen des Lernspiels als unabhängige Variable (Intervention bzw. kein Intervention). Der in den Fragebogen erzielte Punktwert (siehe Kapitel 6.9) ist hierbei als abhängige Variable zu verstehen. Diese mögliche Sensibilisierung gegenüber Social Engineering wird im Rahmen dieser Arbeit auch einfach als Awareness bezeichnet. Die genauen Kriterien zur Messung der Awareness wird in Kapitel 5.5 erläutert. Der zu erwartende Effekt ist in Kapitel 1.3 beschrieben.

5.1 Generelles Studiendesign

Die Umsetzung der experimentellen Studie untergliedert sich zeitlich in mehrere Phasen. Der Ablauf lässt sich grob so darstellen, dass es eine vorbereitende Phase vor der Studie gibt, die Durchführung der eigentlichen Studie, sowie eine abschließende Phase zur Auswertung der Daten. Die einzelnen Studienabschnitte und deren zeitliche Abfolge wird in Abbildung 5.1 veranschaulicht.

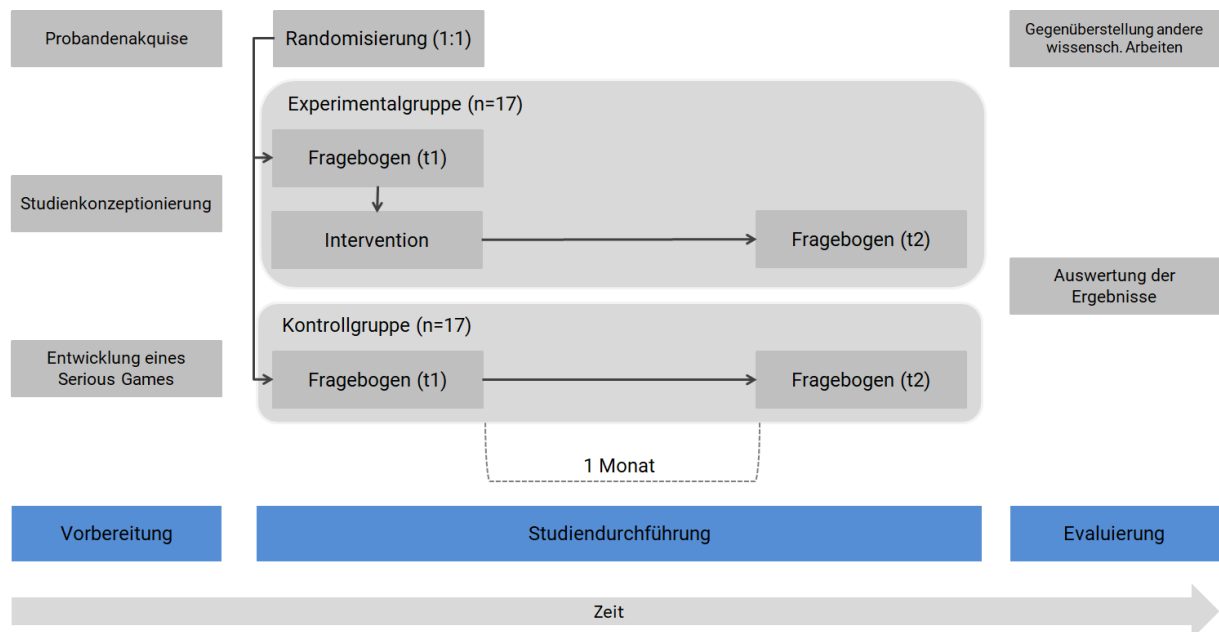


Abbildung 5.1: Studienphasen

Vorbereitung

Innerhalb der ersten Phase werden alle vorbereitenden Tätigkeiten für die Durchführung der experimentellen Studie abgeschlossen. Dies umfasst die Auswahl eines Forschungsdesigns sowie das Definieren weiterer Rahmenbedingungen. So muss etwa die gewünschte Anzahl der Testpersonen bestimmt, die Dauer der Studie festgelegt und vorab entschieden werden, wie die Daten erhoben und ausgewertet werden. Diese Entscheidungen werden basierend auf dem aktuellen Stand der empirischen Sozialforschung getroffen und vor allem im Kapitel 5 nachfolgend genauer erläutert.

Ein weiterer essentieller Bestandteil der Vorbereitungsphase ist das Schaffen der Intervention, welche für diese Studie die Konzeption und Herstellung eines Serious Games bedeutet. Das für diese Studie geschaffene Spiel wird ausführlich in Kapitel 4 beschrieben.

Studiendurchführung

Für die Durchführung werden die Teilnehmenden randomisiert in eine Experimental- und eine Kontrollgruppe eingeteilt. Beide Gruppen füllen zum Zeitpunkt t1 und einen Monat später zum Zeitpunkt t2 Fragebogen aus, während die Experimentalgruppe

zwischen t1 und t2 die Intervention in Form des Lernspiels SANIAG erhalten (siehe Abbildung 5.1). Durch den Vergleich beider Gruppen im Zeitverlauf kann der Lerneffekt ermittelt werden.

Evaluierung

In dieser Phase sind alle erforderlichen Daten erhoben und somit die Arbeiten mit den Testpersonen abgeschlossen. Die Daten sollen nun mittels statistischer Verfahren ausgewertet werden, um eine Aussage über das aufgestellte Hypothesenpaar treffen zu können.

5.2 Rechtliche und ethische Rahmenbedingungen

5.2.1 Ethische Aspekte

Im Vorfeld der Studie werden die ethischen Gesichtspunkte der geplanten Studie überdacht. Als Referenz und Orientierung dient die im Ethikantrag der Ethikkommission TU Darmstadt enthaltene Checkliste. Die ausgefüllte Checkliste ist in Tabelle 5.1 dargelegt.

Sind die Versuchspersonen körperlichen Belastungen oder Risiken (z.B. durch Laserstrahlen, Lärm, starke körperliche Belastung, bewegliche Maschinen) ausgesetzt?	Ja ☐	Nein ☒
Kann Ihre Untersuchung bei Versuchspersonen Schmerz oder psychischen Stress durch starke Emotionen (z.B. traumatische Erfahrungen, Ärger, Angst) hervorrufen, die das im Alltag zu erwartende Maß überschreiten?	Ja ☐	Nein ☒
Arbeiten Sie im Rahmen Ihrer Studie mit einer Täuschung oder Manipulation von Versuchspersonen?	Ja ☐	Nein ☒
Werden (auch) erkrankte Personen (Patienten) als Versuchspersonen eingesetzt?	Ja ☐	Nein ☒
Werden in Ihrer Studie (auch) Minderjährige als Versuchspersonen einbezogen?	Ja ☐	Nein ☒

Könnten Einzelne, Minderheiten oder sozial verletzliche Gruppen – z.B. durch die statistische Verknüpfung von Daten – bloßgestellt werden?	Ja ☐	Nein ☒
Kann es indirekt Beteiligte bzw. Betroffene des Vorhabens geben (z.B. Angehörige)?	Ja ☐	Nein ☒
Werden personenbezogene Daten (z.B. Alter, Geschlecht, Ausbildung, Staatsangehörigkeit, Gesundheitsdaten, physische Merkmale) von Versuchspersonen erhoben?	Ja ☒	Nein ☐
Sind im Rahmen Ihres Projekts Gefahrstoffe (Chemikalien, biologische Agenzien, radioaktive Materialien) im Einsatz - ggf. auch innerhalb gesetzlicher Grenzen - oder werden solche wesentlich oder potentiell erzeugt?	Ja ☐	Nein ☒
Planen Sie, Ihre Forschungsergebnisse zu publizieren, ohne dabei die Anonymität der Versuchspersonen garantieren zu können (z.B. durch Anonymisierung von Datensätzen, Verpixelung von Aufnahmen)?	Ja ☐	Nein ☒
Forschen Sie mit kommerziell erstellten Datensätzen? Bestehen Unklarheiten bezüglich der Herkunft von verwendeten Daten? Könnten bei deren Erhebung ethische/rechtliche Grundsätze ggf. nicht beachtet worden sein?	Ja ☐	Nein ☒
Kooperieren Sie im Rahmen der Studie mit einem kommerziellen Projektpartner, der Daten, die Sie gewinnen (mit) nutzt?	Ja ☐	Nein ☒
Handelt es sich Ihrer Einschätzung nach bei der Studie um ein aus ethischer Sicht unkritisches Forschungsvorhaben?	Ja ☒	Nein ☐

Tabelle 5.1: Checkliste des Ethikantrags [Tec]

Basierend auf den Fragestellungen der Checkliste wird die geplante Studie als ethisch unbedenklich eingeschätzt.

Der Aspekt des Datenschutzes wird in der darauf folgenden Sektion abgehandelt. Die Testpersonen werden nach Abschluss der Studie über den genauen Zweck aufgeklärt und der Kontrollgruppe soll angeboten werden, ebenfalls an der Intervention teilzunehmen.

5.2.2 Datenschutz

Da im Rahmen des Forschungsvorhabens personenbezogene Daten natürlicher Personen erhoben bzw. verwendet werden, sind die Vorgaben des Datenschutzes zu beachten. In diesem Fall sind die gesetzlichen Regelungen durch die Datenschutz Grundverordnung¹ vorgegeben. Da keine personenbezogenen Daten besonderer Kategorien erhoben werden, bleibt diese Arbeit unberührt von sogenannten Erlaubnistatbeständen, welche häufig im Kontext von Forschungsvorhaben herangezogen werden. Es handelt sich dabei um eine Ausnahmeregelung für Forschungszwecke, die eine Verarbeitung besonderer Kategorien personenbezogener Daten nach Artikel 9 zulässt.

Unter anderem ist eine Einwilligung der Probanden zur Erhebung, Verarbeitung und zum Nutzen der mittels Fragebogen gewonnenen Daten erforderlich. Dies kann auch elektronisch erfolgen. Zudem werden in Kapitel 3 (Artikel 12-23) die Rechte der betroffenen Personen beschrieben.

Infolgedessen beinhaltet der Fragebogen einen Hinweistext über den Datenschutz im einleitenden Abschnitt. Der Proband wird außerdem aufgefordert eine freiwillige Einverständniserklärung durch Anklicken eines Kästchens zu bekunden. Sofern dies nicht erfolgt, kann der Fragebogen nicht abgesendet werden. Zusätzlich werden die Daten der Probanden pseudonymisiert, um eine spätere Zuordnung der Prä- und Postfragebogen zu gewährleisten, ohne auf den Probanden schließen zu können (siehe Kapitel 5.5.4).

¹Die amtliche Fassung der Verordnung (EU) 2016/679 mit dem Kurztitel Datenschutz-Grundverordnung ist online abrufbar unter <https://eur-lex.europa.eu/eli/reg/2016/679/oj> abgerufen am 11.03.2020

5.3 Stichprobenumfang

Ein Schätzwert für den Stichprobenumfang (Anzahl der Probanden) wird mit der Software G*Power ² berechnet [Fau+07]. Die Bedienung des Programms orientiert sich an den Beispielen nach Rasch [Ras+14, Kapitel 7.1].

Zur Berechnung sind drei Parameter notwendig. Diese umfassen den Fehler 1. Art, den Fehler 2. Art sowie die erwartete Effektgröße. Anschließend kann für eine experimentelle Studie mit 2 Messpunkten (Prä- und Post-Intervention) und 2 Gruppen (Experimental- und Kontrollgruppe), welche mittels Varianzanalyse (ANOVA) ausgewertet wird, ein Stichprobenumfang berechnet werden. Der hier berechnete Wert ist als ein Minimum zu verstehen.

Wie die G*Power Berechnung in Abbildung 5.2 aufzeigt, ist ein signifikantes Ergebnis ab einem Stichprobenumfang von mindestens 34 Testpersonen möglich. Dies schließt beide Gruppen (Experimental- und Kontrollgruppe) mit ein. Die Bedeutung der einzelnen statistischen Werte und eine Begründung, weshalb die entsprechenden Werte ausgewählt wurden, wird nachfolgend erläutert.

Signifikanzniveau (significance level bzw. α err prob): 0,05

Das Signifikanzniveau (auch Irrtumswahrscheinlichkeit) gibt an, wie wahrscheinlich es ist, dass die Nullhypothese irrtümlich zurückgewiesen wird, obwohl sie in Wirklichkeit wahr ist. Man spricht hierbei auch vom Fehler 1. Art. Das Signifikanzniveau muss stets vor der Hypothesenprüfung (a priori) festgelegt werden und wird in der Regel auf 5% fixiert.[Dör+15, Seiten 664-666] Demnach ist ein falsch-positives Stichprobenergebnis mit maximal 5% sehr unwahrscheinlich. Somit ist das irrtümliche Aufdecken eines positiven Lerneffekts durch die Studie sehr unwahrscheinlich. Jedoch ist dies nie gänzlich auszuschließen. Beispielsweise könnte der Stichprobenumfang zu klein oder nicht zufällig genug gewählt sein.

²Das Programm G*Power wird von der Heinrich-Heine-Universität Düsseldorf zur Verfügung gestellt und ermöglicht die Durchführung von unterschiedlichen statistischen Tests.

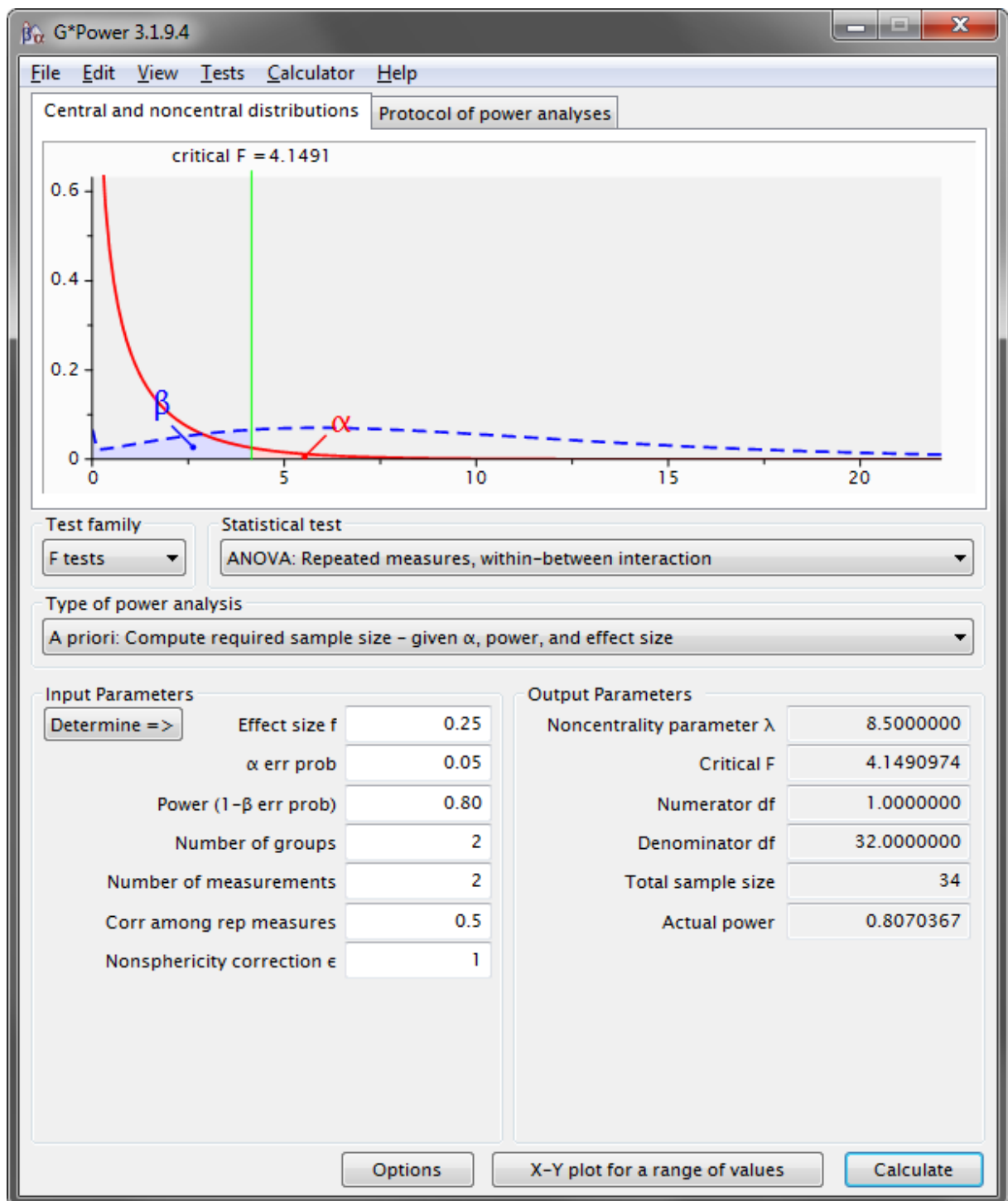


Abbildung 5.2: Bestimmung des Stichprobenumfangs

Teststärke (power bzw. $1-\beta$ err prob): 0,80

Die Teststärke gibt die Wahrscheinlichkeit an, mit welcher ein wahrer Effekt tatsächlich aufgedeckt wird und somit die Alternativhypothese richtigerweise als korrekt angenommen wird. Konventionell wird eine Teststärke von 80% oder mehr gefordert

[Dör+15, Seite 809]. Demzufolge besteht eine Wahrscheinlichkeit von maximal 20%, dass ein tatsächlich vorhandener positiver Lerneffekt durch die Studie nicht entdeckt wird.

In dem Zusammenhang wird häufig vom Fehler 2. Art gesprochen. Hierbei handelt es sich um die Wahrscheinlichkeit β , mit der die Nullhypothese fälschlicherweise bestätigt wird, obwohl die Alternativhypothese korrekt ist.

Erwartete Effektstärke (effect size f): 0,25

Die Effektstärke ist ein Maß, um die Größe eines statistischen Effekts zu beschreiben [Dör+15, Seite 814]. Im Rahmen der Studie bestimmt der Wert, ob bzw. in welchem Maße ein Lerneffekt vorliegt. Der Wertebereich ist hierbei grundsätzlich von $-\infty$ bis ∞ definiert, jedoch handelt es sich bei Effektstärken meist um kleine Zahlen. An dieser Stelle ist es wichtig zu verstehen, dass verschiedene Effektstärkemaße existieren.[Coh13] Diese hängen von dem verwendeten statistischen Verfahren bzw. der verwendeten Formel ab. Sie lassen sich nicht direkt vergleichen, können aber durch eine Umrechnung vergleichbar gemacht werden. Da es in der wissenschaftlichen Literatur keine Referenzwerte für Lernspiele in Kontext Social Engineering gibt, ist ein mittlerer Wert für eine effect size f von 0,25 anzunehmen.[Dör+15, Tabelle 14.5]

Korrelation zwischen Messwiederholungen

Die mittlere Korrelation zwischen den wiederholten Messzeitpunkten wird bei einem Wert von 0,5 belassen, da keine vorausgehenden Daten abschätzbar sind. Der Wert sagt aus, wie zeitlich stabil die Ergebnisse von Messungen sind. Eine hohe Veränderbarkeit zwischen den Messpunkten, etwa wenn die Ergebnisse zusätzlich von einer zufälligen Variable abhängen, würde einen niedrigen Wert erfordern. Hingegen würde eine zu erwartende konstante Messung einen hohen Wert erfordern. Beispielsweise verändern sich die Körpermaße von einer Testperson bei einem Testzeitraum von einem Monat kaum, relativ gesehen zu anderen Testpersonen.[Ras+14, Kapitel 7.1, Seite 2].

Korrekturparameter ε der Sphärizitätsannahme

Die Varianz der Differenz zwischen allen Messpunkten innerhalb einer Gruppe sollte paarweise ähnlich sein. Beispielsweise sollten bei drei Messpunkten die Werte der Differenzen t_1-t_2 , t_1-t_3 , sowie t_2-t_3 in etwa gleich sein. Wenn solch eine Sphärizitätsannahme nicht erwartet werden kann, sollte der Wert verringert werden. Der kleinstmögliche Wert ist $1 / (\text{Anzahl an Wiederholungen} - 1)$. Folglich kann der Wert bei zwei Messwiederholungen nur 1,0 annehmen.[Dör+15, Seite 884]

5.4 Dauer der Studie

Für die Dauer des eigentlichen Experiments wird bewusst ein Zeitraum von einem Monat gewählt. Somit entsteht ein zeitlicher Abstand von 30 Tagen zwischen den beiden Messpunkten. Die Testpersonen bearbeiten also 30 Tage nach der Intervention den zweiten Fragebogen. Dieser Zeitraum befindet sich in einer für die Praxis relevanten Größenordnung und ist zugleich im zeitlichen Rahmen der Masterarbeit realisierbar. Eine kürzere Dauer für das Experiment wäre ebenso denkbar. Der zu erwartende Lerneffekt ist bei einer zweiten Messung mit nur wenigen Tagen Abstand womöglich signifikant höher, da das Spielen des Spiels viel präsenter ist. Jedoch wäre dann die Bedeutung des Effekts sehr gering, da die Probanden das erlernte Wissen potentiell binnen weniger Tage vergessen könnten und somit die Intervention als nicht praxistauglich bezeichnet werden kann. Dies soll ausgeschlossen werden, weshalb die experimentelle Studie über den Zeitraum weniger Tage hinaus geht.

5.5 Datenerhebungsmethode

Im Folgenden werden Überlegungen zur Datenerhebung sowie die Entscheidung für den Einsatz von vollstandardisierten Online-Fragebogen erläutert. Der vollständige Fragebogen, welcher in identischer Form vor und nach der Intervention an die Probanden ausgehändigt wird, kann dem Anhang A entnommen werden.

5.5.1 Auswahl der Datenerhebungsmethode

Die Ermittlung der Effektgröße basiert auf empirisch erhobenen Datensätzen. Die zu erhebenden Daten können durch unterschiedliche Methoden gewonnen werden, etwa durch Interviews, Beobachtung oder Fragebogen. Dabei orientiert sich die Auswahl der idealen Methode nach Döring et al.[Dör+15, Kapitel 10.3]. Auf Methoden, die nicht in Erwägung gezogen werden, wird an dieser Stelle nicht eingegangen.

Für die geplante Studie ist die Durchführbarkeit ein essentielles Kriterium. Dies bezieht sich sowohl auf zeitliche, als auch auf finanzielle Rahmenbedingungen. D.h. die Arbeitsbelastung der Studienleiter soll möglichst gering ausfallen, da insbesondere die zeitlichen Vorgaben im Rahmen der Masterarbeit strikt sind. Komplexe Auswertungsmethoden, etwa eine Kodierung der Antworten, welche bei Interviews erforderlich ist, erhöhen zudem das Risiko, dass Fehler bei der Datenerhebung entstehen. Ebenso soll den Probanden ein möglichst geringer Aufwand entstehen und die Methode der Datenerhebung akzeptiert sein. Dadurch sollen hohe Rücklaufquoten und ein gewissenhaftes Beantworten der Fragen bei den Teilnehmenden erzielt werden.

Die Datenerhebung soll deshalb mittels vollstandardisiertem Fragebogen erfolgen. Dies bedeutet, dass Anzahl, Abfolge und Wortlaut der geschlossenen Fragen sowie der Antwortmöglichkeiten exakt vorgegeben sind.

Hinsichtlich des Mediums kann der Fragebogen in einer Face-to-Face-Situation, postalisch, per Internet oder mobilem Endgerät zur Verfügung gestellt werden. An dieser Stelle sollen die Fragebogen online zur Verfügung gestellt werden. Somit erfordert das Ausfüllen der Fragebogen nicht die Anwesenheit der Studienleiter oder Probanden. Dies verringert zum einen den zeitlichen Aufwand und erhöht die Akzeptanz bei den Probanden. Zum anderen treten keine möglichen ungewollten Verzerrungen durch die Anwesenheit der Studienleiter auf. Letztendlich sollen die Fragebogen mittels Google Forms³ bereitgestellt werden. Dabei handelt es sich um einen kostenfreien

³<https://www.google.de/intl/de/forms/about/> abgerufen am 01.03.2020

Dienst des Unternehmens Google LLC, welcher einen Export der Ergebnisse im .csv-Dateiformat (Comma-separated values) zulässt.

5.5.2 Antwortmodalitäten der Fragebogen

Die Art der Items bzw. der Antwortformate des Fragebogens wirken sich stark auf den Antwortspielraum der Probanden und die Komplexität der Auswertung aus. In den Fragebogen werden ausschließlich geschlossene Items (Items mit Antwortvorgaben) verwendet. Dabei handelt es sich um Items mit Alternativantworten (z. B. richtig, falsch) sowie Auswahlantworten (Multiple Choice Items). Dabei lassen sich Multiple-Choice-Fragen weiter unterscheiden, ob genau eine Antwortoption zutreffen kann ("single answer question") oder ob mehrere der vorgegebenen Antwortmöglichkeiten zutreffen können ("multiple answer question").[Dör+15, Kapitel 10.4] Diese Differenzierung ist von Bedeutung, da beide Antwortformate unterschiedlich ausgewertet werden müssen. Dies ist notwendig um Effekte hinsichtlich dem Raten von Antworten zu korrigieren und wird näher im Abschnitt 6.9 beschrieben. In der angegebenen Literatur gilt es zu beachten, dass Multiple Choice im Englischen strikt eine gültige Antwort aus mehreren bedeutet, was sich vom deutschen Sprachgebrauch unterscheidet.

Die positiven sowie negativen Konsequenzen durch das Verwenden von Multiple-Choice-Frage beschreiben Roedinger und Marsh[RM05]. Dabei stellen sie insbesondere eine negative Auswirkung fest, nämlich, dass Probanden durch Distraktoren (eine falsche Antwortmöglichkeit) dazu verleitet, werden falsches Wissen zu erlernen. Entscheidet sich ein Proband für eine falsche Option, behält dieser sich seine Antwort im Gedächtnis. Er erhält anschließend jedoch keine Rückmeldung über seine falsche Annahme. Somit sind Multiple-Choice-Fragen tendenziell ungeeignet um einen Lerneffekt durch das Beantworten des Fragebogens zu erzielen. Diese Charakteristik ist für die geplante Studie jedoch sogar förderlich. Auf der anderen Seite führen die Forscher aus, dass Multiple-Choice-Antwortformate aufgrund der einfachen Auswertung weit verbreitet sind. Letztendlich werden die Fragebogen mit Multiple-

Choice-Fragen gestaltet, wodurch die Auswertung einfach zu realisieren ist (siehe Kapitel 6.9), jedoch die Konstruktion des Fragebogens nicht trivial ist (siehe Kapitel 5.5.3).

5.5.3 Distraktoren

Um die Wahl der richtigen Antwort bei Multiple-Choice-Fragen zu erschweren, müssen alternative Antwortmöglichkeiten genau so konstruiert werden, dass sie zwar wie richtige Antworten erscheinen, aber inhaltlich falsch sind. Solche falschen Antwortalternativen werden Distraktoren genannt. [MK11, Seite 45] Dabei sind Distraktoren eindeutig formuliert und klar verständlich. Eine Person, die das Wissen bereits erworben hat, sollte Distraktoren zweifelsfrei als falsch bewerten können ("To those who possess the knowledge asked for in the item, the distractors are clearly wrong choices." [Hal04, Seite 69]).

Insbesondere die Anzahl der Items, Exhaustivität und Disjunktheit sind maßgeblich für die Konstruktion guter Multiple-Choice-Fragen. [MK11]

Anzahl der Antwortmöglichkeiten (Items)

Über die bestmögliche Anzahl an Antwortmöglichkeiten wird in der Literatur kontrovers diskutiert. Häufig wird eine Anzahl von rund drei Multiple-Choice Items angegeben [Hal04, Seite 69][RM05, Seite 455]. Der Fragebogen dieser Forschungsarbeit ist deshalb in der Regel so konstruiert, dass Fragen insgesamt fünf Antwortmöglichkeiten zulassen. Eine vierte Antwortmöglichkeit ist erforderlich um die Anforderung der Vollständigkeit zu erfüllen, wie nachfolgend erklärt (etwa "keine der genannten Antwortmöglichkeiten trifft zu"). Eine fünfte Antwortmöglichkeit (etwa "weiß nicht") ermöglicht es dem Probanden, die Auswahl einer Antwort klar abzulehnen. Dies ist notwendig für die Testfairness, sodass Testpersonen mit mehr Mut zum Raten nicht belohnt werden. Die Ratekorrektur wird in Kapitel 6.9 genauer erläutert. Entscheidungsfragen, bei der eine von zwei dichotomen Antworten richtig ist, werden mit drei Antwortmöglichkeiten konstruiert (richtig, falsch, weiß nicht).

Exhaustivität

Ebenso gilt es zu beachten, dass die Vollständigkeit der Antwortmöglichkeiten gegeben ist. Es soll dadurch vermieden werden, dass eine Testperson keine für ihn passende Alternative unter den Antwortenvorgaben findet. Die Fragen sind daher durch die Antwortmöglichkeit "Keine der anderen Antworten trifft zu" ergänzt.

Disjunktheit

Disjunktheit bedeutet, dass sich alle Antwortmöglichkeiten gegenseitig ausschließen bzw. die Schnittmenge der Aussagen leer ist. In Folge dessen können nicht mehrere Antworten richtig sein, was essentiell für die gewählten Distraktoren ist.

5.5.4 Aufbau der Fragebogen

1. Abschnitt

In dem ersten und damit einleitenden Abschnitt wird die Testperson über den Zweck der Befragung aufgeklärt sowie auf Aspekte des Datenschutzes hingewiesen. Bezüglich der Fragen wird der Proband darauf hingewiesen, dass das Beantworten der einzelnen Fragen optional ist, d.h. es kann stets die Antwortmöglichkeit "Weiß nicht" ausgewählt werden sofern die Angabe einer Antwort erforderlich ist. Auch erfährt die Testperson welchen Umfang der Fragebogen hat, dass ihre Antworten pseudonymisiert ausgewertet werden und welche Kontaktmöglichkeiten zu den Studienleitern bestehen.

2. Abschnitt: Persönliches

Im zweiten Abschnitt wird ein Pseudonym (Versuchspersonencode) generiert, indem persönliche Merkmale der Testperson erfasst werden, die nicht direkt auf sie schließen lassen. Dies dient dem Zwecke der Pseudonymisierung von Testpersonen. Eine Frage erfasst etwa die ersten zwei Buchstaben des Straßennamens, in welcher der Proband wohnt. So lassen sich stets zwei Fragebogen (pre- sowie post-Intervention) einem Probanden zuordnen, ohne dessen Identität zu kennen. Zusätzlich werden mittels einer

Likert-Skala das Vorwissen und Einstellungen zu dem Themenfeld Social Engineering der Testperson abgefragt.

3. Abschnitt: Wissen

Im dritten Abschnitt des Fragebogens wird anhand von 11 Fragestellungen Wissen über den Bereich Social Engineering abgefragt. Die Fragen sind so konstruiert, dass möglichst viele Teilbereiche des Themenfeldes thematisiert werden und dass das bloße Abfragen von Begriffen möglichst vermieden wird. Eine der Fragen ist nachfolgend in Abbildung 5.3 exemplarisch dargestellt.

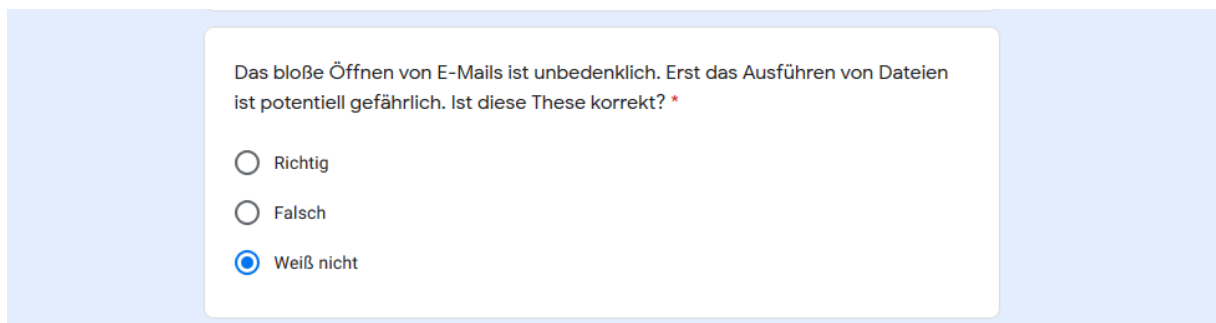
The image shows a screenshot of a survey question. The text of the question is: "Das bloße Öffnen von E-Mails ist unbedenklich. Erst das Ausführen von Dateien ist potentiell gefährlich. Ist diese These korrekt? *". Below the text are three radio button options: "Richtig", "Falsch", and "Weiß nicht". The "Weiß nicht" option is selected, indicated by a blue dot inside the radio button circle. The entire question is enclosed in a white box with a thin border, set against a light blue background.

Abbildung 5.3: Beispielhafte Fragestellung zu einer These

Die Fragen sind teilweise als These formuliert, d.h. es handelt es sich um eine Entscheidungsfrage (die These ist entweder wahr oder falsch). Andere Multiple-Choice-Fragen lassen die Auswahl mehrerer Antworten zu ("multiple answer question"). Binärfragen sind dabei durch einen Radiobutton (Kreis) gekennzeichnet. Multiple-Choice-Fragen sind durch Checkboxes (Auswahlkästchen) gekennzeichnet. Dies wird dem Probanden zu Beginn des Abschnitts genau erläutert.

4. Abschnitt: Szenarien

Der vierte und somit letzte Abschnitt des Fragebogens umfasst weitere 10 Fragestellungen. Dabei soll der Proband die richtige Verhaltensweise für bestimmte Szenarien identifizieren, sodass dieser bzw. dessen Unternehmen nicht Opfer eines Social Engineering Angriffs wird. Eine Beispielfrage zeigt die Abbildung 5.4.

Schlussendlich soll der Proband auf diese Weise mit, in der Praxis relevanten, Situationen konfrontiert werden und bestimmen, wie er sich in den jeweiligen Szenarien

Vor der Eingangstüre zu den Büroräumen stellt sich Herr Müller als neuer Kollege vor. Da dieser einen großen Kuchen trägt, bittet er beim Öffnen der Türe zu helfen. *

- ☐ Ich öffne Herrn Müller mit meiner Zugangskarte die Türe wenn er einen Mitarbeiterausweis bei sich trägt.
- ☐ Ich öffne Herrn Müller die Türe, da auf der letzten Mitarbeiterversammlung verkündet wurde, dass diesen Monat Herr Müller neu anfängt.
- ☐ Ich nehme Herrn Müller den Kuchen ab, sodass er seinen Mitarbeiterausweis an das Lesegerät der Türe halten kann.
- ☐ Keine der anderen Antworten trifft zu.
- ☐ Weiß nicht.

Abbildung 5.4: Beispielhafte Fragestellung zu einem Szenario

verhalten würde. Jede Frage hat stets genau eine korrekt, Antwort ("single answer question"), wobei im Sinne der Exhaustivität auch stets eine Antwortmöglichkeit "Keine der anderen Antworten trifft zu" angeboten wird.

5.5.5 Quantitative Gütekriterien der Fragebogen

Für Messmethoden gelten allgemein die drei Hauptgütekriterien Objektivität, Reliabilität und Validität.[HSE13, S.23] Zwei der drei Hauptgütekriterien für die Messmethode sind klar gegeben. Die Objektivität wird anhand von geschlossenen Fragen gegeben, die keinen Spielraum für eine abweichende Interpretation der Antworten zulassen. Reliabilität ist durch die automatisierte Auswertung gegeben, welche sporadische Messfehler nicht zulässt oder Messfehler zumindest zuverlässig auf die gleiche Weise stattfinden. Inwieweit das Gütekriterium der Validität erfüllt wird, soll nun diskutiert werden.

Kruger et al. beschäftigen sich damit, wie Schulungseffekte bzw. die Sensibilisierung für Informationssicherheit objektiviert werden kann. Sie ordnen ihre Fragestellungen eines Fragebogens drei Kategorien zu. Diese beinhalten das Wissen einer Testperson ("Knowledge"), wie sie über das Thema denkt ("Attitude") und wie sich die Person in einer bestimmten Situation verhalten würde ("Behaviour").[KK06] Diese drei Kategorien werden auch im Fragebogen dieser Arbeit abgedeckt. Exemplarisch wird in

Tabelle 5.2 für jede Kategorie eine Fragestellung vorgestellt.

Wissen ("Knowledge")
Was besagt die Clean-Desk Richtlinie?
Einstellung ("Attitude")
Das bloße Öffnen von E-Mails ist unbedenklich. Erst das Ausführen von Dateien ist potentiell gefährlich. Ist diese These korrekt?
Verhalten ("Behaviour")
Der technische Support benötigt Ihr Benutzerpasswort um ein Laptop-Problem per Fernwartung zu lösen. Tatsächlich erwarten Sie die Hilfe des technischen Supports.

Tabelle 5.2: Beispielhafte Fragestellungen nach Kruger[KK06]

Inhaltlich sind die Fragestellungen basierend auf den im Grundlagenteil beschriebenen Angriffsvektoren und Gegenmaßnahmen von Social Engineering konzipiert. Das Grundlagenkapitel 3 stützt sich auf eine ausgiebige Literaturrecherche. Zusätzlich orientiert sich der Charakter der Fragen an öffentlich zugänglichen Schulungen für Informationssicherheit, wie etwa derer von UNDSS⁴, Proofpoint⁵ und ESET⁶.

5.5.6 Post-Intervention Fragebogen

Nach einer Zeitdauer von 30 Tagen nach dem ersten Fragebogen soll von beiden Gruppen erneut ein Fragebogen bearbeitet werden. Von der Experimentalgruppe wird dieser entsprechend 30 Tage nach Durchführung der Intervention bearbeitet. Inhaltlich wurde sich dazu entschieden den exakt gleichen Fragebogen zu verteilen. So soll gewährleistet werden, dass die Ergebnisse der Fragebogen (Prä- und Post-Fragebogen) vergleichbar sind.

⁴<https://training.dss.un.org/user/login> abgerufen am 12.03.2020

⁵<https://www.proofpoint.com/us/learn-more/attack-spotlight/content> abgerufen am 12.03.2020

⁶<https://www.eset.com/us/cybertraining/register/eloqua/Fce/thankyou/#thankyou> abgerufen am 12.03.2020

Kapitel 6

Durchführung der Studie

6.1 Pretest

Um das in Kapitel 4 beschriebene Lernspiel sowie den in Kapitel 5.5.4 beschriebenen Fragebogen vor dem Studienbeginn erproben zu können, wurden mehrere Vortests durchgeführt.

6.1.1 Pretest des Spiels SANIAG

Bei dem Pretest des Lernspiels liegt der Fokus insbesondere darauf, dass Spieler das Spielprinzip (das Regelwerk) verstehen, sowie Unklarheiten bezüglich der Awareness-Fragen vermieden werden. Hierzu wurden am 21.11.2019 zwei Vortests durchgeführt. Dabei wurden alle Spielkarten per Hand auf farbigem Papier angefertigt und das Spielbrett exemplarisch aufgemalt, wie der Abbildung 6.1 zu entnehmen ist.

Die erste Partie umfasst fünf Spieler bei einer Spieldauer von 90 Minuten. Eine im Anschluss durchgeführte Partie mit den gleichen Spielern dauerte 60 Minuten. Jedoch wurde nach dem ersten Durchgang eine leichte Anpassung des Regelwerks vorgenommen. Die Vortests haben gezeigt, dass wenige Awareness-Fragen zum Teil unklar formuliert gewesen sind. Diese wurden entsprechend angepasst. Das grundlegende Spielprinzip wurde von allen Pretest-Teilnehmenden schnell und lückenlos verstanden. Mangels Spielanleitung zu dem Zeitpunkt des Pretests, wurde das Spielprinzip

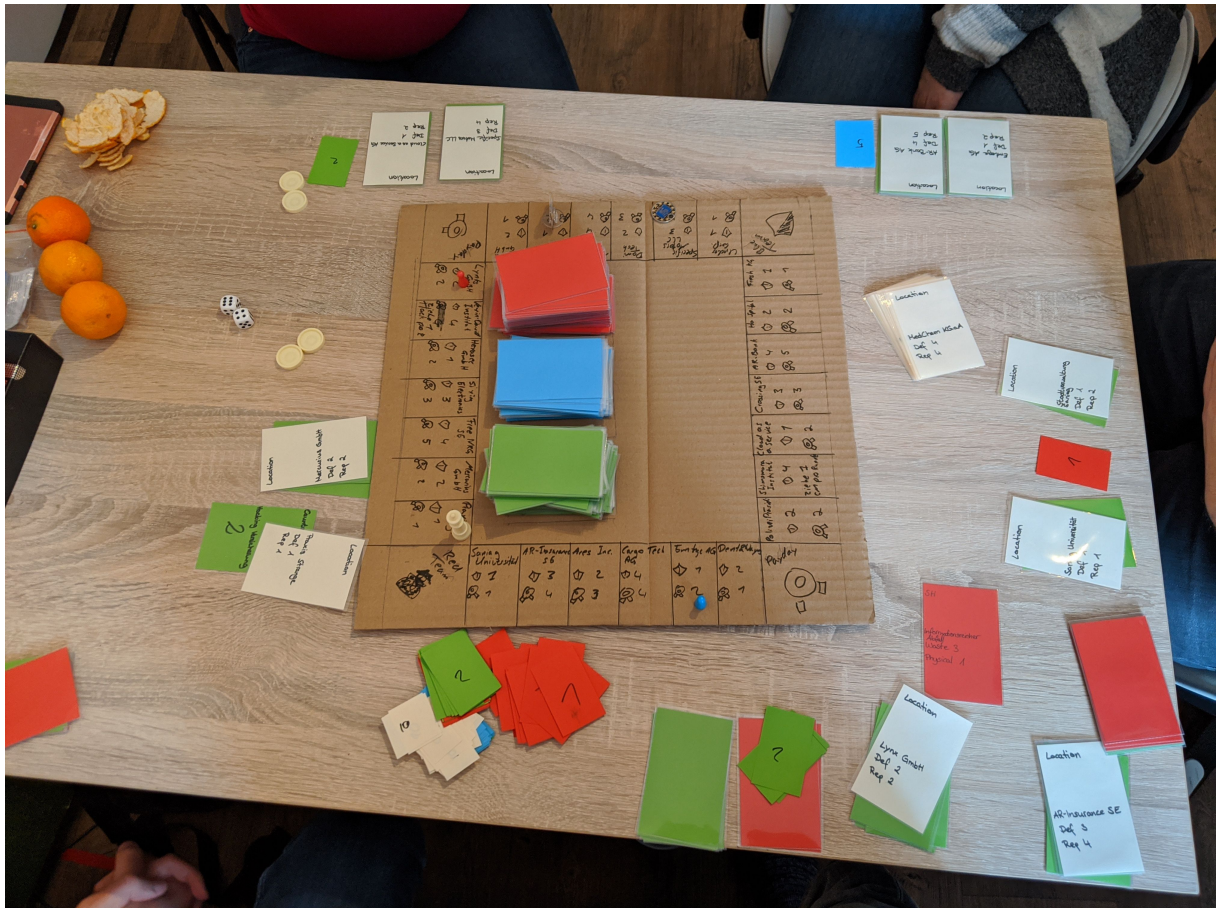


Abbildung 6.1: Pretest des Lernspiels SANIAG

vor Spielbeginn mündlich erklärt. Bereits während des zweiten Durchgangs zeigten sich mutmaßlich erste Lerneffekte. Awareness-Fragen, die in der ersten Partie falsch beantwortet wurden, wurden nun richtig beantwortet. Nach 150 Minuten Spielzeit äußerten zwei Spieler ungern eine dritte Partie durchführen zu wollen.

6.1.2 Pretest des Fragebogens

Vor Beginn der Studie wurde auch die Datenerhebungsmethode evaluiert. Konkret sollten vier Personen den für die Studie angefertigten Fragebogen bearbeiten. Anschließend sollte der Inhalt der Fragestellungen in eigenen Worten wiedergegeben werden. Es konnten keine missverständlich formulierten Fragen identifiziert werden. Einige Fragen konnten aufgrund von Unwissenheit nicht beantwortet werden. Dies ist jedoch erwünscht. Die Personen wurden von der Hauptstudie ausgeschlossen.

6.2 Generelle Studiendurchführung

Sofern nicht anders angegeben, sind stets beide Studienleiter bei der Durchführung der Studie anwesend. Zum Schaffen von Anreizen zur Teilnahme an der Studie wurden die Testpersonen darüber aufgeklärt, dass ein 30€ Amazon-Gutschein unter den Teilnehmenden verlost wird. Die Teilhabe von direkten Freunden an der Studie wurde im Vorfeld ausgeschlossen. Zum einen soll dadurch eine mögliche Verzerrung der Ergebnisse verhindert werden. Zum anderen handelt es sich hierbei zum Teil um Beteiligte der Pretests.

6.3 Randomisierung

Die Testpersonen werden vor bzw. während dem Ausfüllen des ersten Fragebogens zufällig der Experimentalgruppe oder Kontrollgruppe zugewiesen. Dies geschieht mittels eines Skripts, welches durch den Quelltext im Anhang B beschrieben ist. Dabei wird eine Liste von Vornamen zufällig neu angeordnet und alternierend einer der beiden Gruppen zuordnet. Das Ergebnis nach erfolgter Randomisierung wird beispielhaft in Abbildung 6.2 veranschaulicht.

B10		f_x					
	A	B	C	D	E	F	G
1	Name	Gruppe					
2	Proband 3	Experimentalgruppe					
3	Proband 5	Kontrollgruppe					
4	Proband 1	Experimentalgruppe					
5	Proband 4	Kontrollgruppe					
6	Proband 2	Experimentalgruppe					
7							
8							
9							
10							
11							

Abbildung 6.2: Randomisierung der Testpersonen

6.4 Kohorte THM

Messpunkt vor der Intervention

Eine Kohorte wurde an der Technischen Hochschule Mittelhessen in Friedberg (Hessen) rekrutiert. Der erste Termin fand am 17.01.2020 im Anschluss einer Gastvorlesung, gehalten von einem der Studienleiter, statt. Der Link zu dem Online-Fragebogen wurde bereits vorab durch den Dozenten an alle Studierenden des Kurses übermittelt. Seitens der Studienleiter wurde im Wesentlichen auf die Gewinnchance eines Gutscheins hingewiesen. Insgesamt sechs Personen erklärten sich bereit, an der Studie teilzunehmen. Diese füllten den Fragebogen am gleichen Tag aus.

Intervention

Das Spielen des Lernspieles SANIAG fand am 24.01.2020 statt. Eine Spielsituation in den Räumlichkeiten der THM Friedberg zeigt die Abbildung 6.3. Den drei Spielern wurde zu Beginn eine mündliche Einweisung bezüglich der Spielregeln gegeben. Alle Spieler haben das Regelwerk weitestgehend verstanden, nachdem jeder der Spieler einmal am Zug war. Kleinere Fragen über das Regelwerk wurden während des Spiels beantwortet. Auch wurden vereinzelt inhaltliche Fragen über das Thema Social Engineering beantwortet, da die Probanden diesbezüglich ein großes Interesse zeigten. Die angesetzte Spieldauer von ca. einer Stunde wurde mit einer Spielzeit von 15:00-16:40 Uhr überschritten.

Die Probanden äußerten, dass das Spiel viel Spaß mache und man viel lernen könne. Nach Abschluss der Spielrunde wurden die Probanden gebeten, ihre Pseudonyme in einer Liste zu markieren, sodass deren Ergebnisse der Experimentalgruppe zugeordnet werden können.



Abbildung 6.3: Spielen des Lernspiels SANIAG der Kohorte THM

6.5 Kohorte HDA

Messpunkt vor der Intervention

An der Hochschule Darmstadt, University of Applied Sciences, wurden am Fachbereich Informatik insgesamt zehn Probanden mit Intervention und zehn ohne Intervention befragt. Die Zuteilung der Gruppen erfolgte zufällig durch das im Quelltext C.1 beschriebene VBA-Skript. Die Testpersonen der Experimentalgruppe wurde gebeten ihre Pseudonyme in einer Liste zu vermerken. Sowohl das Ausfüllen des ersten Fragebogens sowie das anschließende Spielen des Lernspiels erfolgte am 23.01.2020 vor Ort. Dabei spielten zwei Spielgruppen zu je fünf Teilnehmenden parallel das Spiel.

Intervention Gruppe 1:

Zu Beginn wurde der Fragebogen von allen zehn Teilnehmenden ausgefüllt. Dieser wurde per E-Mail verteilt. Ein Rückschluss von den E-Mail Adressen zu den Pseud-

onymen ist nicht möglich. Nach erfolgter Randomisierung wurde den Testpersonen der Experimentalgruppe mitgeteilt, dass eine Spielzeit von ungefähr einer Stunde angesetzt ist. Dies war zu dem Zeitpunkt eine realistische Spielzeit basierend auf den Erfahrungen der Pretests. Eine Spielsituation zeigt die Abbildung 6.4.



Abbildung 6.4: Spielen des Lernspiels SANIAG der Kohorte HDA

Den Teilnehmenden wurde zu Beginn für 25 Minuten eine mündliche Einführung in das Regelwerk gegeben. Anschließend wurde von den freiwilligen Testpersonen von 12:40-15:40 gespielt. Nach der ersten Runde wurde das Spiel bereits vollständig verstanden. Jedoch erschien den Teilnehmenden das Spiel anfänglich kompliziert. Kleinere Regelfragen wurden während des Spiels beantwortet. An Stelle der im Spiel verwendeten Begrifflichkeit Reputation hat sich der Begriff Geld für die Spielchips eingebürgert. Den Teilnehmenden fiel auf, dass sie bereits viele Fragen der Awareness-Karte aus dem Fragebogen kennen. Einige Awareness-Fragen wurden durch den Studienleiter weiter inhaltlich erläutert. Während des gesamten Spiels wurden etwa 15 verschiedene Awareness-Karten besprochen. Die Partie endete nach ca. drei Stunden

Spielzeit mit einem knappen Sieg.

Intervention Gruppe 2:

Eine weitere Gruppe mit fünf Spielern spielte das Spiel SANIAG. Dabei wurde das Spiel zweieinhalb Stunden mit vorausgehender Einweisung von 15 Minuten gespielt. Einer der Spieler musste das Spiel wegen Terminen vorzeitig beenden. Einer der Studienleiter nahm nun seinen Platz ein. Nach der ersten Spielrunde wurde das Spiel gänzlich verstanden. Kleinere Rückfragen bezüglich des Regelwerks wurden durch den Studienleiter beantwortet bzw. konnten teilweise eigenständig durch Nachlesen der Anleitung durch die Spieler beantwortet werden. Die Spieler diskutierten oftmals über Awareness-Fragen, und persönliche Verhaltensweisen der Spieler wurden reflektiert. Dabei entstand häufig die Einsicht, dass die auf den Awareness-Karten empfohlenen Verhaltensweisen vorteilhaft im Kontext des Social Engineerings sind.

6.6 Kohorte PRIVSA

Messpunkt vor der Intervention

Eine Gruppe von insgesamt 12 Testpersonen wurde am 25.01. rekrutiert. Diese umfassen hauptsächlich Freunde von Freunden eines Studienleiters. Der Fragebogen wurde via E-Mail an die Teilnehmenden versandt und anschließend die Experimentalgruppe für den Abend in private Räumlichkeiten eingeladen.

Intervention

Sechs der Testpersonen spielten darauffolgend das Spiel SANIAG. Ein Spieler übernahm während des Spielverlaufs freiwillig und unaufgefordert die Rolle des Spielers und koordinierte einerseits das Spiel und kontrollierte auch die Aktionen der anderen Spieler. Im weiteren Spielverlauf haben die Spieler angefangen Karten und Aktionen gegen Informationen zu handeln. Beispielsweise hat ein Spieler die Instant Hacking-Karte "Rejection" zugunsten eines anderen Spielers gespielt und im Gegenzug zwei Hacking-Karten erhalten. Auch wurden Informationen zu Countermeasures

der Locations im Tausch gegen Hacking-Karten getauscht. Nach etwa drei Stunden Spielzeit konnte ein Spieler das Spiel sehr knapp für sich entscheiden. Nach dem Spiel wurde noch ca. eine halbe Stunde über das Spiel diskutiert. Gegenstand der Diskussion war insbesondere, was die Spieler an ihrer Strategie hätten ändern können, um zu gewinnen. Die Probanden äußerten, dass man durch das Spiel über ein bestimmtes Themengebiet etwas mit viel Spielspaß lernen kann. Es wurden außerdem Wünsche nach verschiedenen Versionen des Spiels geäußert, um andere Themengebiete tiefer kennenzulernen, wie zum Beispiel Geographie oder Biologie.

6.7 Kohorte PRIVNI

Messpunkt vor der Intervention

Am 01.02.2020 nahmen sechs weitere Teilnehmende an der Studie teil. Diese umfassen hauptsächlich Freunde von Freunden eines Studienleiters. Der Fragebogen wurde via E-Mail an die Teilnehmenden versandt und anschließend die Experimentalgruppe für den Abend in private Räumlichkeiten eingeladen.

Intervention

Die drei Spieler wurden von nur einem der Studienleiter betreut. Wie in den vorherigen Kohorten wurde das Spielprinzip vorab mündlich erklärt. Die Erklärung dauerte diesmal nur wenig Minuten, eine vergleichsweise kurze Dauer, da die Probanden dazu drängten, das Spiel zu spielen. Das Spielgeschehen zeigt die Grafik 6.5. Die Partie des Spiels SANIAG dauerte von 20:00 bis 21:40 Uhr und wurde mit einem knappen Sieg beendet. Während des Spielens hat sich eine Auffälligkeit gezeigt, dass Awareness-Fragen nicht gemieden, sondern vielmehr als Herausforderung angesehen wurden. Einer der Spieler bezeichnete sich als "Quizmaster" und las freiwillig sämtliche Awareness-Karten der anderen Spieler vor.



Abbildung 6.5: Spielen des Lernspiels SANIAG der Kohorte PRIVNI

6.8 Messpunkt nach der Intervention

Der Post-Fragebogen wurde am 22.02.2020 allen Kohorten per E-Mail zugeschickt. In dem Anschreiben wurde vereinbart, dass zusätzlich ein zweiter Gutschein im Wert von 30€ verlost wird, wenn bis zum 26.02.2020 ein genügender Rücklauf der Fragebogen erfolgt ist.

6.9 Quantifizierung und Zuordnung der Datensätze

Das Überführen der Antworten der Testpersonen in einen numerischen Wert umfasst drei Schritte. Zuerst werden die Datensätze aus Google Docs exportiert. Anschließend werden die exportierten Excel-Dateien mittels im Anhang C beschriebenen VBA-Skript bereinigt und in ein auswertbares Format gebracht. Dabei werden die exportierten Excel-Dateien automatisiert und anhand der in Grafik 6.6 abgebilde-

ten Hilfstabelle sortiert in ein zweites Excel-Tabellenblatt überführt. Die Hilfstabelle enthält alle Fragen sortiert nach Antworttyp sowie alle Antwortmöglichkeiten mit jeweiliger Bepunktung. Um ein Pseudonym (Versuchspersonencode) zu bilden werden die ersten drei persönlichen Fragen vereinheitlicht und verkettet. Konkret wird dabei der Tag des Geburtstags herausgefiltert, sofern dieser nicht korrekt eingetragen wurde. Falls der Tag nicht herausgefiltert werden kann, weil beispielsweise Buchstaben in dem Antwortfeld eingetragen sind, so wird der Wert automatisch mit der Zahl "00" ersetzt. Danach werden die Datensätze anonymisiert, indem ein Hashverfahren¹ auf die drei Werte zur Bildung des Pseudonyms angewandt wird.

Kategorie	Frage	Antwort	Punkte	Mehrfachauswahl	Antwort 1	Punkte 1	Mehrfachauswahl
Persönliches	An welchem Tag im Monat sind Sie geboren? (z.B. Geburtsdatum 30.12.1990 = 30)						
Persönliches	Wie lauten die ersten zwei Buchstaben des Straßennamens in der Sie wohnen? (z.B. Mustermannstraße = MU)						
Persönliches	Wie lauten die ersten zwei Buchstaben des Vornamens Ihrer Mutter? (z.B. Lisa = Li)						
Persönliches	Karriere						
Persönliches	Ich stimme dem zu ... [Der Begriff Social Engineering ist mir bekannt.]						
Persönliches	Ich stimme dem zu ... [Ich kenne mich sehr gut mit Social Engineering aus.]						
Persönliches	Ich stimme dem zu ... [Social Engineering stellt ein großes Risiko dar.]						
Persönliches	Ich stimme dem zu ... [Ich erhalte regelmäßig Schulungen zu dem Thema Social Engineering.]						
Einfachauswahl	Intelligenz ist ein wirksamer Schutz gegen Social Engineering Angriffe. Ist diese These korrekt?	Falsch	1				
Einfachauswahl	Social Engineering Angriffe erfordern einen Computer. Ist die These korrekt?	Falsch	1				
Einfachauswahl	Eine Datei lässt sich auch dann wiederherstellen, wenn sie aus dem Papierkorb entfernt wurde. Ist diese These korrekt?	Richtig	1				
Einfachauswahl	Das bloße Öffnen von E-Mails ist unbedenklich. Erst das Ausführen von Dateien ist potentiell gefährlich. Ist diese These korrekt?	Falsch	1				
Mehrfachauswahl	Was wird unter dem Begriff Social Engineering verstanden?	Zwischenmenschliche Beeinflussungen mit dem Ziel, bestimmte Vertrauensverhältnisse zu zerstören.	1	Zwischenmenschliche Beeinflussungen	1	Software	1
Mehrfachauswahl	Was besagt die Clean-Desk Richtlinie?	Keine vertraulichen Daten auf dem Schreibtisch liegen zu lassen.	1	Keine Getränke und Speisen am Arbeitsplatz	-1	Den Arbeitsplatz sauber halten	1
Mehrfachauswahl	Social Engineering Angriffe beruhen auf psychologischer Manipulationen. Welche Prinzipien werden sich dabei zunutze gemacht?	Reziprozität, Autorität, Sympathie	3	Reziprozität	1	Reziprozität	1
Mehrfachauswahl	Welche der genannten Optionen sind Maßnahmen gegen E-Mail Phishing?	E-Mail Filter (Spamfilter), Digitale Signaturen	2	E-Mail Filter (Spamfilter)	1	VPN	1
Mehrfachauswahl	Laut den Digital Identity Guidelines "NIST SP 800-63B-3" des National Institute of Standards and Technology sollen Passwörter aus mindestens 8 Zeichen bestehen. Das Passwort muss aus mindestens 8 Zeichen bestehen. Das Passwort muss aus mindestens 8 Zeichen bestehen.	Das Passwort muss aus mindestens 8 Zeichen bestehen. Das Passwort muss aus mindestens 8 Zeichen bestehen. Das Passwort muss aus mindestens 8 Zeichen bestehen.	2	Das Passwort muss aus mindestens 8 Zeichen bestehen	1	Es ist nicht erforderlich, dass das Passwort aus mindestens 8 Zeichen besteht.	1
Mehrfachauswahl	Welche der genannten Optionen sind Quellen für Open Source Intelligence (OSINT)?	Google Earth, öffentliche Unternehmenswebsite, Tageszeitungen	3	Google Earth	1	öffentliche Unternehmenswebsite	1
Mehrfachauswahl	Laut der Richtlinie NIST SP 800-63B-3 aus dem Jahr 2017 handelt es sich um ein gutes Passwort bei?	sauerstoff4sche	1	passwort	-1	abcd1234	1
Einfachauswahl	Sie erhalten eine Datei "rechnung.pdf.exe" als Anhang einer E-Mail.	Keine der anderen Antworten trifft zu.	1				
Einfachauswahl	Sie erhalten streng geheime Anweisungen über einen Geldtransfer von Ihrem Chef via E-Mail.	Auch bei Anweisungen des Vorgesetzten sind die Prozesse zu befolgen.	1				
Einfachauswahl	Ein gut gelaunter Kollege spricht im Restaurant mit Ihnen über Firmengeheimnisse.	Ich weise den Kollegen darauf hin das Gespräch an einen anderen Ort zu verlegen.	1				
Einfachauswahl	Sie erhalten in der Cafeteria einen USB-Stick als Werbegeschenk.	Ich bespreche die Situation mit dem IT-Sicherheitsbeauftragten.	1				
Einfachauswahl	Eine Person, die sich als Polizist meldet, bittet Sie am Telefon Firmengeheimnisse herauszugeben.	Ich gebe keine Firmengeheimnisse am Telefon preis.	1				
Einfachauswahl	Ihre Passwörter bewahren Sie aus Sicherheitsgründen an folgendem Ort auf.	Keine der anderen Antworten trifft zu.	1				
Einfachauswahl	Vor der Eingangstüre zu den Büroräumen stellt sich Herr Müller als neuer Kollege vor. Da dieser einen großen Kuchen mitbringt, lässt er sich ein Foto machen.	Ich nehme Herrn Müller den Kuchen ab, sodass er seinen Mitarbeiter nicht beleidigen muss.	1				
Einfachauswahl	Sie werden in einer E-Mail glaubhaft erpresst Firmengeheimnisse zu verraten, da der Erpresser sonst Nacktbilder von Ihnen veröffentlichen wird.	Keine der anderen Antworten trifft zu.	1				
Einfachauswahl	Sie nehmen für die Anreise zu einem Kunden den Zug als Verkehrsmittel. Die Zeit der Zugfahrt können Sie als Arbeitszeit geltend machen.	Bei mobilem Arbeiten bringe ich einen Blickschutzfilter am Laptop mit.	1				
Einfachauswahl	Der technische Support benötigt Ihr Benutzerpasswort um ein Laptop-Problem per Fernwartung zu lösen. Tatsächlich ist das Problem aber ein Hardware-Problem.	Ich bestehe darauf, dass mein Laptop-Problem anders gelöst wird.	1				

Abbildung 6.6: Fragebogen Hilfstabelle

Zuletzt werden die Datensätze durch das VBA-Skript in einen Punktwert überführt. Da bei Multiple-Choice-Fragen das Phänomen des Ratens eine Verzerrung der Ergebnisse bewirkt, wird die Ratekorrektur nach Döring [Dör+15, Seite 441] umgesetzt. Das Skript wird nachfolgend erläutert. Für jeden Datensatz werden die Antworten zuerst nach Antworttyp ausgewertet.

Single answer questions

Bei Fragen mit Alternativantworten wird die gegebene Antwort mit der korrekten Antwort aus der Hilfstabelle 6.6 abgeglichen und die jeweilige Punktzahl für die Antwort ausgelesen. Die Gesamtpunktzahl des Antworttyps für einen Datensatz wird

¹Bei Hashverfahren handelt es sich um Einwegfunktionen, die praktisch nicht umkehrbar sind.

anhand der folgenden Formel berechnet [Dör+15, Seite 441]:

$$x_{corr} = N_R \frac{N_F}{k - 1}$$

x_{corr} = korrigiertes Ergebnis

N_R = Anzahl richtig gelöster Aufgaben

N_F = Anzahl falsch gelöster Aufgaben

k = Anzahl der Antwortalternativen

Die Punktzahl für "single answer questions" mit vier Antwortmöglichkeiten wird äquivalent zu den Fragen mit Alternativantworten berechnet [Dör+15, Seite 441].

Multiple answer questions

Für Antworten, bei denen mehrere vorgegebene Antwortmöglichkeiten zutreffen können, wird der Rate-Effekt anders neutralisiert [Dör+15, Seite 441]. Für jedes richtige Ankreuzen wird ein Pluspunkt, für jedes falsche Ankreuzen ein Minuspunkt und für jede nicht angekreuzte Antwortvorgabe kein Punkt vergeben. Die Antworten sind in der Hilfstabelle jeweils mit einem Plus- oder Minuspunkt versehen und werden durch das Skript ausgelesen.

Insgesamt gibt es 27 korrekte Antworten, was auch die Anzahl der erreichbaren Gesamtpunktzahl der Fragebogen darstellt. Nachdem die Werte der drei Antworttypen ausgewertet sind, werden die Ergebnisse addiert und als Gesamtpunktzahl einem Hash zugeordnet.

Nachdem die Datensätze im ersten Fragebogen gesammelt wurden, wurde eine zweite Liste unter Verwendung der Pseudonyme erstellt, welche ausschließlich die Hashes der Probanden getrennt nach Experimental- und Kontrollgruppen enthält. Diese Liste dient dazu, die Ergebnisse im weiteren Verlauf der Studie mittels der Funktion

SVERWEIS² den richtigen Gruppen zuzuordnen. Die Anzahl der ausgefüllten Prä-Fragebogen ist höher ausgefallen als die eigentliche Anzahl an Probanden. Grund hierfür ist, dass der Link des ersten Fragebogens von einem der Probanden in einer Chatgruppe geteilt wurde. Die Hashes dieser Probanden sind der Kontrollgruppe zugeordnet, da sie nicht an der Intervention teilnehmen. Nach Ausfüllen des zweiten Fragebogens wurden diese ausgefiltert, da sie keinem Hash im Post-Fragebogen zugeordnet werden können.

²<https://support.office.com/de-de/article/sverweis-funktion-0bbc8083-26fe-4963-8ab8-93a18ad188a1> abgerufen am 01.03.2020

Kapitel 7

Ergebnisse

7.1 Einblick in die Daten

Dieses Unterkapitel dient dazu einen ersten Einblick in die erhobenen Daten zu geben.

7.1.1 Rücklaufquote

Für die Studie zeichnet sich ein hoher Rücklauf ab. Insgesamt haben 38 Personen sowohl den Prä-Fragebogen als auch den Post-Fragebogen ausgefüllt. Damit ergibt sich eine Rücklaufquote von etwa 86% bei 44 zu erwartenden Datensätzen. Die Daten umfassen ausgefüllte Fragebogen von 20 Testpersonen, die der Experimentalgruppe zugeordnet werden können. Folglich sind Messpunkte von 18 Testpersonen vorhanden, die der Kontrolle zuzuordnen sind.

Grundsätzlich werden pro Testperson zwei Messpunkte erhoben. Probanden, welche den Post-Fragebogen nach Verstreichen der Frist nicht ausgefüllt haben, werden von der Auswertung ausgeschlossen. Ebenso werden alle Messpunkte verworfen, wenn dem angegebenen Pseudonym nur ein Messpunkt zuzuordnen ist. Datensätze, deren Pseudonym sich im Prä-Fragebogen und Post-Fragebogen unterscheiden werden nicht verworfen, sofern diese zweifelsfrei zugeordnet werden können. Während der Studiendauer beendete keiner der Probanden aktiv die weitere Studienteilnahme durch das Widersprechen der weiteren Datenverarbeitung.

7.1.2 Population

In dieser Studie wird die Grundgesamtheit anhand des Merkmals Karriere unterschieden. Dies dient dazu eine Aussage über die externe Validität treffen zu können. So lässt sich feststellen, dass die Stichprobe zu 42% aus Arbeitnehmern besteht und einen Anteil von 39% Informatikstudierenden umfasst. Eine starke Repräsentation von Berufstätigen ist sehr erwünscht. Der Umstand, dass überproportional viele Studierende vertreten sind, ist nicht optimal. Jedoch sind diese auch der beschriebenen Zielgruppe zugehörig. Der durch die Probanden angegebene berufliche Status wird in Abbildung 7.1 mit absoluten Werten angegeben.

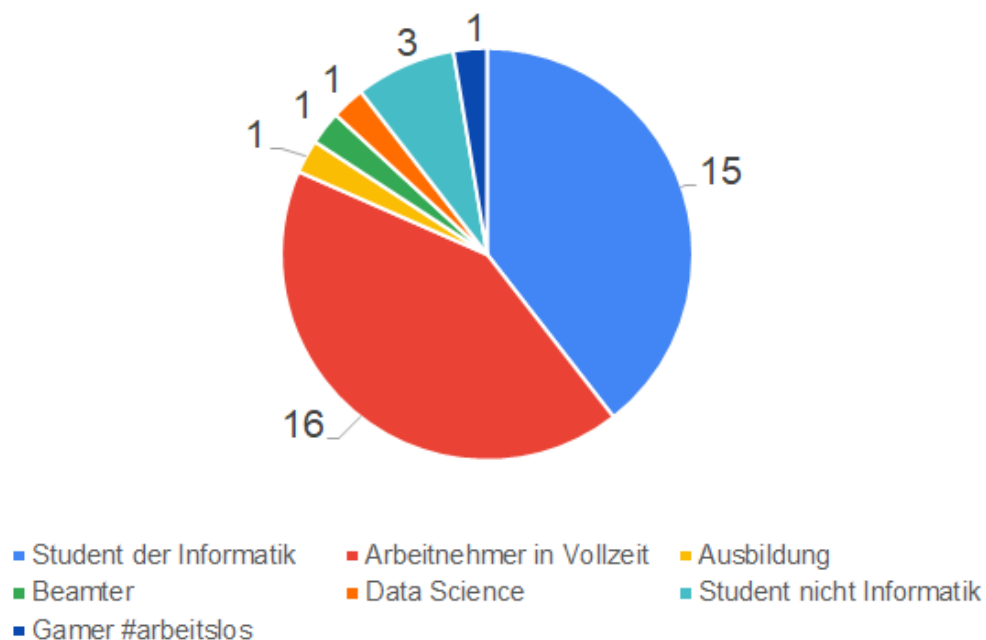


Abbildung 7.1: Beruflicher Status der Testpersonen

7.1.3 Selbsteinschätzung der Testpersonen

Im zweiten Abschnitt des Fragebogens werden die Testpersonen gebeten eine Selbsteinschätzung abzugeben. Die Aussagen zur Messung der persönlichen Einstellung sind formuliert als "Ich stimme dem zu". Die Probanden können vier Aussagen jeweils mehr oder weniger zustimmen. Dabei stellt die Abbildung 7.2 die Daten für die Experimentalgruppe und die Abbildung 7.3 die Daten der Kontrolle dar. Die Balkendiagramme zeigen sowohl die Prä- als auch die Post-Daten in einem Säulendiagramm.

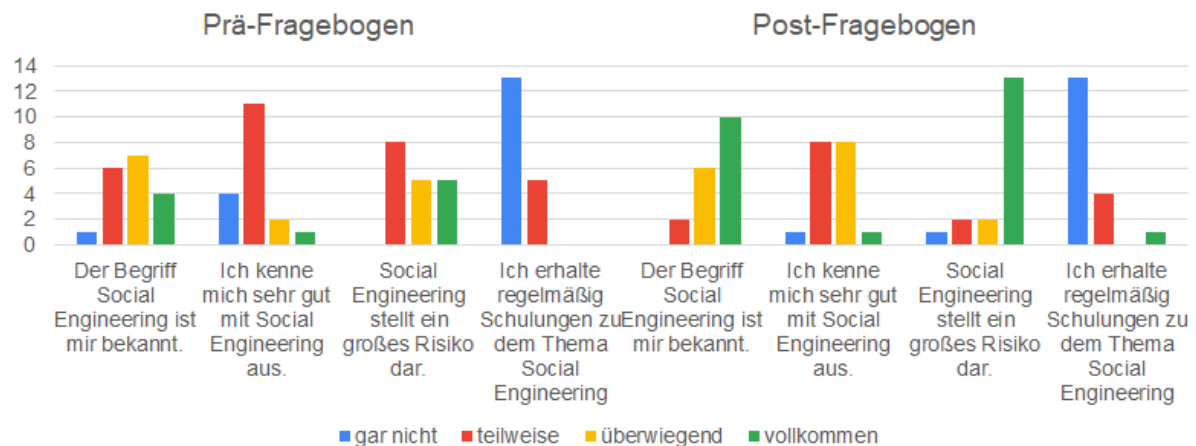


Abbildung 7.2: Statistiken der Likert-Skala (Experimentalgruppe)

In der Grafik 7.2 zeigt sich anhand der ersten zwei Aussagen die Selbsteinschätzung, dass Probanden nach der Intervention ein größeres Wissen über das Themengebiet Social Engineering vermuten. Auffällig ist die Einschätzung bezüglich der dritten Frage. Hier ändert sich das Meinungsbild bezüglich des Risikos. Es wird, bezogen auf Social Engineering Attacken, nun höher eingeschätzt. Erwähnenswert ist auch, dass nahezu keiner der Probanden Schulungen zu dem Themenfeld erhält.

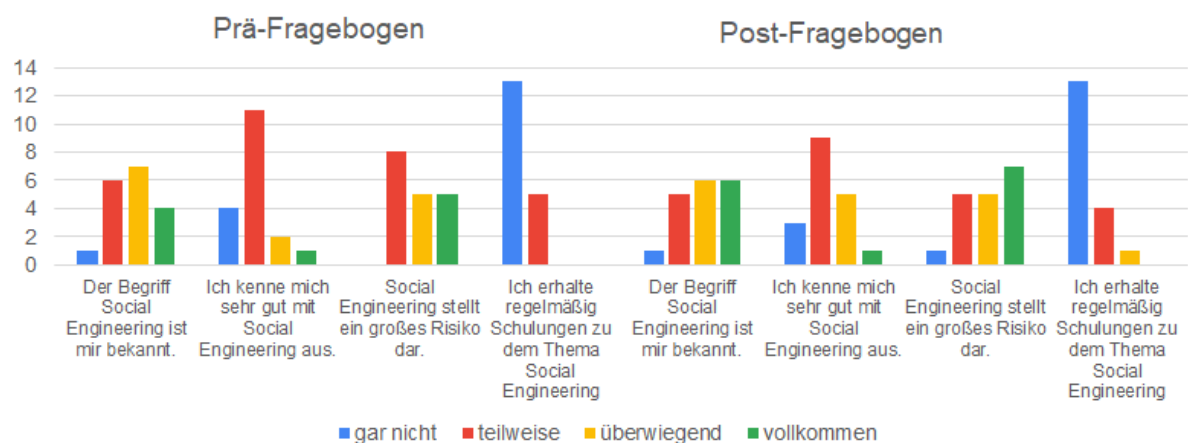


Abbildung 7.3: Statistiken der Likert-Skala (Kontrolle)

In der Grafik 7.3 spiegelt sich die Selbsteinschätzung der Kontrolle wider. Interessanterweise ist hier ebenfalls ein leichter Anstieg bei den ersten zwei Aussagen zu erkennen. Die Probanden schätzen ihr Wissen also auch ohne Intervention bei dem Post-Fragebogen besser ein. Die Einschätzung des potentiellen Risikos bleibt hingen-

gen unverändert. Auch die Kontrollgruppe erhält nach eigener Aussage selten bis gar keine Schulungen.

7.1.4 Vergleich zwischen Primär- und Sekundärgruppe

Wie in Kapitel 4.2.1 beschrieben, adressiert das Lernspiel SANIAG eine große Zielgruppe, welche in Primär- und Sekundärgruppe aufgeteilt werden kann. Dieses Kapitel beschreibt die Zuordnung der Probanden in die Primär- und Sekundärgruppe. Durch den Vergleich der Selbsteinschätzung soll die Zuordnung in die jeweiligen Gruppen bekräftigt werden. Zuletzt wird anhand eines Vergleichs der Awareness beider Gruppen durch das Lernspiel SANIAG der Lerneffekt der Sekundärgruppe betrachtet. Dadurch soll ermittelt werden, ob Spieler mit erhöhten Vorkenntnissen von Social Engineering ebenfalls durch das Lernspiel dazulernen können.

Aufteilung in Primär- und Sekundärgruppe

Eine Aufteilung in die jeweiligen Gruppen wird einzig anhand der Experimentalgruppe durchgeführt, da nur diese Probanden an der Intervention teilnehmen. Die Zuordnung erfolgt mittels der erreichten Gesamtpunktzahl des Prä-Fragebogens. Als Schwellenwert werden 18 Punkte gesetzt, was zwei Drittel der erreichbaren Gesamtpunktzahl entspricht. Jeder Proband der Experimentalgruppe, welcher diesen Schwellenwert im Prä-Fragebogen nicht erreicht, ist im Rahmen dieser Arbeit der Primärgruppe zugeordnet. Demnach sind die Probanden mit 18 oder mehr Punkten entsprechend der Sekundärgruppe zugeordnet. 61% aller Probanden der Experimentalgruppe gehören der Primärgruppe an. Folglich ordnen wir 39% der Probanden aus der Experimentalgruppe der Sekundärgruppe zu.

Vergleich der Selbsteinschätzung

Nach der Zuordnung in Primär- und Sekundärgruppen wird die Selbsteinschätzung der Gruppen betrachtet. Hierzu wird folgende Punkteskala aus den Antwortmöglichkeiten der Fragen in Abschnitt 2 des Fragebogens erstellt (siehe Tabelle 7.1).

Antwort	Punktzahl
gar nicht	0
teilweise	1
überwiegend	2
vollkommen	3

Tabelle 7.1: Punkteskala der Selbsteinschätzung

Nach Umwandlung der Antworten in einen numerischen Wert, werden die Mittelwerte betrachtet. Die Sekundärgruppe bewertet sich beim Ausfüllen des Prä-Fragebogens durchschnittlich 15% besser als die Primärgruppe und spiegelt den erhöhten Wissensstand wider.

Vergleich der Awareness

Zuletzt wird die Awareness der beiden Gruppen betrachtet. An dieser ist zu erkennen, dass die Primärgruppe sich in etwa doppelt so sehr verbessert hat als die Sekundärgruppe. Die Primärgruppe verbessert sich durchschnittlich um 6,72 Punkte, während die Sekundärgruppe eine Verbesserung von 3,28 Punkten erzielt. Dementsprechend kann davon ausgegangen werden, dass Spieler mit einem erhöhten Wissensstand auf dem Gebiet des Social Engineerings, im Falle einer signifikanten Verbesserung durch das Lernspiel SANIAG, weiteres Wissen erlangen können. Im weiteren Verlauf dieser Arbeit wird jedoch nicht zwischen Primär und Sekundärgruppe unterschieden. Die Zuordnung in Primär- und Sekundärgruppen ist für die Beantwortung der Forschungsfrage dieser Arbeit unwesentlich.

7.1.5 Erzielte Punktwerte der Testpersonen

Die empirisch erhobenen Daten sind in quantifizierter Form in den Abbildungen 7.4 und 7.5 aufgetragen. Dabei sind die Messwerte der Prä-Fragebogen rot und die des Post-Fragebogens blau eingezeichnet. Die Daten sind aufsteigend nach der Verbesserung (Post-Punktwert minus Prä-Punktwert) von links nach rechts sortiert.

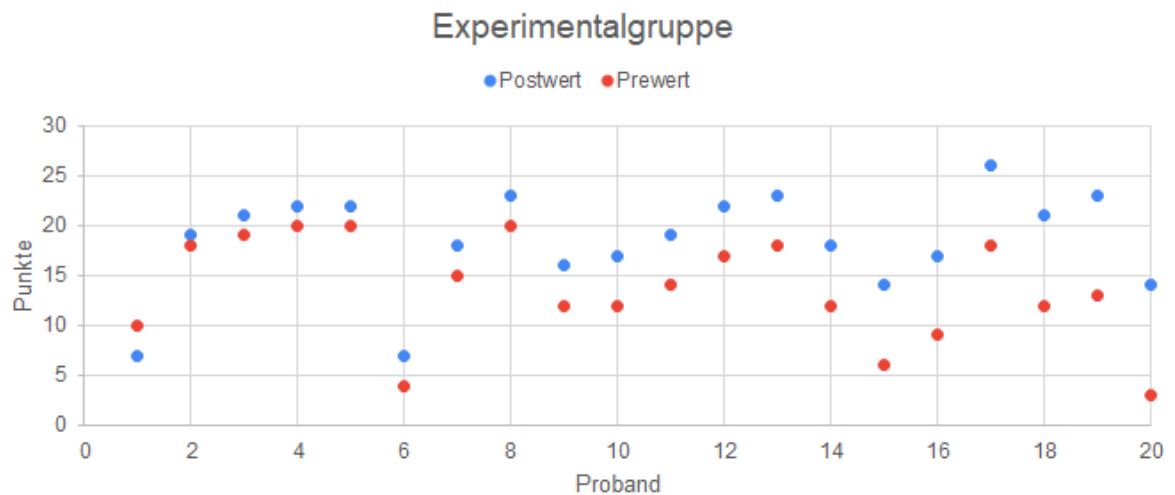


Abbildung 7.4: Messpunkte der Experimentalgruppe

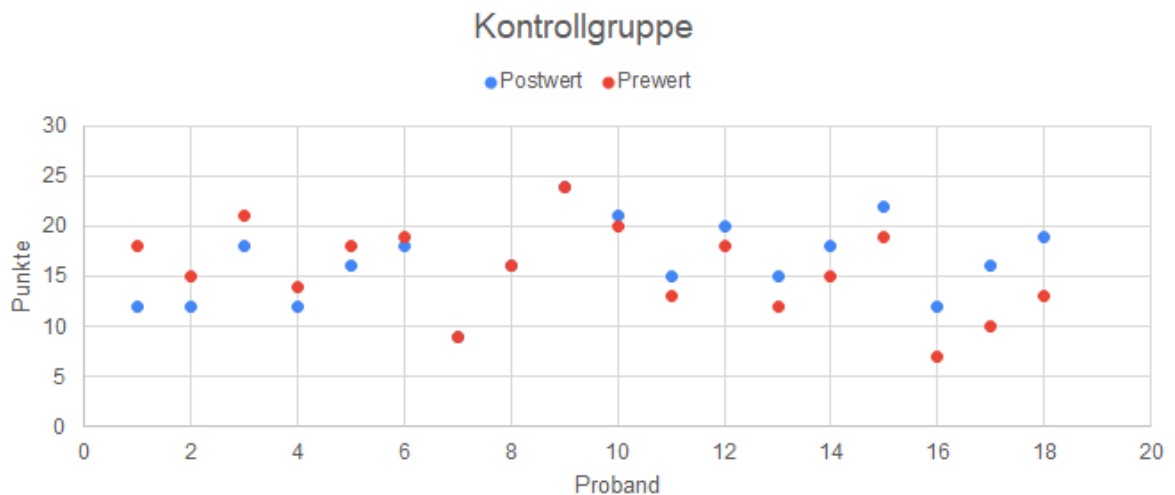


Abbildung 7.5: Messpunkte der Kontrolle

Die Auswertung und Interpretation der Daten erfolgen im nachfolgenden Kapitel.

7.2 Statistische Auswertung

In dieser Arbeit wird der Grundsatz der American Psychological Association (APA) verfolgt, der besagt dass das statistische Testverfahren nicht aufwändiger oder komplexer ist als es die Fragestellung bzw. die Hypothesenprüfung erfordert.[HSE13] Die nachfolgend durchgeführten Auswertungen stützen sich auf dem Verfahren der Analysis of Variance (ANOVA). Die Berechnungen werden mittels der Software Microsoft Excel durchgeführt. Bezeichnungen und übliche Maßeinheiten aus der Statistik sind im Glossar erläutert.

7.2.1 Prämissen der ANOVA

Die statistische Auswertung der Daten soll mittels ANOVA erfolgen. Die Aussagekraft einer Varianzanalyse hängt davon ab, inwieweit ihre Voraussetzungen erfüllt werden. Zwar gilt das Verfahren als robust gegenüber einer Verletzung der Voraussetzungen, jedoch soll in dieser Arbeit eine hohe Zuverlässigkeit erzielt werden.

Prämisse	Prüfungsmethode	Verletzung heilbar über
Keine Ausreißer	Plausibilitätsprüfung	Eliminierung von Probanden
Randomisierte Gruppenzuordnung	(ex ante festgelegt)	Muss im Vorhinein sichergestellt werden
Gruppengröße > 20	Sichtung des Datensatzes	Muss im Vorhinein sichergestellt werden
Varianzhomogenität	Levene-Test	Gleichbesetzung der Zellen
Normalverteilung	Kolmogorov-Smirnov-Test	Gleichbesetzung der Zellen

Tabelle 7.2: Prämissen der ANOVA nach Huber[Hub+14]

Huber und andere identifizieren insgesamt fünf unterschiedliche Prämissen, wie in Tabelle 7.2 abgebildet [Hub+14, Tabelle 4.4]. Unter anderem soll die Gruppenzuteilung

randomisiert erfolgen und die Stichprobengröße mehr als 20 Testpersonen umfassen. Die beiden Prämissen sind offensichtlich gegeben. Die verbliebenen drei Voraussetzungen werden mittels statistischer Verfahren berechnet.

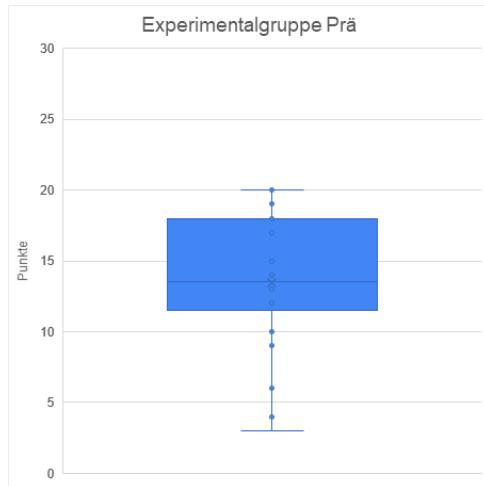
7.2.1.1 Ausreißer

Ausreißer sind Messwerte, die nicht den Erwartungen entsprechen und deutlich von der Messreihe abweichen. Ein einziger Ausreißer kann ein sonst signifikantes Ergebnis nicht signifikant werden lassen. Daher wird die Messreihe auf Ausreißer hin untersucht.

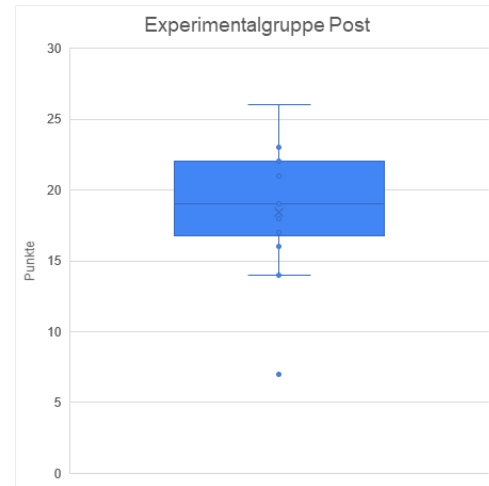
Die Untersuchung nach Ausreißern wird mit Hilfe des Interquartilabstandes und eines Boxplots in Microsoft Excel angestellt. Die Definition eines Ausreißers wird nach Müller-Benedict übernommen.[Mül11, S.94-99] Zuerst werden jeweils das erste und dritte Quartil in Excel mittels der Funktion `QUARTILE.INKL()`¹ errechnet. Aus der Differenz der beiden Werte ergibt sich der Interquartilsabstand. In den Kastengrafiken entspricht dieser der Höhe der Box. Die Box entspricht dem Bereich, in dem die mittleren 50% der Messwerte liegen. Mögliche Ausreißer liegen 1,5 Quartilsabstände über dem dritten Quartil bzw. 1,5 Quartilsabstände unter dem ersten Quartil. Im Diagramm liegen sie außerhalb der Antenne bzw. dem sogenannten Whisker.

Die Abbildungen 7.6 und 7.7 zeigen jeweils den Boxplot mit den Quartilsabständen. In den erstellten Boxplots können genau zwei Ausreißer identifiziert werden. Hierbei handelt es sich zweimal um den gleichen Messwert der Post-Punktwerte der Experimentalgruppe. Die zwei Ausreißer werden für die weitere Analyse eliminiert.

¹<https://support.office.com/de-de/article/quartile-inkl-funktion-1bbacc80-5075-42f1-aed6-47d735c4819d> abgerufen am 01.03.2020

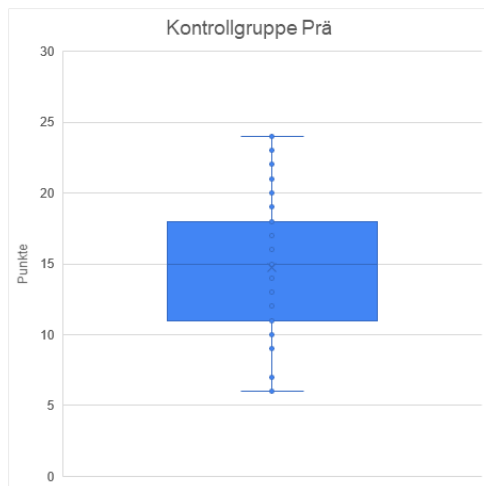


(a) Experimentalgruppe Prä

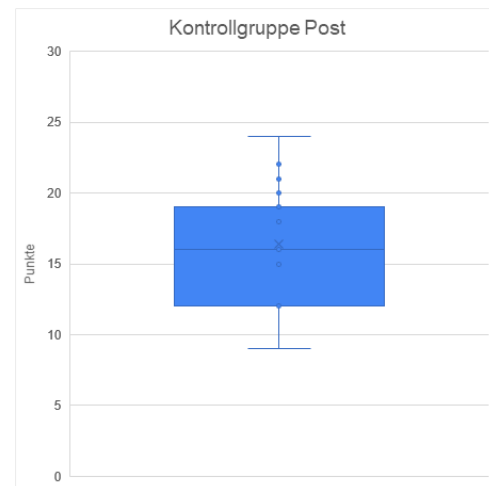


(b) Experimentalgruppe Post

Abbildung 7.6: Ausreißer-Messwerte der Experimentalgruppe



(a) Kontrollgruppe Prä



(b) Kontrollgruppe Post

Abbildung 7.7: Ausreißer-Messwerte der Kontrolle

7.2.1.2 Varianzhomogenität

Varianzhomogenität (auch Homoskedastizität) ist gegeben, wenn die Varianzen der Prä-Gruppen in etwa gleich sind. Eine starke Abweichung der Varianzen würde die Wahrscheinlichkeit erhöhen einen Fehler erster Art zu begehen. Die Messwerte werden mittels dem Levene-Test auf Varianzhomogenität hin untersucht. Der Levene-Test beruht auf einem F-Test, bei dem die Teststatistik der Quotient der Varianzen zweier Stichproben ist.[KSV12] Der Test wird mit der Software Microsoft Excel für alle Gruppen manuell durchgeführt, da Excel die Funktionalität nicht bereitstellt.

Zunächst werden für die zwei Stichproben jeweils die Varianzen σ_1^2 und σ_2^2 berechnet. Dies erfolgt durch die Funktion VAR.S()² in Excel. Anschließend wird eine Teststatistik F mit σ_1^2/σ_2^2 berechnet, wobei die Stichprobe mit der größeren Varianz σ_1^2 im Zähler des Quotienten steht. Zuletzt wird der kritische Wert der F-Verteilung bestimmt. Dies geschieht mit der Funktion mit F.INV()³ in Excel bei $\alpha = 0,05$ und 17 Freiheitsgraden. Wenn der kritische Wert größer als die Teststatistik ist, dann wird von Varianzgleichheit gesprochen. Die Werte der beiden Prä-Messpunkte sind der Tabelle 7.3 zu entnehmen.

Varianzen σ_1^2 (Experimentalgruppe)	24,47058824
Varianzen σ_2^2 (Kontrolle)	19,89869281
Teststatistik F	1,229758581
kritischer Wert	2,271892889

Tabelle 7.3: Varianzgleichheit der Prä-Gruppen

Die Varianzen der Prä-Messpunkte erfüllen demnach die Homogenität der Varianzen.

7.2.1.3 Normalverteilung der abhängigen Variable

Eine weitere Prämisse besteht darin, dass die abhängige Variable in etwa einer Normalverteilung entspricht. Ein geeignetes Verfahren, um die Normalverteilung von Messwerten zu prüfen, ist der Kolmogorov-Smirnov-Test (KS-Test).[Mas51]

Mangels einer Softwarelizenz für IBM SPSS Statistics muss auch der KS-Test händisch berechnet werden. Microsoft Excel bietet für den KS-Test keine Funktion. Die zugrundeliegenden Werte der Berechnung samt Ergebnis sind der Tabelle 7.4 zu entnehmen.

²<https://support.office.com/de-de/article/var-s-funktion-913633de-136b-449d-813e-65a00b2b990b>
abgerufen am 01.03.2020

³<https://support.office.com/de-de/article/f-inv-funktion-0dda0cf9-4ea0-42fd-8c3c-417a1ff30dbe>
abgerufen am 01.03.2020

Zunächst werden alle Prä-Messwerte der Größe nach aufsteigend dem fortlaufenden Rang von 1 bis 36 zugeordnet. Von den Prä-Messwerten wird der Mittelwert sowie die Standardabweichung mit den Excel Funktionen MITTELWERT()⁴ und STABW.S()⁵ berechnet. Danach wird der tatsächlich kumulierte Anteil der Größe mittels der Excel Funktion NORM.VERT()⁶ berechnet. Die Absolutbeträge der Differenzen der zwei vorletzten Spalten werden in der letzten Spalte eingetragen. Der maximale Wert der letzten Spalte von Abweichungen stellt die Teststatistik dar. Der kritische Wert kann für $n > 35$ in gängigen KS-Tabellen[Uni] nicht abgelesen werden. Jedoch ist eine grobe Approximation für $\alpha=0,05$ und $n=36$ möglich:

$$K_{36;1-0.05/2} = \frac{\sqrt{\ln \frac{2}{0.05}}}{\sqrt{2 * 36}} = 0.226350253$$

Wenn die Teststatistik kleiner als der kritische Wert ist, kann von einer zugrundeliegenden Normalverteilung ausgegangen werden. Diese liegt mit 0,15751262 unterhalb des kritischen Wertes. Demnach wird auf eine Normalverteilung der Messwerte bei der Prä-Gruppen geschlossen.

7.2.1.4 Sphärizität

Normalerweise muss für die mehrfaktorielle Varianzanalyse auch die Sphärizitätsannahme überprüft werden. Diese ist jedoch bei Faktoren mit nur zwei Stufen stets gegeben. Der Faktor der Gruppenzugehörigkeit hat die Stufen Experimentalgruppe und Kontrolle. Der Faktor der Zeit hat die Stufen Prä- und Post-Intervention. Der mathematische Hintergrund ist bereits in Kapitel 5.3 erläutert worden. An dieser Stelle wird auf einen Mauchly-Test, welcher auf Sphärizität prüft, verzichtet.

⁴<https://support.office.com/de-de/article/mittelwert-funktion-047bac88-d466-426c-a32b-8f33eb960cf6> abgerufen am 01.03.2020

⁵<https://support.office.com/de-de/article/stabw-s-funktion-7d69cf97-0c1f-4acf-be27-f3e83904cc236> abgerufen am 11.03.2020

⁶<https://support.office.com/de-de/article/norm-vert-funktion-edb1cc14-a21c-4e53-839d-8082074c9f8d> abgerufen am 11.03.2020

Rang	Größe	(Rang-1)/n	tats. kum. Anteil	Differenz
1	3	0	0.00532173	0.00532173
2	6	0.02777778	0.02779972	2.1944E-05
3	7	0.05555556	0.04448849	0.01106706
4	9	0.08333333	0.1013082	0.01797487
5	9	0.11111111	0.1013082	0.00980291
6	10	0.13888889	0.14439278	0.00550389
7	12	0.16666667	0.26300672	0.09634006
8	12	0.19444444	0.26300672	0.06856228
9	12	0.22222222	0.26300672	0.0407845
10	12	0.25	0.26300672	0.01300672
11	12	0.27777778	0.26300672	0.01477105
12	13	0.30555556	0.33696514	0.03140958
13	13	0.33333333	0.33696514	0.0036318
14	13	0.36111111	0.33696514	0.02414597
15	14	0.38888889	0.41784212	0.02895323
16	14	0.41666667	0.41784212	0.00117546
17	15	0.44444444	0.5023642	0.05791975
18	15	0.47222222	0.5023642	0.03014198
19	15	0.5	0.5023642	0.0023642
20	16	0.52777778	0.58677988	0.0590021
21	17	0.55555556	0.66735184	0.11179629
22	18	0.58333333	0.74084596	0.15751262
23	18	0.61111111	0.74084596	0.12973485
24	18	0.63888889	0.74084596	0.10195707
25	18	0.66666667	0.74084596	0.07417929
26	18	0.69444444	0.74084596	0.04640151
27	18	0.72222222	0.74084596	0.01862374
28	19	0.75	0.80491215	0.05491215
29	19	0.77777778	0.80491215	0.02713438
30	19	0.80555556	0.80491215	0.0006434
31	20	0.83333333	0.8582841	0.02495076
32	20	0.86111111	0.8582841	0.00282701
33	20	0.88888889	0.8582841	0.03060479
34	20	0.91666667	0.8582841	0.05838257
35	21	0.94444444	0.90077587	0.04366858
36	24	0.97222222	0.97294872	0.0007265
Anzahl	36		Teststatistik	0.15751262
Mittelwert	14.9722222		Kritischer Wert	0.22635025
Standardabw.	4.68728439			

Tabelle 7.4: Kolmogorov-Smirnov-Test

7.2.2 Zweifaktorielle ANOVA mit Messwiederholung

In dieser Arbeit wird ein randomisierter Prä-Post-Kontrollgruppenvergleich durchgeführt. [Dör+15, S.727-730] Dabei handelt es sich um ein typisches experimentelles Design, das eine Kombination des Kontrollgruppendesigns und Messwiederholungsdesigns darstellt. Das Kontrollgruppendesign strebt einen Vergleich zwischen der Experimentalgruppe und der Kontrollgruppe an. Das Messwiederholungsdesign wird gewählt, wenn die abhängige Variable (der erzielte Punktwert) vor der Intervention und nach der Intervention verglichen werden soll. Entscheidend bei dem Design ist, dass der Messzeitpunkt als weitere unabhängige Variable in das Design aufgenommen wird.

Für den Vergleich wird das statistische Auswertungsverfahren ANOVA eingesetzt. Die Durchführung orientiert sich nach Cleff[Cle18, S.192]. Welches Verfahren zur Auswertung durchgeführt wird, ist vor Beginn der Studie festgelegt worden und in Kapitel 5 bereits beschrieben. Prinzipiell soll ein Forschungsdesign konsequent beibehalten werden. In dem konkreten Fall handelt es sich bei dem Verfahren um eine zweifaktorielle ANOVA, da zwei unabhängige Variablen betrachtet werden. Eine unabhängige Variable stellt die Gruppenzugehörigkeit dar (Experimental- und Kontrollgruppe). Zusätzlich wird der Zeitpunkt der Messung (Vorher- bzw. Nachher-Messung in Bezug auf die Intervention) als weitere unabhängige Variable verstanden. Eine ANOVA mit Messwiederholung wird auch als rmANOVA bezeichnet.

Die zugrundeliegenden Messwerte für alle nachfolgend durchgeführten statistischen Auswertungen sind dem Anhang D zu entnehmen. Die nun durchgeführte zweifaktorielle ANOVA wird mit Hilfe des Programms Microsoft Excel berechnet. Die Tabelle 7.5 gewährt zunächst einen Überblick, in welcher Relation die empirisch erhobenen Messwerten zueinander stehen. Zu sehen sind vier Innersubjektfaktoren, nämlich, ob es sich um den Messwert der Experimentalgruppe bzw. der Kontrolle handelt oder ob der Messpunkt vor bzw. nach der Intervention erhoben wurde.

	Prä-Messwerte	Post-Messwerte	Gesamt
<i>Experimentalgruppe</i>			
Anzahl	18	18	36
Summe	258	355	613
Mittelwert	14.3333333	19.7222222	17.0277778
Varianz	24.4705882	11.2712418	24.8277778
<i>Kontrollgruppe</i>			
Anzahl	18	18	36
Summe	281	295	576
Mittelwert	15.6111111	16.3888889	16
Varianz	19.8986928	16.1339869	17.6571429
<i>Gesamt</i>			
Anzahl	36	36	
Summe	539	650	
Mittelwert	14.9722222	18.0555556	
Varianz	21.9706349	16.168254	

Tabelle 7.5: Deskriptive Statistiken

Zunächst bestimmt eine mehrfaktorielle ANOVA lediglich, ob überhaupt signifikante Unterschiede zwischen den Faktoren vorliegen. Ein möglicher Lerneffekt durch die Intervention würde sich bei einem Messwiederholungsdesign in einem signifikanten Interaktionseffekt der zweifaktoriellen Varianzanalyse widerspiegeln.[Dör+15, S.201-202] Eine ANOVA kann vorerst keine Aussage darüber treffen, welche Gruppe eine Signifikanz erreicht oder wie hoch die Effektstärke ausfällt.

ANOVA						
<i>Streuungsursache</i>	<i>SS</i>	<i>df</i>	<i>MS</i>	<i>F</i>	<i>P-Wert</i>	<i>krit. F-Wert</i>
Stichprobe	19.0138889	1	19.0138889	1.05964577	0.30694363	3.98189626
Spalten	171.125	1	171.125	9.53681191	0.00291487	3.98189626
Wechselwirkung	95.6805556	1	95.6805556	5.33228612	0.02397869	3.98189626
Fehler	1220.16667	68	17.9436275			
Gesamt	1505.98611	71				

Tabelle 7.6: Zweifaktorielle ANOVA mit Messwiederholung

Die drei Zeilen in Tabelle 7.6 der rmANOVA werden nun bezüglich Haupteffekte und Interaktionseffekte interpretiert. Prinzipiell sind die F-Werte und P-Werte entscheidend, ob ein signifikanter Unterschied vorliegt. Statistische Signifikanz ist gegeben, wenn der kritische F-Wert kleiner dem Wert der Spalte *F* ist und zugleich der P-Wert unterhalb des Signifikanzniveaus von $\alpha = 0,05$ liegt.

Stichprobe

Die von Excel beschriftete Zeile *Stichprobe* beschreibt den Haupteffekt, ob die Gruppenzugehörigkeit einen signifikanten Unterschied zur Folge hat. Da der P-Wert von 0,30694363 deutlich über der Grenze von 0,05 liegt, kann nicht auf einen signifikanten Haupteffekt zwischen den Faktoren Experimentalgruppe und Kontrollgruppe geschlossen werden. Das Fehlen dieses Haupteffekts bedeutet, dass beide Gruppen generell gleich wären, würde eine der Gruppen nicht der Intervention ausgesetzt sein.

Spalten

Die von Excel beschriftete Zeile *Stichprobe* beschreibt den Haupteffekt bezüglich des Unterschieds zwischen den Prä-Werten und den Post-Werten. Da der P-Wert von 0,00291487 deutlich unterhalb der Grenze von 0,05 liegt, lässt sich auf einen sehr signifikanten Unterschied zwischen den Messzeitpunkten zu schließen. Das Vorhandensein des Haupteffekts bedeutet, dass eine gewisse Variabilität der Awareness in Bezug auf den zeitlichen Verlauf gegeben ist. Die Deutung von Haupteffekten gestaltet bei gleichzeitig vorliegendem Interaktionseffekt jedoch schwierig. Der Haupteffekt kann im Rahmen dieser Studie aber vernachlässigt werden.

Wechselwirkung

Neben den zwei beschriebenen Haupteffekten bestimmt Excel in der Zeile *Wechselwirkung* den Interaktionseffekt zwischen den zwei Faktoren. Im Sinne der durchgeführten Studie handelt es sich hierbei um den maßgeblichen Effekt. Die Hypothese lautet nämlich, dass Probanden, die Teil der Experimentalgruppe sind, im Post-Fragebogen ein besseres Ergebnis erzielen würden. Die Hypothese ist also basierend

auf beiden Faktoren formuliert. Damit ist der Interaktionseffekt zu bestimmen. Die Wechselwirkung ist mit einem F-Wert von 5,33228612 gegenüber dem kritischen F-Wert von 3,98189626 bei einem P-Wert von 0,02397869 als signifikant zu betrachten.

Nachdem ein signifikanter Interaktionseffekt angenommen werden kann, werden die Prä-Post-Unterschiede der Experimentalgruppe sowie Kontrollgruppe untersucht. Hierzu eignen sich T-Tests, welche bei dem einfachen Prä-Post-Vergleich identisch mit einer einfaktoriellen ANOVA sind. Um die in Kapitel 1.3 aufgestellte Arbeitshypothese nicht sofort verwerfen zu müssen, sollte es bei der Experimentalgruppe zu einer signifikanten Veränderung der abhängigen Variable kommen. Bei der Kontrolle dagegen sollten keine signifikanten Prä-Post-Unterschiede erkennbar sein. Sofern diese Umstände zutreffen, muss anschließend die Effektstärke berechnet werden, um ein Beibehalten bzw. Verwerfen der Hypothesen zu rechtfertigen.

7.2.3 Einfaktorielle ANOVA der Experimentalgruppe Prä/Post

In dieser Sektion wird eine isolierte Betrachtung der Experimentalgruppe vorgenommen. Die zugehörige ANOVA ist in Tabelle 7.7 aufgeführt.

ZUSAMMENFASSUNG

<i>Gruppen</i>	<i>Anzahl</i>	<i>Summe</i>	<i>Mittelwert</i>	<i>Varianz</i>
Prä	18	258	14.3333333	24.4705882
Post	18	355	19.7222222	11.2712418

ANOVA

<i>Streuungsursache</i>	<i>SS</i>	<i>df</i>	<i>MS</i>	<i>F</i>	<i>P-Wert</i>	<i>krit. F-Wert</i>
Zwischen Gruppen	261.361111	1	261.361111	14.6249429	0.00053425	4.13001775
Innerhalb Gruppen	607.611111	34	17.870915			
Gesamt	868.972222	35				

Tabelle 7.7: Einfaktorielle Varianzanalyse der Experimentalgruppe

Der Mittelwertunterschied zeigt auf, dass die Experimentalgruppe grundsätzlich eine Verbesserung im Zeitverlauf aufweist. Die Veränderung der Varianz lässt darauf schließen, dass insbesondere Testpersonen eine Verbesserung zeigen, die für den Prä-Messwert einen geringeren Punktwert erzielt haben.

Der F-Wert von 14,6249429 liegt über dem kritischen Wert von 4,13001775 bei einem geringen P-Wert von 0,00053425. Dies lässt auf einen hochsignifikanten Unterschied zwischen der Prä- und Post-Erhebung innerhalb der Experimentalgruppe schließen. Das ist vereinbar mit der aufgestellten Arbeitshypothese.

7.2.4 Einfaktorielle ANOVA der Kontrolle Prä/Post

In dieser Sektion wird eine isolierte Betrachtung der Kontrollgruppe vorgenommen. Die zugehörige ANOVA ist in Tabelle 7.8 aufgeführt.

ZUSAMMENFASSUNG

<i>Gruppen</i>	<i>Anzahl</i>	<i>Summe</i>	<i>Mittelwert</i>	<i>Varianz</i>
Prä	18	281	15.6111111	19.8986928
Post	18	295	16.3888889	16.1339869

ANOVA

<i>Streuungsursache</i>	<i>SS</i>	<i>df</i>	<i>MS</i>	<i>F</i>	<i>P-Wert</i>	<i>krit. F-Wert</i>
Zwischen Gruppen	5.44444444	1	5.44444444	0.30219481	0.58610291	4.13001775
Innerhalb Gruppen	612.555556	34	18.0163399			
Gesamt		618	35			

Tabelle 7.8: Einfaktorielle Varianzanalyse der Kontrollgruppe

Für die Kontrolle zeigt sich ebenfalls ein Anstieg des Mittelwerts. Bei Betrachtung des Signifikanzwerts P von 0,58610291 bei einem Signifikanzniveau von $\alpha = 0,05$ wird deutlich, dass der Prä-Post-Vergleich nicht signifikant ausfällt. Dies ist vereinbar mit der aufgestellten Arbeitshypothese.

7.2.5 Einfaktorielle ANOVA bezüglich Awareness

Ursprünglich war geplant, lediglich die Punktwertdifferenzen (Post-Wert minus Prä-Wert) der zwei Gruppen zu vergleichen. Dieses wird in dieser Arbeit auch als Awareness bezeichnet und entspricht der Verbesserung bzw. Verschlechterung eines Probanden zwischen den Messzeitpunkten. Solch ein einfaches Differenzmaß innerhalb von Stichproben als Indikator für Unterschiede wird in der Literatur jedoch oftmals kritisiert.[Dör+15, S.732] Insbesondere, wenn die Experimental- und Kontrollgruppe bereits vor der Intervention (Prä-Werte) Unterschiede aufweisen, kann die interne Validität der Studie beeinträchtigt werden. Da die Analyse so geplant war, wird sie dennoch in Tabelle 7.9 dargestellt.

ZUSAMMENFASSUNG

<i>Gruppen</i>	<i>Anzahl</i>	<i>Summe</i>	<i>Mittelwert</i>	<i>Varianz</i>
Experimental	18	97	5.38888889	9.0751634
Kontrolle	18	14	0.77777778	10.8888889

ANOVA

<i>Streuungsursache</i>	<i>SS</i>	<i>df</i>	<i>MS</i>	<i>F</i>	<i>P-Wert</i>	<i>krit. F-Wert</i>
Zwischen Gruppen	191.361111	1	191.361111	19.170568	0.00010812	4.13001775
Innerhalb Gruppen	339.388889	34	9.98202614			
Gesamt	530.75	35				

Tabelle 7.9: Einfaktorielle Varianzanalyse der Prä-Post-Differenz

Der Vergleich der Punktwertdifferenzen zeigt einen hochsignifikanten Unterschied bei einer Prüfgröße von 19,170568 verglichen mit dem kritischen Wert von 4,13001775. Der P-Wert liegt mit 0,00010812 deutlich unter $\alpha = 0,05$. An dieser Stelle sei erneut erwähnt, dass die Werte vielmehr aus Gründen der Vollständigkeit vorgestellt werden. Statistisch gesicherte, valide Werte sind der Tabelle 7.6 zu entnehmen.

7.2.6 Berechnung der Effektstärke

An dieser Stelle kann bereits über das Hypothesenpaar entschieden werden. Um eine genauere Aussage treffen zu können, ist die Effektstärke interessant. In diesem Fall gibt sie an, wie hoch der Lerneffekt ausfällt. Microsoft Excel beherrscht die Berechnung der Effektstärke nicht, weshalb auf folgende Formel zur Berechnung der Effektstärke r zurückgegriffen wird [Coh13]:

$$r = \sqrt{\frac{F(1, df_R)}{F(1, df_R) - df_R}} = \sqrt{\frac{5.332286118}{5.332286118 + 68}} = 0.269655393$$

Bei einer Effektstärke von ca. 0,27 handelt es sich nach Cohen um eine schwache Effektstärke. Die Intervalle der Konventionen für schwach, mittel und stark sind in Tabelle 7.10 beschrieben.

r-Wert	Effektstärke
$0,1 \leq r < 0,3$	schwach
$0,3 \leq r < 0,5$	mittel
$r > 0,5$	stark

Tabelle 7.10: Effektstärke nach Cohen [Coh13]

7.2.7 Überprüfung der Forschungshypothese

Die in Kapitel 7.2.2 dargestellte zweifaktorielle Varianzanalyse lässt bereits die Schlussfolgerung zu, dass es signifikante Unterschiede zwischen den vier Innersubjektfaktoren gibt. Die in den Unterkapiteln 7.2.3 und 7.2.4 durchgeführten einfaktoriellen Varianzanalysen geben einen Aufschluss darüber, dass die Experimentalgruppe einen signifikanten Unterschied innerhalb der Gruppe verzeichnet. Dieser fällt bei Betrachtung der Mittelwerte positiv mit einer Steigerung der Werte im Prä-Post-Verlauf aus. Für die Kontrollgruppe hingegen ist kein signifikanter Unterschied zu verzeichnen. Letztendlich kann eine positive Steigerung der Awareness für die Experimentalgrup-

pe festgestellt werden. Der Lerneffekt fällt dabei schwach, jedoch signifikant, aus.

Die Nullhypothese, dass Spieler durch die Intervention keinen positiven Einfluss auf die Sensibilisierung verzeichnen, muss also verworfen werden. Ein positiver Effekt, hervorgerufen durch die Intervention, ist nämlich vorhanden. Im Umkehrschluss ist die aufgestellte Arbeitshypothese beizubehalten. Zusammenfassend lässt sich schlussfolgern: Das Spielen eines Lernspiels zu dem Themenfeld Social Engineering hat einen positiven Einfluss auf die Sensibilisierung bezüglich Social Engineering.

7.3 Diskussion der Ergebnisse

An der Stelle sollen die Ergebnisse dieser Forschungsarbeit hinterfragt werden.

In dieser Arbeit wird danach gestrebt ein wissenschaftlich hohes Niveau zu erreichen. Zwei Bausteine, die für eine hohe Validität sprechen, sind in der Kontrolle und der Randomisierung auszumachen. Keine der recherchierten Veröffentlichungen in Kapitel 2 beschreibt die Durchführung eines echten Experiments. In Hinblick auf die Auswertung der Messwerte werden gängige statistische Verfahren angewandt. Die Berechnung der Ergebnisse wird transparent dargestellt und die Annahme der Alternativhypothese durch die Verwerfung der Nullhypothese wird nachvollziehbar begründet. Dabei handelt es sich um signifikante Ergebnisse bei einem Signifikanzniveau von 5%.

Der Stichprobenumfang von letztlich 38 Probanden lässt, wie in Kapitel 5.3 beschrieben, haltbare Aussagen zu. Die Anzahl von mindestens 34 Probanden, wie a priori berechnet, wird jedoch nur knapp überschritten. An dieser Stelle wäre das Wiederholen des Experiments bei einem größeren Stichprobenumfang wünschenswert. Dementsprechend müssten finanzielle Mittel für die Vergütung der Testpersonen bereitgestellt werden.

Eine mögliche Verzerrung wird in der Anwesenheit der Studienleiter ausgemacht. Tatsächlich wurde die Experimentalgruppe für die Durchführung der Intervention stets von mindestens einem der Studienleiter betreut. Denkbar wäre, dass neben dem Spielen des Serious Games SANIAG auch der Kontakt zu den Studienleitern eine Rolle bei dem gemessenen Lerneffekt spielt.

Die in dieser Arbeit beschriebene schwache Effektstärke von etwa 0,27 erscheint bei Einsicht der Daten zunächst kontraintuitiv. Tatsächlich verbessert sich die Experimentalgruppe um 97 Punkte, wohingegen die Kontrollgruppe eine Verbesserung von 14 Punkten zeigt. Als Grund hierfür wird angenommen, dass sich die Experimental- und Kontrollgruppe bereits in den Prä-Fragebogen unterscheiden. Dieser Umstand soll durch die erfolgte Randomisierung weitestgehend vermieden werden, er ist dennoch nicht völlig auszuschließen. Einen Indikator für diese Annahme ist in der einfaktoriellen Varianzanalyse in Kapitel 7.2.5 zu sehen. In dem Kapitel werden lediglich die Punktwertdifferenzen (Post minus Prä-Erhebung) miteinander verglichen. Die Effektstärke würde dann etwa 0,75 betragen und wäre damit als stark einzustufen. Bei einem solch simplen Vergleich werden jedoch Gegebenheiten wie die unterschiedlichen Prä-Werte einfach eliminiert. Letztendlich kann über eine mögliche höhere Effektstärke durch die Intervention spekuliert werden.

Kapitel 8

Schlusswort

In der vorliegenden Forschungsarbeit sind wir der Fragestellung nachgegangen, ob sich Personen durch das Spielen eines Lernspiels für Social Engineering Angriffe sensibilisieren lassen. Um eine wissenschaftlich fundierte Aussage über die Wirksamkeit von Serious Games treffen zu können, wurde eine randomisierte kontrollierte Studie durchgeführt. Im Rahmen der Studie wurde das Brettspiel SANIAG mit thematischem Bezug zu Social Engineering entwickelt. Das Serious Game soll die Social Engineering Awareness der Testpersonen durch das Spielen steigern. Die Veränderung der Awareness wurde mittels standardisiertem Online-Fragebogen ermittelt. Anschließend wurden die empirisch erhobenen Daten anhand des Verfahrens der Varianzanalyse statistisch ausgewertet. Die Ergebnisse der Studie zeigen, dass ein statistisch signifikanter Anstieg der Social Engineering Awareness in Folge der Intervention (Spielen des Serious Games) zu verzeichnen ist.

Durch die Beantwortung der Forschungsfrage erhoffen wir uns, neben dem Gewinn an wissenschaftlicher Erkenntnis, einen Beitrag zur Stärkung der Informationssicherheit leisten zu können. Ebenso ist unsere Intention, dass die vorliegende Arbeit Motivation für weitere Forschungsaktivitäten ist. Ein möglicher Gegenstand nachfolgender Arbeiten könnte in einem direkten Vergleich von unterschiedlichen Maßnahmen zur Sensibilisierung liegen. Beispielsweise könnten zusätzlich klassische Schulungsansätze für Social Engineering auf ihren Effekt hin untersucht werden.

Abkürzungsverzeichnis

ANOVA Analysis of Variance (dt. Varianzanalyse)

CSV Comma-separated values

HBSE Human-based Social Engineering

NIST National Institute of Standards and Technology

rmANOVA repeated measures Analysis of Variance (dt. Varianzanalyse mit Messwiederholung)

SANIAG Saed und Niklas' Awareness Game

TBSE Technical-based Social Engineering

VBA Visual Basic for Applications

Glossar

Anzahl der Freiheitsgrade (df) Die Anzahl der Freiheitsgrade bestimmen die Anzahl der Werte, die geändert werden können, ohne den interessierenden statistischen Parameter zu beeinflussen.

F-Test Bei der Varianzanalyse ist mit dem F-Test der Test gemeint, der die Varianzen zweier Stichproben auf Unterschiede hin prüft.

Kritischer F-Wert Mittels dem kritischen Wert kann die Nullhypothese in der Teststatistik zurückgewiesen werden. Sie beschreibt einen Punkt, der eine Menge von Werten definiert, die als kritischer oder Ablehnungsbereich bezeichnet werden.

Mittelwert Das arithmetische Mittel bzw. der Durchschnitt von zwei oder mehreren Zahlen wird als Mittelwert bezeichnet. Er ist der Quotient aus der Summe aller Werte und der Anzahl der Werte.

Mittlere Quadratsumme (MS) Die Mittel der Quadrate zeigen, wie viel der Varianz zwischen den Gruppen und innerhalb der Gruppen liegt. Je mehr Varianz es zwischen den Gruppen gibt, umso besser sagen die Gruppen die Größe vorher.

Prüfgröße (F) Die Prüfgröße dient bei einem F-Test zur Überprüfung, ob der Unterschied zwischen zwei Mittelwerten signifikant ist, indem sie mit dem kritischen F-Wert verglichen wird.

P-Wert Der P-Wert eines Signifikanztests gibt an, wie hoch die Wahrscheinlichkeit ist, dass die untersuchten Unterschiede allein auf Zufall beruhen. Liegt der P-Wert unterhalb des Signifikanzniveaus α wird von Signifikanz gesprochen.

Quadratsumme (SS) Die Summe aller quadrierten Abweichungen der Maßzahlen von ihrem Mittelwert wird als Quadratsumme bezeichnet. Sie bildet den Zähler in der Formel zur Berechnung der Varianz.

Signifikanz Die Signifikanz bedeutet, dass ein gefundener Unterschied nur mit geringer Wahrscheinlichkeit durch eine zufällige Abweichung zu erklären ist. In dieser Arbeit ist die zugrundeliegende Wahrscheinlichkeit eines falsch-positiven Resultats 0,05.

Varianz σ^2 Die Varianz beschreibt den durchschnittlichen quadratischen Abstand zum Mittelwert. Mathematisch ausgedrückt bezeichnet die Varianz der Quotient aus jeweils der Summe aller Werte minus Durchschnittswert sowie der Anzahl der Freiheitsgrade.

Literaturverzeichnis

- [Abt70] Clark C. Abt. „Serious Games. New York: Viking, 1970, 176 pp., \$5.95, L.C. 79-83234“. In: *American Behavioral Scientist* 14.1 (1970), S. 129–129. DOI: 10.1177/000276427001400113. URL: <https://doi.org/10.1177/000276427001400113>.
- [AL19] Accenture und Ponemon Institute LLC. „Ninth Annual Cost of Cybercrime Study“. In: (2019). URL: https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf.
- [ANM18] David Airehrour, Nisha Nair und Samaneh Madanian. „Social Engineering Attacks and Countermeasures in the New Zealand Banking System: Advancing a User-Reflective Mitigation Model“. In: *Information* 9 (Mai 2018), S. 110. DOI: 10.3390/info9050110.
- [BKM84] Benjamin Samuel Bloom, David R. Krathwohl und Bertram B. Masia. *Taxonomy of educational objectives - the classification of educational goals*. New York: Longman, 1984. ISBN: 978-0-582-28010-6.
- [BP16] Kristian Beckers und Sebastian Pape. „A serious game for eliciting social engineering security requirements“. In: *2016 IEEE 24th International Requirements Engineering Conference (RE)*. IEEE. 2016, S. 16–25.
- [BPF16] Kristian Beckers, Sebastian Pape und Veronika Fries. „HATCH: hack and trick capricious humans-a serious game on social engineering“. In: *Proceedings of the 30th International BCS Human Computer Interaction Conference: Companion Volume*. BCS Learning & Development Ltd. 2016, S. 34.

- [Bun10] Bunchball Inc. *Gamification 101: An Introduction to the Use of Game Dynamics to Influence Behavior*. <https://www.bunchball.com/gamification101>. Zugegriffen am: 16.02.2020. 2010.
- [Cai61] Roger Caillois. *Man, Play, and Games*. Thames & Hudson, 1961.
- [Cia13] Robert B. Cialdini. *Die Psychologie des Überzeugens*. Hogrefe AG, 2013. ISBN: 978-3456851501.
- [Cle18] Thomas Cleff. *Angewandte Induktive Statistik und Statistische Testverfahren - Eine computergestützte Einführung mit Excel, SPSS und Stata*. Berlin Heidelberg New York: Springer-Verlag, 2018. ISBN: 978-3-834-96973-6.
- [Coh13] Jacob Cohen. *Statistical Power Analysis for the Behavioral Sciences* -. New York: Routledge, 2013. ISBN: 113-4-742-703-.
- [CS16] Nabie Y. Conteh und Paul J. Schmick. „Cybersecurity:risks, vulnerabilities and countermeasures to prevent social engineering attacks“. In: *International Journal of Advanced Computer Research* 6 (2016). DOI: <http://dx.doi.org/10.19101/IJACR.2016.623006>.
- [Den+13] Tamara Denning u. a. „Control-Alt-Hack: the design and evaluation of a card game for computer security awareness and education“. In: *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. ACM. 2013, S. 915–928.
- [Det+11] Sebastian Deterding u. a. „From Game Design Elements to Gamefulness: Defining Gamification“. In: *Proceedings of the 15th International Academic MindTrek Conference: Envisioning Future Media Environments, MindTrek 2011* 11 (Sep. 2011), S. 9–15. DOI: 10.1145/2181037.2181040.
- [Dja+11] Damien Djaouti u. a. „Origins of Serious Games“. In: (2011), S. 25–43. DOI: 10.1007/978-1-4471-2161-9_3. URL: https://doi.org/10.1007/978-1-4471-2161-9_3.

- [Dör+15] Nicola Döring u. a. *Forschungsmethoden und Evaluation in den Sozial- und Humanwissenschaften*. 5. Aufl. Berlin Heidelberg New York: Springer-Verlag Berlin Heidelberg, 2015. ISBN: 978-3-642-41089-5. DOI: 10.1007/978-3-642-41089-5.
- [Fau+07] Franz Faul u. a. „G*Power 3: A flexible statistical power analysis program for the social, behavioral, and biomedical sciences“. In: *Behavior Research Methods* 39 (2 2007), S. 175–191.
- [FK05] Dirk Fox und Sven Kaun. „Security Awareness-Kampagnen“. In: (Mai 2005).
- [Foo+11] Cik Feresa Mohd Foozy u. a. „Generic Taxonomy of Social Engineering Attack“. In: *Malaysian Technical Universities International Conference on Engineering & Technology* (2011).
- [GT14] Bill Gardner und Valerie Thomas. *Building an Information Security Awareness Program: Defending Against Social Engineering and Technical Threats 1st Edition*. Aug. 2014, S. 1–194. ISBN: 978-0124199675.
- [Hal04] Thomas M. Haladyna. *Developing and Validating Multiple-choice Test Items*. 3. Auflage. London: Psychology Press, 2004. ISBN: 978-0-805-84661-4.
- [HL15] R. Heartfield und G. Loukas. „A Taxonomy of Attacks and a Survey of Defence Mechanisms for Semantic Social Engineering Attacks“. In: *ACM Computing Surveys* (2015). DOI: <http://dx.doi.org/10.1145/0000000.0000000>.
- [HLZ04] Robin Hunicke, Marc Leblanc und Robert Zubek. „MDA: A Formal Approach to Game Design and Game Research“. In: *AAAI Workshop - Technical Report 1* (Jan. 2004).
- [HSE13] Walter Hussy, Margrit Schreier und Gerald Echterhoff. *Forschungsmethoden in Psychologie und Sozialwissenschaften für Bachelor -*. Berlin Heidelberg New York: Springer-Verlag, 2013. ISBN: 978-3-642-34362-9.

- [Hub+14] Frank Huber u. a. *Grundlagen der Varianzanalyse - Konzeption - Durchführung - Auswertung*. 1. Aufl. Berlin Heidelberg New York: Springer-Verlag, 2014. ISBN: 978-3-658-05666-7.
- [HW10] C. Hadnagy und P. Wilson. *Social Engineering: The Art of Human Hacking*. Wiley, 2010. ISBN: 9781118029718.
- [IJ11] Koteswara Ivaturi und Lech Janczewski. „A Taxonomy for Social Engineering attacks“. In: *CONF-IRM 2011 Proceedings* (2011). URL: <http://aisel.aisnet.org/confirm2011/15>.
- [Juu05] Jesper Juul. *Half-Real: Video Games between Real Rules and Fictional Worlds*. The MIT Press, 2005. ISBN: 0262101106.
- [KK06] H.A. Kruger und W.D. Kearney. „A prototype for assessing information security awareness“. In: *Computers & Security* 25.4 (Juni 2006), S. 289–296. DOI: 10.1016/j.cose.2006.02.008. URL: <https://doi.org/10.1016/j.cose.2006.02.008>.
- [KKK18] A.J. Kim, R. Koster und S. Kim. *Game Thinking: Innovate Smarter & Drive Deep Engagement with Design Techniques from Hit Games*. gamethinking.io, 2018. ISBN: 9780999788547. URL: <https://books.google.de/books?id=7wXItwEACAAJ>.
- [KOS+09] Eric Klopfer, Scot Osterweil, Katie Salen u. a. „Moving learning games forward“. In: *Cambridge, MA: The Education Arcade* (2009).
- [KRW] Klemens Köhler, René Röpke und Martin R Wolf. „Through a Mirror Darkly—On the Obscurity of Teaching Goals in Game-Based Learning in IT Security“. In: ().
- [KSV12] Wolfgang Köhler, Gabriel Schachtel und Peter Voleske. *Biostatistik eine Einführung für Biologen und Agrarwissenschaftler*. Berlin, Heidelberg: Springer, 2012. ISBN: 9783642292712 3642292712 9783642292705 3642292704. URL: <http://nbn-resolving.de/urn:nbn:de:1111-201208141460>.

- [Lip09] Marcus Lipski. *Social Engineering - Der Mensch als Sicherheitsrisiko in der IT*. Diplomica Verlag, 2009. ISBN: 9783836675741.
- [Lon08] Johnny Long. *No Tech Hacking: A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing*. Elsevier, Inc., 2008. ISBN: 978-1-59749-215-7.
- [Mas51] Frank J Massey Jr. „The Kolmogorov-Smirnov test for goodness of fit“. In: *Journal of the American statistical Association* 46.253 (1951), S. 68–78.
- [MHZ16] Amir Matallaoui, Nicolai Hanner und Rüdiger Zarnekow. „Introduction to Gamification: Foundation and Underlying Theories“. In: (Okt. 2016), S. 3–18. DOI: 10.1007/978-3-319-45557-0_1. URL: https://doi.org/10.1007/978-3-319-45557-0_1.
- [MK11] Helfried Moosbrugger und Augustin Kelava. *Testtheorie und Fragebogenkonstruktion* -. 2. Aufl. Berlin Heidelberg New York: Springer-Verlag, 2011. ISBN: 978-3-642-20072-4.
- [Mül11] Volker Müller-Benedict. *Grundkurs Statistik in den Sozialwissenschaften - Eine leicht verständliche, anwendungsorientierte Einführung in das sozialwissenschaftlich notwendige statistische Wissen*. 5. Aufl. Berlin Heidelberg New York: Springer-Verlag, 2011. ISBN: 978-3-531-93225-5.
- [NF09] Michael Newbould und Stephen Furnell. „Playing Safe: A prototype game for raising awareness of social engineering“. In: *Australian Information Security Management Conference*. 2009, S. 4.
- [Ras+14] Björn Rasch u. a. *Quantitative Methoden 2: Einführung in die Statistik für Psychologen und Sozialwissenschaftler*. 4. Aufl. G*Power-Ergänzungen. Heidelberg: Springer-Verlag Berlin Heidelberg, 2014. ISBN: 978-3-662-43548-9.
- [RM05] Henry L. Roediger und Elizabeth J. Marsh. „The Positive and Negative Consequences of Multiple-Choice Testing.“ In: *Journal of Experimental Psychology: Learning, Memory, and Cognition* 31.5 (2005), S. 1155–1159. DOI: 10.1037/0278-7393.31.5.1155. URL: <https://doi.org/10.1037/0278-7393.31.5.1155>.

- [RW06] Ute Ritterfeld und René Weber. „Video games for entertainment and education“. In: *Playing video games: Motives, responses, and consequences* (2006), S. 399–413.
- [Saw07] Ben Sawyer. „Serious Games: Broadening Games Impact Beyond Entertainment“. In: *Comput. Graph. Forum* 26 (Sep. 2007). DOI: 10.1111/j.1467-8659.2007.01044.x.
- [Sch] Margit Scholl. „Analog Games for Information Security (Awareness) in the Digital World“. In: ().
- [Sch+17] Margit Scholl u. a. *Das Projekt SecAware4job: Auf spielerischem Weg zu erhöhtem Informationssicherheitsbewusstsein für den Berufseinstieg*. 2017. DOI: 10.15771/0949-8214_2017_3. URL: <https://opus4.kobv.de/opus4-th-wildau/frontdoor/index/index/docId/938>.
- [Sch19] Margit Scholl. „Sensitizing students to information security and privacy awareness with analogue gamification“. en. In: (2019). DOI: 10.15771/0949-8214_2019_3. URL: <https://opus4.kobv.de/opus4-th-wildau/1078>.
- [SK19] Fatima Salahdine und Naima Kaabouch. „Social Engineering Attacks: A Survey“. In: *Future Internet* 11 (Apr. 2019). DOI: 10.3390/fi11040089.
- [Staa] Statista Infografiken. *Infografik: Die 10 erfolgreichsten Kickstarter-Projekte*. <https://de.statista.com/infografik/14978/top-kickstarter-projekte-nach-unterstuetzerzahl/>. Zugriffen am: 01.11.2019.
- [Stab] Statista Infografiken. *Infografik: Die beliebtesten Gesellschaftsspiele der Deutschen*. <https://de.statista.com/infografik/19742/umfrage-welche-gesellschaftsspiele-die-deutschen-zuhause-haben/>. Zugriffen am: 01.11.2019.
- [Ste16] J. Stenros. „The Game Definition Game: A Review“. In: *Games and Culture* (Juni 2016). DOI: 10.1177/1555412016655679. URL: <https://doi.org/10.1177/1555412016655679>.

- [SZ03] Katie Salen und Eric Zimmerman. *Rules of Play: Game Design Fundamentals*. The MIT Press, 2003. ISBN: 0262240459.
- [Tec] Technische Universität Darmstadt. *EK - Antragstellung - Technische Universität Darmstadt*. <https://www.intern.tu-darmstadt.de/gremien/ethikkommission/antragstellung/antragstellung.de.jsp>. Zugegriffen am: 06.02.2020.
- [Uni] Universität Siegen. *Quantile für den zweiseitigen Kolmogorov-Smirnov-Anpassungstest*. https://www.wiwi.uni-siegen.de/stat/runde/material/tabellen_quantile/tabellen_quantile/ks-tabelle.pdf. Zugegriffen am: 09.03.2020.
- [WH03] Mark Wilson und Joan Hash. *SP 800-50. Building an Information Technology Security Awareness and Training Program*. 2003.

Anhang

Auf der beigefügten CD befinden sich folgende Inhalte:

- diese Arbeit im $\text{\LaTeX}$ - und PDF-Format
- sämtliche Literaturquellen im PDF-Format
- sämtliche Internetquellen im HTML-Format
- das Spielbrett im PNG-Format
- Bildquellen für die Spielkarten
- die erhobenen Messwerte in quantifizierter, anonymisierter Form im XLSX-Format
- die zwei beschriebenen VBA-Skripte zur Auswertung der Messdaten

Anhang A

Fragebogen

Abschnitt 1 - SANIAG Fragebogen

Die Richtlinien der Deutschen Forschungsgemeinschaft (DFG) sehen vor, dass Sie sich an empirischen Studien explizit und nachvollziehbar einverstanden erklären, dass Sie freiwillig an unserer Forschung teilnehmen. Aus diesem Grund möchten wir Sie bitten, die nachfolgenden Erläuterungen zum Inhalt der Studie zu lesen und der untenstehenden Einverständniserklärung zuzustimmen, sofern Sie damit einverstanden sind.

Der Fragebogen umfasst 4 Abschnitte:

- SANIAG Fragebogen (dieser einleitende Text)
- Persönliches
- Frageteil I - Wissen (11 Fragen)
- Frageteil II - Szenarien (10 Fragen)

Durch das Ausfüllen dieses Fragebogens unterstützen Sie eine Masterarbeit an der Hochschule Darmstadt, in welcher Fragestellungen zu Social Engineering Awareness nachgegangen werden. Bitte füllen Sie den Fragebogen nur nach Absprache mit einem der Studienleiter aus.

Bei Rückfragen dürfen Sie uns gerne kontaktieren unter:

saed.alavi@stud.h-da.de

niklas.bessler@stud.h-da.de

Beantworten Sie alle Fragen bitte nach Ihrem besten Wissen. Sehen Sie davon ab, Antworten im Internet zu recherchieren. Bei den meisten Fragen handelt es sich um sogenanntes Single Choice oder Multiple Choice. D.h. Ihnen werden verschiedene Antwortmöglichkeiten vorgegeben.

Beachten Sie bitte, dass bei Fragen mit einer Checkbox (Auswahlkasten) mehrere Antworten richtig sein können. Ein Radiobutton (Kreis) hingegen bedeutet, dass Sie sich für genau eine Antwort entscheiden müssen. Der Fragebogen wurde absichtlich so konzipiert, dass Sie womöglich nicht alle Fragen beantworten können. In diesem Fall können Sie auch die Antwortmöglichkeit "Weiß nicht" auswählen.

Die Bearbeitung des Fragebogens sollte nicht mehr als 15 Minuten beanspruchen. Nach Abschluss der Studie wird ein Amazon Gutschein im Wert von 30€ unter den Teilnehmenden der Studie verlost. Durch die Teilnahme der Studie werden Sie keinem Risiko ausgesetzt, das über die Risiken des alltäglichen Lebens hinausgeht.

Wir, Niklas Bessler und Saed Alavi, bedanken uns herzlich für Ihre Unterstützung und Zeit!

Erklärung zum Datenschutz

Auch bei einer Umfrage haben Sie gemäß Datenschutz gegenüber dem Informations-träger das Recht auf Auskunft sowie Löschung Ihrer personenbezogenen Daten. Sie können diese Einwilligungserklärung jederzeit widerrufen. Hierzu können Sie den Fragebogen erneut unter Angabe Ihres Pseudonyms ausfüllen und Ihre Löschaufforderung mittels des Feedback-Felds kundtun oder uns eine E-Mail unter Nennung Ihres Pseudonyms senden. Nach erfolgtem Widerruf werden Ihre Daten gelöscht.

Vertraulichkeit

Alle im Rahmen dieser Studie erhobenen Daten sind selbstverständlich vertraulich und werden nur in anonymisierter Form genutzt. Demographische Angaben wie Alter oder Geschlecht lassen keinen eindeutigen Schluss auf Ihre Person zu. Zu keinem Zeitpunkt im Rahmen der jeweiligen Untersuchung werden wir Sie bitten, Ihren Namen oder andere eindeutige Informationen zu nennen.

Aufbewahrung

Die mit dieser Studie erhobenen Daten werden auf Servern von Google gespeichert und nach abgehaltenem Kolloquium der Studienleiter gelöscht. Die Teilnahme an dieser Umfrage ist ohne die Nennung Ihres Namens möglich. Ihre Daten werden pseudonymisiert ausgewertet. Eine Registrierung ist für die Teilnahme nicht erforderlich.

Freiwilligkeit & Rechte der Versuchspersonen

Ihre Teilnahme an dieser Untersuchung ist freiwillig. Es steht Ihnen zu jedem Zeitpunkt dieser Studie frei, Ihre Teilnahme abzubrechen und damit diese Einwilligung zurückziehen (Widerruf), ohne dass Ihnen daraus Nachteile entstehen. Wenn Sie die Teilnahme abbrechen, werden keine Daten von Ihnen gespeichert und alle bisher vorliegenden Daten zu Ihrer Person vernichtet. Sie haben das Recht, Auskunft über die Sie betreffenden personenbezogenen Daten zu erhalten sowie ggf. deren Berichtigung oder Löschung zu verlangen. In Streitfällen haben Sie das Recht, sich beim Hessischen Datenschutzbeauftragten zu beschweren.

Einverständnis

Ich habe die Erläuterungen zur Studie gelesen und bin damit einverstanden, an der genannten Studie teilzunehmen. Ich erkläre mich einverstanden, dass die im Rahmen der Studie erhobenen Daten zu wissenschaftlichen Zwecken ausgewertet und in pseudonymisierter Form gespeichert werden. Ich bin mir darüber bewusst, dass meine Teilnahme freiwillig erfolgt und ich den Versuch jederzeit und ohne die Angabe von Gründen abbrechen kann.

● Ich bin einverstanden und möchte an der Umfrage teilnehmen.

Abschnitt 2 - Persönliches

Dieser Abschnitt des Fragebogens dient dazu, Ihre Antworten pseudonymisiert auswerten zu können.

An welchem Tag im Monat sind Sie geboren? (z.B. Geburtsdatum 30.12.1990 = 30)

...

Wie lauten die ersten zwei Buchstaben des Straßennamens, in der Sie wohnen? (z.B. Mustermannstraße = MU)

...

Wie lauten die ersten zwei Buchstaben des Vornamens Ihrer Mutter? (z.B. Lisa = LI)

...

Karriere

- ☐ Student der Informatik
- ☐ Student nicht Informatik
- ☐ Arbeitnehmer in Vollzeit
- ☐ Sonstiges: ...

Ich stimme dem zu:

Der Begriff Social Engineering ist mir bekannt.

☐ gar nicht ☐ teilweise ☐ überwiegend ☐ vollkommen

Ich kenne mich sehr gut mit Social Engineering aus.

☐ gar nicht ☐ teilweise ☐ überwiegend ☐ vollkommen

Social Engineering stellt ein großes Risiko dar.

☐ gar nicht ☐ teilweise ☐ überwiegend ☐ vollkommen

Ich erhalte regelmäßig Schulungen zu dem Thema Social Engineering.

☐ gar nicht ☐ teilweise ☐ überwiegend ☐ vollkommen

Der Begriff Social Engineering ist mir bekannt

☐ gar nicht ☐ teilweise ☐ überwiegend ☐ vollkommen

Abschnitt 3 - Frageteil I Wissen

Im folgenden Frageteil werden Ihnen einige Fragen zum Themenfeld Social Engineering gestellt. Bitte sehen Sie davon ab, Fragen im Internet zu recherchieren. Die Auswahl Ihrer Antwort sollte möglichst spontan erfolgen.

Die Fragestellungen geben Ihnen verschiedene Antwortmöglichkeiten vor. Hierbei bedeutet eine Checkbox (Kästchen), dass mehrere Antworten richtig sein können. Sie müssen jedoch keine Antwort auswählen. Ein Radiobutton (Kreis) hingegen bedeutet, dass die Auswahl genau einer Antwort erforderlich ist. Insgesamt umfasst dieser Frageteil 11 Fragen.

Was wird unter dem Begriff Social Engineering verstanden?

☒ Zwischenmenschliche Beeinflussungen mit dem Ziel, bestimmte Verhaltensweisen hervorzurufen.

☐ Software, die der menschlichen Kommunikation und der Zusammenarbeit dient.

☐ Das Vernetzen von Nutzern im Internet sowie der Austausch medialer Inhalte.

☐ Soziales Handeln, das meist auf den Prinzipien der Ehrenamtlichkeit und Freiwilligkeit beruht.

Was besagt die Clean-Desk Richtlinie?

☐ Keine Getränke und Speisen am Arbeitsplatz.

☐ Den Einsatz von Cleaner-Software auf Desktop-PCs.

☐ Keine vertraulichen Daten auf dem Desktop des Computers zu speichern.

☒ Keine vertraulichen Daten auf dem Schreibtisch liegen zu lassen.

Intelligenz ist ein wirksamer Schutz gegen Social Engineering Angriffe. Ist die These korrekt?

☐ Richtig

☒ Falsch

☐ Weiß nicht

Social Engineering Angriffe erfordern einen Computer. Ist die These korrekt?

☐ Richtig

☒ Falsch

☐ Weiß nicht

Eine Datei lässt sich auch dann wiederherstellen, wenn sie aus dem Papierkorb entfernt wurde. Ist diese These korrekt?

☒ Richtig

☐ Falsch

☐ Weiß nicht

Das bloße Öffnen von E-Mails ist unbedenklich. Erst das Ausführen von Dateien ist potentiell gefährlich. Ist diese These korrekt?

☐ Richtig

☒ Falsch

☐ Weiß nicht

Social Engineering Angriffe beruhen auf psychologischen Manipulationen. Welche Prinzipien werden sich dabei zunutze gemacht?

☐ Remanenz

☒ Reziprozität

☒ Autorität

☒ Sympathie

Welche der genannten Optionen sind Maßnahmen gegen E-Mail Phishing?

☒ E-Mail Filter (Spamfilter)

☐ VPN (Virtual Private Network)

☒ Digitale Signaturen

☐ Festplattenverschlüsselung

Laut der Richtlinie NIST SP 800-63B-3 aus dem Jahr 2017 handelt es sich um ein gutes Passwort bei?

☐ passwort

☐ abcd1234

☒ sauerstofffl4sche

☐ K1n.d3r

Welche der genannten Optionen sind Quellen für Open Source Intelligence (OSINT)?

☒ Google Earth

☒ öffentliche Unternehmenswebsite

☐ Intranet

☐ Private Gruppenkommunikation (Chatgruppen)

☒ Tageszeitungen

Laut den Digital Identity Guidelines "NIST SP 800-63B-3" des National Institute of Standards and Technology sollen Passwörter folgende Merkmale erfüllen:

☒ Das Passwort muss aus mindestens 8 Zeichen bestehen.

☐ Es ist erforderlich, das Passwort periodisch zu ändern.

☐ Das Passwort muss Sonderzeichen sowie Großbuchstaben enthalten.

☒ Das Passwort darf keine Muster enthalten, etwa "abcd1234".

Abschnitt 4 - Frageteil II Szenarien

Im Folgenden werden Ihnen unterschiedliche Szenarien beschrieben. Dabei nehmen Sie die Rolle eines gewöhnlichen Mitarbeiters in einem Unternehmen ein. Mit Ihrem Verhalten sollen Sie mögliche Gefährdungen für sich und Ihr Unternehmen vermeiden. Entsprechend sollen Sie auswählen, welches Verhalten zutreffend ist.

Die Szenarien geben Ihnen verschiedene Antwortmöglichkeiten vor, wie Sie sich verhalten können. Hierbei ist stets genau eine der ersten vier Antwortmöglichkeiten richtig. Wenn Sie sich unsicher sind, können Sie auch die Antwort "Weiß nicht." auswählen. Insgesamt umfasst dieser Frageteil 10 Fragen.

Sie haben den Fragebogen nach diesem Abschnitt abgeschlossen. Sie erhalten eine Datei "rechnung.pdf.exe" als Anhang einer E-Mail.

- ☐ Wenn die Datei das Symbol des PDF Readers hat und zugleich der Dateiname "rechnung.pdf" angezeigt wird, kann ich sie bedenkenlos öffnen.
- ☐ Ich kann die Datei nur dann bedenkenlos öffnen, wenn die E-Mail von der Adresse eines definitiv vertrauenswürdigen Kollegen stammt (Feld "Absender" im E-Mail Programm).
- ☐ Ich habe die Datei bereits geöffnet und auf dem Monitor erscheint erwartungsgemäß eine eingescannte Rechnung. In dem Fall ist alles in Ordnung.
- ☒ Keine der anderen Antworten trifft zu.
- ☐ Weiß nicht.

Sie erhalten streng geheime Anweisungen über einen Geldtransfer von Ihrem Chef via E-Mail.

- ☐ Ich hinterfrage die Anweisung nur, sofern es sich nur um einen größeren Betrag handelt.
- ☐ Ich habe die Anweisung schriftlich und bin somit abgesichert. Also befolge ich die Anweisung.
- ☒ Auch bei Anweisungen des Vorgesetzten sind die Prozesse zu befolgen, weshalb ich die Anweisung nicht ausführe.
- ☐ Keine der anderen Antworten trifft zu.
- ☐ Weiß nicht.

Ein gut gelaunter Kollege spricht im Restaurant mit Ihnen über Firmengeheimnisse.

- ☐ Ich möchte dem Kollegen nicht die gute Laune nehmen und lass ihn aussprechen.
- ☒ Ich weise den Kollegen darauf hin, das Gespräch an einen anderen Ort fortzusetzen.
- ☐ Wenn ausschließlich Personal des Restaurants zuhört ist das in Ordnung.
- ☐ Keine der anderen Antworten trifft zu.
- ☐ Weiß nicht.

Sie erhalten in der Cafeteria einen USB-Stick als Werbegeschenk.

- ☐ Ich stecke den Datenträger ein um ihn vorsichtshalber mit dem Antivirenprogramm zu scannen.

- ☐ Ich stecke den Datenträger ein und öffne lediglich harmlose Word-Dokumente.
- ☒ Ich bespreche die Situation mit dem IT-Sicherheitsbeauftragten.
- ☐ Keine der anderen Antworten trifft zu.
- ☐ Weiß nicht.

Eine Person, die sich als Polizist meldet, bittet Sie am Telefon Firmengeheimnisse herauszugeben.

- ☐ Ich gebe die Daten raus, da es sich bei Polizisten um eine Autoritätsperson handelt.
- ☐ Ich gebe die Daten raus, da der Polizist mir eine Strafe androht.
- ☒ Ich gebe keine Firmengeheimnisse am Telefon preis.
- ☐ Keine der anderen Antworten trifft zu.
- ☐ Weiß nicht.

Ihre Passwörter bewahren Sie aus Sicherheitsgründen an folgendem Ort auf.

- ☐ Ich hefte das Passwort mit einem Klebezettel an den Monitor.
- ☐ Ich verwahre das Passwort auf einem Zettel in einer verschlossenen Schublade.
- ☐ Ich kommuniziere das Passwort mündlich an einen vertrauenswürdigen Kollegen.
- ☒ Keine der anderen Antworten trifft zu.
- ☐ Weiß nicht.

Vor der Eingangstüre zu den Büroräumen stellt sich Herr Müller als neuer Kollege vor. Da dieser einen großen Kuchen trägt, bittet er beim Öffnen der Türe zu helfen.

- ☐ Ich öffne Herrn Müller mit meiner Zugangskarte die Türe, wenn er einen Mitarbeiterausweis bei sich trägt.
- ☐ Ich öffne Herrn Müller die Türe, da auf der letzten Mitarbeiterversammlung verkündet wurde, dass diesen Monat Herr Müller neu anfängt.
- ☒ Ich nehme Herrn Müller den Kuchen ab, sodass er seinen Mitarbeiterausweis an das Lesegerät der Türe halten kann.
- ☐ Keine der anderen Antworten trifft zu.
- ☐ Weiß nicht.

Sie werden in einer E-Mail glaubhaft erpresst Firmengeheimnisse zu verraten, da der Erpresser sonst Nacktbilder von Ihnen veröffentlicht. Sie dürfen mit niemandem darüber sprechen und müssen innerhalb von 24 Stunden die geforderten Informationen preisgeben.

- ☐ Ich mache mein Verhalten abhängig davon, wie wichtig die geforderten Firmengeheimnisse sind.
- ☐ Ich gebe die vertraulichen Informationen preis und gehe danach zur örtlichen Polizei.
- ☐ Ich behalte einen kühlen Kopf und lösche die E-Mail einfach. Den Vorfall melde ich nicht in meinem Unternehmen.
- ☒ Keine der anderen Antworten trifft zu.
- ☐ Weiß nicht.

Sie nehmen für die Anreise zu einem Kunden den Zug als Verkehrsmittel. Die Zeit der Zugfahrt können Sie als Arbeitszeit verbuchen. ☐ Ich rufe den Kunden vor meiner Ankunft an, um noch dringende vertrauliche Daten telefonisch zu besprechen. ☐ Ein anderer Fahrgast möchte seine Reiseanbindung prüfen. Ich leihe ihm hierzu kurz das Firmenlaptop. ☒ Bei mobilem Arbeiten bringe ich einen Blickschutzfilter am Laptop an. Ggf. setze ich mich so, dass der Bildschirm nicht leicht eingesehen werden kann. ☐ Keine der anderen Antworten trifft zu. ☐ Weiß nicht.
Der technische Support benötigt Ihr Benutzerpasswort um ein Laptop-Problem per Fernwartung zu lösen. Tatsächlich erwarten Sie die Hilfe des technischen Supports. Sie kennen den Kollegen nicht persönlich. ☒ Ich bestehe darauf, dass mein Laptop-Problem anders gelöst wird. Der Support soll mein Kennwort für die Hilfestellung abändern. ☐ Ich bin misstrauisch und frage sicherheitshalber, in welchen Büroräumen der Supportmitarbeiter sitzt. Nur wenn der Support richtig antwortet, gebe ich mein Passwort preis. ☐ Ich befrage einen Kollegen im Büro. Nur wenn dieser den Vorgang für üblich hält, nenne ich mein Passwort am Telefon. ☐ Weiß nicht.
Vielen Dank! Sie können den Fragebogen nun absenden!
Feedback (optional) ...

Tabelle A.1: Fragebogen mit korrekten Antworten

Die Repräsentation der Symbole ist in der folgenden Tabelle erläutert.

falsche Single-Choice Antwort	☐
korrekte Single-Choice Antwort	☒
eine falsche Multiple-Choice Antwort	☐
eine korrekte Multiple-Choice Antwort	☒
Freitextfeld	...

Anhang B

VBA-Skript zur Randomisierung

```
1 Sub Randomer()  
2 Dim i As Long, startRow As Long, endRow As Long  
3 Dim ws As Worksheet  
4 Application.ScreenUpdating = False  
5 Application.Calculation = xlCalculationManual  
6 Set ws = ActiveSheet  
7 startRow = 2  
8 endRow = WorksheetFunction.Max( _  
9 ws.Cells(ws.Rows.Count, 1).End(xlUp).Row, _  
10 ws.Cells(ws.Rows.Count, 2).End(xlUp).Row)  
11  
12 For i = startRow To endRow  
13 Randomize  
14 ws.Cells(i, 3).Value = WorksheetFunction.RandBetween(1, 1000)  
15 Next i  
16  
17 ws.Sort.SortFields.Clear  
18 ws.Sort.SortFields.Add Key:=Range("C" & startRow & ":C" & endRow), SortOn:=xlSortOnValues,  
    Order:=xlAscending, DataOption:=xlSortNormal  
19  
20 With ws.Sort  
21 .SetRange Range("A" & startRow & ":C" & endRow)  
22 .Header = xlNo  
23 .MatchCase = False
```

```

24 .Orientation = xlTopToBottom
25 .SortMethod = xlPinYin
26 .Apply
27 End With
28
29 ws.Range(ws.Cells(startRow, 3), ws.Cells(endRow, 3)).ClearContents
30 Call group(ws)
31 Application.Calculation = xlCalculationAutomatic
32 Application.ScreenUpdating = True
33
34 End Sub
35
36 Sub group(ws As Worksheet)
37 startRow = 2
38 endRow = WorksheetFunction.Max( _
39 ws.Cells(ws.Rows.Count, 1).End(xlUp).Row, _
40 ws.Cells(ws.Rows.Count, 2).End(xlUp).Row)
41
42 For i = startRow To endRow
43 Randomize
44 If (i Mod 2) = 0 Then
45 ws.Cells(i, 2).Value = "Experimentalgruppe"
46 Else
47 ws.Cells(i, 2).Value = "Kontrollgruppe"
48 End If
49 Next i
50
51 End Sub

```

Quelltext B.1: VBA-Skript zur Randomisierung

Anhang C

VBA-Skript zur Quantifizierung der Fragebogen

```
1 Sub importData()  
2 Call applicationPreparation  
3 Dim sourceWB As Workbook  
4 Dim sourceWS As Worksheet  
5 Dim targetWS As Worksheet  
6 Dim caWS As Worksheet  
7 Dim lRowCA As Integer  
8 Dim columnName As String  
9  
10  
11 ' Set targetWS = ActiveWorkbook.Sheets.Add(After:=ActiveWorkbook.Sheets(  
12 ' ActiveWorkbook.Sheets.Count))  
13 Set targetWS = ActiveWorkbook.Worksheets("Answers")  
14 targetWS.UsedRange.Clear  
15 Set caWS = ActiveWorkbook.Worksheets("CorrectAnswers")  
16 ' targetWS.Name = "Antworten" & (ActiveWorkbook.Sheets.Count - 2)  
17 Set sourceWB = FileOpenDialogBox  
18 Set sourceWS = sourceWB.Worksheets(1)  
19  
20  
21 lRowCA = caWS.Cells(caWS.Rows.Count, "B").End(xlUp).Row
```



```

22
23 'Loop throw all cols and bring them sorted into target file
24 'Note: String swith more than 255 chars have been shorten to 255 manually
25 Dim i As Integer
26 For i = 3 To lRowCA
27     columnName = caWS.Cells(i, 3)
28     Call importAnswerRows(columnName, sourceWS, targetWS, i)
29 Next i
30 sourceWB.Close (0)
31
32 Call correctDatesAndAnonymize(targetWS)
33 Call applicationEnding
34 End Sub
35
36
37 Sub importAnswerRows(columnName As String, sourceWS As Worksheet, targetWS As
    Worksheet, rowNr As Integer)
38 Dim inCol As Integer
39 inCol = sourceWS.Cells(1, 1).EntireRow.Find(What:=columnName, LookIn:=xlValues, LookAt
    :=xlPart, SearchOrder:=xlByColumns, SearchDirection:=xlNext, MatchCase:=False).
    Column
40 sourceWS.Columns(inCol).Copy Destination:=targetWS.Columns(rowNr - 2)
41
42
43 End Sub
44 Sub correctDatesAndAnonymize(ws As Worksheet)
45 ws.Range("A:A").Insert
46 ws.Cells(1, 1) = "Proband"
47 lRow = ws.Cells(ws.Rows.Count, 2).End(xlUp).Row
48
49 Dim i As Integer
50 For i = 2 To lRow
51 If IsEmpty(ws.Cells(i, 2)) Then
52 ws.Cells(i, 2) = 0
53 Else
54 ws.Cells(i, 2) = Left(ws.Cells(i, 2), 2)

```

```

55 If Not IsNumeric(ws.Cells(i, 2)) Then
56 ws.Cells(i, 2) = 0
57 End If
58 End If
59 ws.Cells(i, 1) = SHA256(UCCase(ws.Cells(i, 2) & ws.Cells(i, 3) & ws.Cells(i, 4)))
60 ws.Cells(i, 2) = ws.Cells(i, 2) & ws.Cells(i, 3) & ws.Cells(i, 4)
61 Next i
62 ws.Columns("B:D").Delete
63 End Sub
64
65
66
67
68 Function FileOpenDialogBox() As Workbook
69
70 'Display a Dialog Box that allows to select a single file.
71 'The path for the file picked will be stored in fullpath variable
72 With Application.FileDialog(msoFileDialogFilePicker)
73 'Makes sure the user can select only one file
74 .AllowMultiSelect = False
75 'Filter to just the following types of files to narrow down selection options
76 .Filters.Add "Excel Files", "*.xlsx; *.xlsm; *.xls; *.xlsb", 1
77 'Show the dialog box
78 .Show
79
80 'Store in fullpath variable
81 fullpath = .SelectedItems.Item(1)
82 End With
83
84 'It's a good idea to still check if the file type selected is accurate.
85 'Quit the procedure if the user didn't select the type of file we need.
86 If InStr(fullpath, ".xls") = 0 Then
87
88 Exit Function
89 End If
90

```

```

91 'Open the file selected by the user
92 Set FileOpenDialogBox = Workbooks.Open(fullpath)
93
94 End Function
95
96 Sub calculateResults()
97 Call applicationPreparation
98 Dim wb As Workbook
99 Dim ws As Worksheet
100 Dim caWS As Worksheet
101 Dim resultWS As Worksheet
102 Set wb = ThisWorkbook
103 Set ws = wb.Worksheets("Answers")
104 Set caWS = wb.Worksheets("CorrectAnswers")
105 Set resultWS = wb.Worksheets("Results")
106 Dim i As Integer
107 Dim j As Integer
108 Dim NReasySelection2 As Integer
109 Dim NFeasySelection2 As Integer
110 Dim easySelectionResult2 As Double
111 Dim NReasySelection4 As Integer
112 Dim easySelectionResult4 As Double
113 Dim multiSelection As Integer
114 Dim lRow As Integer
115 Dim lCol As Integer
116 resultWS.UsedRange.Clear
117 'Ergebnisse Einfachauswahl 2-----
118
119 lRow = ws.Cells(ws.Rows.Count, 1).End(xlUp).Row
120 lCol = ws.UsedRange.Columns(ws.UsedRange.Columns.Count).Column
121 NReasySelection2 = 0
122 For i = 2 To lRow
123 NFeasySelection2 = 0
124 NReasySelection2 = 0
125 For j = 7 To 10
126

```

```

127 If ws.Cells(i, j) = caWS.Cells(j + 4, 4) Then
128 NReasySelection2 = NReasySelection2 + 1
129 End If
130 If ws.Cells(i, j) <> caWS.Cells(j + 4, 4) And ws.Cells(i, j) <> "Weiß nicht" Then
131 NFeasySelection2 = NFeasySelection2 + 1
132 End If
133 Next j
134 ' easySelectionResult2 = easySelection2 - ((4 - easySelection2) / (2 - 1))
135 easySelectionResult2 = NReasySelection2 - (NFeasySelection2) / (2 - 1)
136
137 ' -----
138 'Ergebnisse Mehrfachauswahl
139
140 -----
139 multiSelection = 0
140 For j = 11 To 17
141 If ws.Cells(i, j) = caWS.Cells(j + 4, 4) Then
142 multiSelection = multiSelection + (caWS.Cells(j + 4, 5))
143 Else
144 For k = 6 To 13
145 If InStr(ws.Cells(i, j), caWS.Cells(j + 4, k)) > 0 Then
146 multiSelection = multiSelection + (caWS.Cells(j + 4, k + 1))
147 End If
148 k = k + 1
149 Next k
150 End If
151
152 Next j
153 ' -----
154 'Ergebnisse Einfachauswahl 4
155 NReasySelection4 = 0
156 For j = 18 To 27
157 If ws.Cells(i, j) = caWS.Cells(j + 4, 4) Then
158 NReasySelection4 = NReasySelection4 + 1
159 End If
160 If ws.Cells(i, j) <> caWS.Cells(j + 4, 4) And ws.Cells(i, j) <> "Weiß nicht" Then
161 NFeasySelection4 = NFeasySelection4 + 1

```

```

162 End If
163 Next j
164
165 '     easySelectionResult4 = easySelection4 - ((10 - easySelection4) / (4 - 1))
166 easySelectionResult4 = NReasySelection4 - (NF4easySelection4 / (4 - 1))
167 ws.Cells(1, lCol + 1) = "Einfachauswahl 2 Ergebnis"
168 ws.Cells(1, lCol + 2) = "Mehrfachauswahl Ergebnis"
169 ws.Cells(1, lCol + 3) = "Einfachauswahl 4 Ergebnis"
170 ws.Cells(1, lCol + 4) = "Gesamtwert"
171 ws.Cells(i, lCol + 1) = easySelectionResult2
172 ws.Cells(i, lCol + 2) = multiSelection
173 ws.Cells(i, lCol + 3) = easySelectionResult4
174 ws.Cells(i, lCol + 4) = easySelectionResult2 + multiSelection + easySelectionResult4
175
176 Next i
177 ' Push results to result worksheet
178 ws.Columns(1).Copy Destination:=resultWS.Columns(1)
179 ws.Columns(lCol + 1).Copy Destination:=resultWS.Columns(2)
180 ws.Columns(lCol + 2).Copy Destination:=resultWS.Columns(3)
181 ws.Columns(lCol + 3).Copy Destination:=resultWS.Columns(4)
182 ws.Columns(lCol + 4).Copy Destination:=resultWS.Columns(5)
183
184 Call applicationEnding
185 End Sub
186
187 Public Function SHA256(sIn As String, Optional bB64 As Boolean = 0) As String
188
189
190 Dim oT As Object, oSHA256 As Object
191 Dim TextToHash() As Byte, bytes() As Byte
192
193 Set oT = CreateObject("System.Text.UTF8Encoding")
194 Set oSHA256 = CreateObject("System.Security.Cryptography.SHA256Managed")
195
196 TextToHash = oT.Getbytes_4(sIn)
197 bytes = oSHA256.ComputeHash_2((TextToHash))

```

```

198
199 If bB64 = True Then
200   SHA256 = ConvToBase64String(bytes)
201 Else
202   SHA256 = ConvToHexString(bytes)
203 End If
204
205 Set oT = Nothing
206 Set oSHA256 = Nothing
207
208 End Function
209
210 Sub applicationPreparation()
211   Application.ScreenUpdating = False
212   Application.DisplayStatusBar = False
213   Application.Calculation = xlCalculationManual
214   Application.EnableEvents = False
215 End Sub
216 Sub applicationEnding()
217   Application.ScreenUpdating = True
218   Application.DisplayStatusBar = True
219   Application.Calculation = xlCalculationAutomatic
220   Application.EnableEvents = True
221
222 End Sub

```

Quelltext C.1: VBA-Skript zur Quantifizierung der Fragebogen

Anhang D

Messwerte

Experimental		Kontrolle	
Prä	Post	Prä	Post
18	19	13	15
18	23	15	12
12	18	19	18
20	23	14	12
6	14	21	18
14	19	13	19
20	22	18	20
13	23	18	12
17	22	18	16
15	18	15	18
19	21	7	12
12	16	16	16
18	26	20	21
12	21	24	24
9	17	12	15
3	14	19	22
20	22	9	9
12	17	10	16

Tabelle D.1: Empirisch erhobene und quantifizierte Messwerte