Entwicklung und Wirksamkeit einer präventiven Veranstaltung im Kontext von Cybercrime

–

„adressatInnenorientierte Vermittlung von Strategien gegen Cybercrime“ für Erwachsene

Eine quantitativ-empirische Untersuchung zur Wirksamkeit eines präventiven Projekts in Mecklenburg-Vorpommern

Dissertation
zur Erlangung des akademischen Grades Dr. phil.
an der Universität Vechta,
Fakultät Erziehungswissenschaften

vorgelegt von:

Heiko Franke
Hornshagen 8
17348 Woldegk
heiko.franke@mail.uni-vechta.de

Gutachterinnen:

Prof. Dr. Marie-Christine Vierbuchen
Prof. Dr. Margit Stein

Woldegk, im Februar 2021

Inhaltsverzeichnis

Tabellenverzeichnis **5**
Abbildungsverzeichnis **8**
Vorwort **10**

1 Einleitung **11**
1.1 Problem- und Fragestellung 11
1.2 Grundlegende Vorgehensweise im Forschungsprozess und forschungsleitende Annahmen 13
1.3 Aufbau der Arbeit 14

2 Theoretische Fundierung **16**
2.1 Cybercrime 16
2.1.1 Definitionen und Eingrenzung 16
2.1.2 Ist-Situation 19
2.1.3 Staatliche Maßnahmen gegen Cyberangriffe 20
2.1.4 Problem der Identifizierung von Cyberangriffen und deren Konsequenz 22
2.1.5 Cyberkriminelle: eine Kategorisierung 24
2.2 Arten von Cyberangriffen 32
2.2.1 Angriffsziel: Der Mensch als Informationsträger (Social Engineering) 33
2.2.2 Angriffsziel: Infrastruktur 46
2.2.3 Begünstigung von Cybercrime durch Komplexität 59
2.3 Erklärung von sicherheitskonformem Verhalten im Kontext von Cybercrime 62
2.3.1 Das Elaboration-Likelihood-Modell (ELM) 63
2.3.2 Das heuristisch-systematische Modell (HSM) 66
2.3.3 Die Theorie der Schutzmotivation (PMT) 67
2.3.4 Die Theorie der Selbstwirksamkeitserwartung (SET) 69
2.3.5 Das Konstrukt der Kontrollüberzeugung (LoC) 70
2.3.6 Die Einstellungstheorie (FAT) 71
2.3.7 Die Theorie des überlegten Handelns (TRA) 72
2.3.8 Die Theorie des geplanten Verhaltens (TPB) 73
2.3.9 Das transtheoretische Modell 75
2.3.10 Die empirische Unterfütterung der dargelegten Erklärungsmodelle im Kontext von Cybercrime 76
2.4 Präventive Veranstaltungen 80
2.4.1 Prävention im Kontext von Cybercrime 81
2.4.2 Wirksamkeitsbezogene Vorüberlegungen 87
2.4.3 Kompetenzen Lehrender in präventiven Maßnahmen 96
2.5 AdressatInnenorientierte Medienkompetenz 98
2.5.1 Der digitale Raum als dynamische Informationsquelle 100
2.5.2 Weiterbildung als Instrument der Arbeitsmarktförderung 101

3 Entwicklung einer präventiven Maßnahme **104**
3.1 Theoretische Fundierung 104
3.2 Entwicklung der präventiven Maßnahme „Der zweite Blick“ 108
3.2.1 Entwicklungsprozess der präventiven Maßnahme 109
3.2.2 Erstellungsprozess einer präventiven Maßnahme 110
3.3 Theorien der Verhaltensbeeinflussung als Grundlage 111
3.4 Recherche und Aufbereitung 112
3.5 Lernziel und Methoden 113
3.6 Ablauforganisation 118

4 Hypothesen ... 120
4.1 Erster Hypothesenkomplex: Messinstrumente ... 120
4.1.1 Hypothese 1: Faktorenstruktur der selbst entwickelten Skalen ... 120
4.1.2 Hypothese 2: Faktorenstruktur der selbst entwickelten Skalen ... 121
4.2 Zweiter Hypothesenkomplex: gesamte Stichprobe ... 122
4.2.1 Hypothese 3: Einstellungsänderung ... 122
4.2.2 Hypothese 4: Urteilsfähigkeit ... 123
4.2.3 Hypothese 5: Kontrollüberzeugung ... 124
4.2.4 Hypothese 6: Selbstwirksamkeit im Kontext von IT-Sicherheit ... 125
4.3 Dritter Hypothesenkomplex: Moderatoren ... 126
4.3.1 Hypothese 7: Generationenzugehörigkeit ... 126
4.3.2 Hypothese 8: Bildungsstand ... 127
4.3.3 Hypothese 9: Geschlecht ... 127
4.3.4 Hypothese 10: VersuchsleiterInnenartefakt ... 128

5 Methodik und Evaluation ... 129
5.1 Forschungsdesign ... 129
5.2 Messinstrumente ... 130
5.2.1 Soziodemografische Daten (FK1) ... 131
5.2.2 Fragenkomplex zur Weiterbildungsmotivation (FK2) ... 131
5.2.3 Fragenkomplex zu den Beweggründen für die Teilnahme (FK3) ... 132
5.2.4 Selbstwirksamkeitserwartung (FK4) ... 132
5.2.5 Evaluation (FK5) ... 133
5.2.6 Geplantes Verhalten (FK6) ... 133
5.3 Untersuchungsdurchführung ... 133
5.3.1 Zeitplan ... 133
5.3.2 Umsetzung der Maßnahme ... 134
5.4 Statistische Analysen ... 134
5.4.1 Explorative Faktorenanalyse (EFA) ... 134
5.4.2 Zweifaktorielle Varianzanalyse mit Messwiederholung ... 137
5.4.3 Regressionsanalyse ... 140
5.4.4 Umgang mit Fehlern erster und zweiter Art ... 142
5.4.5 Umgang mit fehlenden Werten ... 143

6 Ergebnisse ... 144
6.1 Darstellung der Stichprobe ... 144
6.2 Analyse der fehlenden Werte ... 146
6.3 Explorative Faktorenanalysen der neu entwickelten Erhebungsinstrumente ... 146
6.3.1 Hauptkomponentenanalyse des Fragenkomplexes FK1 ... 146
6.3.2 Hauptkomponentenanalyse des Fragenkomplexes FK2 ... 152
6.4 Inferenzstatistische Auswertung ... 155
6.4.1 Wirksamkeit der Maßnahme über die Zeit zwischen EG und KG ... 155
6.4.2 Moderatoren der Wirksamkeit der Maßnahme ... 166

7 Interpretation und Diskussion ... 189
7.1 Interpretation und Diskussion der Ergebnisse ... 189
7.1.1 Einstellung im Kontext von IT-Sicherheit ... 189
7.1.2 Selbstwirksamkeit im Kontext von IT-Sicherheit ... 189
7.1.3 Kontrollüberzeugung im Kontext von IT-Sicherheit ... 190
7.1.4 Moderation der AV durch das Lebensalter ... 191
7.1.5 Moderation der AV durch das Bildungsniveau ... 192
7.1.6 Moderation der AV durch das Geschlecht ... 193
7.1.7 Die Bedeutung des VersuchsleiterInnenartefakts ... 194
7.2 Methodendiskussion ... 194
7.2.1 Entwicklung der präventiven Maßnahme ... 194
7.2.2 Untersuchungsdurchführung ... 196
7.2.3 Auswertung der Daten ... 197

8 Fazit und Ausblick 201

Literaturverzeichnis 204
Anhang 233
Anhang 1: Fragebogen ‚geplantes Verhalten im Kontext IT-Sicherheit' 233
Anhang 2: Fragebogen ‚Weiterbildungsmotivation' 235
Anhang 3: Fragen zu den Beweggründen der Teilnahme (BWG) 236
Anhang 4: Fragen zur Selbstwirksamkeitserwartung (SWE) 236
Anhang 5: Fragen zur Evaluation 237
Anhang 6: Fragebogen zu t1 238
Anhang 7: Fragebogen zu t2 243
Anhang 8: Fragebogen zu t3 247
Anhang 9: Bekanntmachung der Maßnahme im Stadtreporter 250
Anhang 10: Reportage über die präventive Maßnahme 251
Anhang 11: Evaluation der präventiven Maßnahme KG vs. EG 253
Eidesstattliche Erklärung 255

Tabellenverzeichnis

Tab. 1: Beispiele für die Semantik mit Quellen und Ableitungen 38
Tab. 2: Künstliche Verknappung im Kontext von Cybercrime 38
Tab. 3: Medien und deren Syntax 39
Tab. 4: Alter von Cyberstalking-Opfern (Huber 2012, S. 148; Angaben in Prozent) 39
Tab. 5: Interaktionen auf gefälschten Hotspots (Avast 2016, S. 1) 54
Tab. 6: Unkritische Systeme (Husák et al. 2018, S. 5) 57
Tab. 7: Kritische Systeme (Husák et al. 2018, S. 5) 58
Tab. 8: Das heuristisch-systematische Modell (nach Betsch, Funke & Plessner 2011) 66
Tab. 9: Stufen der Verhaltensänderung (Keller 1998, S. 1) 75
Tab. 10: Regressionsanalyse zur Verhinderung von Cyberkriminalität (Ali 2016, S. 21) 83
Tab. 11: Das Modell rationalen Handelns von Obrecht (1996) 85
Tab. 12: Rentabilität präventiver Maßnahmen im Jahr 2015 (nach Hermann & Bubenitschek 2015, S. 37) 85
Tab. 13: Definition von Technologiegenerationen (Sackmann & Winkler 2013, S. 497) 101
Tab. 14: Effektivität der Methoden zur Sensibilisierung für Informationssicherheit (Khan et al. 2011, S. 10863) 106
Tab. 15: Framework des SETA (Whitman & Mattord 2017, S. 212) 106
Tab. 16: Tipps für Sensibilisierungsmaßnahmen des US-Cert (McDowell 2018, S. 1) 108
Tab. 17: Feinziel und Methoden des Moduls 1 für die EG (in Anlehnung an Aulerich et al. 2004, S. 86) 116
Tab. 18: Feinziel und Methoden des Moduls 2 für die EG (in Anlehnung an Aulerich et al. 2004, S. 86) 117
Tab. 19: Feinziel und Methoden der Module 3-6 für die EG (in Anlehnung an Aulerich et al. 2004, S. 86) 117
Tab. 20: Feinziel und Methoden des Moduls 4 für die EG (in Anlehnung an Aulerich et al. 2004, S. 86) 118
Tab. 21: Technikgenerationen im Kontext der präventiven Maßnahme 126
Tab. 22: Abhängige Variablen der Untersuchung 129
Tab. 23: Messinstrumente zur Untersuchung der Wirksamkeit der Maßnahme 130
Tab. 24: Skalen zur Weiterbildungsmotivation 132
Tab. 25: KMO-Koeffizient und Eignung der Daten (Bühner 2011, S. 347) 135
Tab. 26: Grenzwerte nach Kaiser und Rice (1974, S. 112) 136
Tab. 27: Fehlermöglichkeiten bei der Anwendung von Signifikanztests (Janssen & Laatz 2017, S. 317) 142
Tab. 28: Stichprobenbeschreibung hinsichtlich Gruppe, Geschlecht und Bildungsniveau 144
Tab. 29: Stichprobenbeschreibung hinsichtlich des Alters 144
Tab. 30: Motivation der Experimentalgruppe 145
Tab. 31: Motivation der Kontrollgruppe 145
Tab. 32: Entwickelte Messinstrumente 146

Tab. 33: Kommunalitäten der Items zum geplanten Verhalten 147
Tab. 34: Vergleich Eigenwertverlauf zufällig vs. empirisch 148
Tab. 35: Faktorladung beim Fragenkomplex ‚geplantes Verhalten' 149
Tab. 36: Kommunalitäten der Items zu den Beweggründen für die Teilnahme 152
Tab. 37: Vergleich Eigenwertverlauf zufällig vs. empirisch 153
Tab. 38: Faktorladung – Beweggründe der Teilnahme 154
Tab. 39: Vergleich EG und KG über zwei Messzeitpunkte im Hinblick auf das Merkmal ‚Einstellung' 157
Tab. 40: Vergleich EG und KG über drei Messzeitpunkte im Hinblick auf das Merkmal ‚Einstellung' 159
Tab. 41: Vergleich EG und KG über zwei Messzeitpunkte im Hinblick auf das Merkmal ‚Kontrollüberzeugung' 161
Tab. 42: Vergleich EG und KG über drei Messzeitpunkte im Hinblick auf das Merkmal ‚Kontrollüberzeugung' 162
Tab. 43: Vergleich EG und KG über zwei Messzeitpunkte im Hinblick auf das Merkmal ‚Bewertung der Kontrollmöglichkeiten' 164
Tab. 44: Vergleich EG und KG über drei Messzeitpunkte im Hinblick auf das Merkmal ‚Bewertung der Kontrollmöglichkeiten' 166
Tab. 45: Prüfung auf Multikollinearität 168
Tab. 46: Prüfung auf Autokorrelation Alter 168
Tab. 47: Kontrollüberzeugung der Teilnehmenden der EG im Prä-Post-Vergleich 169
Tab. 48: Moderation der AV durch das Lebensalter in der KG im Prä-Post-Vergleich 171
Tab. 49: Moderation der AV durch das Lebensalter in der EG im Prä-Post-Vergleich 171
Tab. 50: Einstellungsänderung zum Lebensalter der EG zum dritten Messzeitpunkt 172
Tab. 51: Einstellungsänderung zum Lebensalter der KG zum dritten Messzeitpunkt 173
Tab. 52: Moderation der AV durch das Lebensalter in der EG im Prä-Follow-up-Vergleich 175
Tab. 53: Moderation der AV durch das Lebensalter in der KG im Prä-Follow-up-Vergleich 175
Tab. 54: Prüfung auf Autokorrelation des Moderators ‚Bildung' 176
Tab. 55: Moderation der AV durch die Bildung in der EG im Prä-Post-Vergleich 178
Tab. 56: Moderation der AV durch die Bildung in der KG im Prä-Post-Vergleich 178
Tab. 57: Selbstwirksamkeit im Kontext von IT-Sicherheit zur Bildung in der EG zum t2 180
Tab. 58: Selbstwirksamkeit im Kontext von IT-Sicherheit zur Bildung in der KG zum t2 181
Tab. 59: Moderation der AV durch die Bildung in der EG im Prä-Post-Follow-up-Vergleich 182
Tab. 60: Moderation der AV durch die Bildung in der KG im Prä-Post-Follow-up-Vergleich 182
Tab. 61: Moderation der AV durch das Geschlecht in der EG im Prä-Post-Vergleich 184
Tab. 62: Moderation der AV durch die Bildung in der KG im Prä-Post-Vergleich 185

Tab. 63: Bedingte Effekte des Prädiktors ‚Selbstwirksamkeit' im Kontext IT-Sicherheit in der EG bei Werten des Moderators ‚Geschlecht' 186
Tab. 64: Bedingte Effekte des Prädiktors ‚Selbstwirksamkeit' im Kontext IT-Sicherheit in der KG bei Werten des Moderators ‚Geschlecht' 187
Tab. 65: Moderation der AV durch das Geschlecht in der EG im Prä-Post-Follow-up-Vergleich 187
Tab. 66: Moderation der AV durch das Geschlecht in der KG im Prä-Post-Follow-up-Vergleich 187
Tab. 67: Moderation der AV durch den Dozenten/die Dozentin 188

Abbildungsverzeichnis

Abb. 1: Digitale Angriffe im Zeitraum 2017-2019 (Berg & Niemeier 2019, S. 3)..... 12
Abb. 2: Gliederung dieser Arbeit 14
Abb. 3: Cybercrime im Jahr 2017 (Fidelis Cybersecurity GmbH 2017, S. 2) 18
Abb. 4: Cybercrime laut der Definition des BKA mit Beispielen 19
Abb. 5: Cyberangriffe auf Scheinrechnern (Boddy 2019, S. 3) 24
Abb. 6: Kategorisierung von Cyberkriminellen (nach Rodgers 2000; Chantler 1996; Hollinger 1988; Chiesa et al. 2009; Füllgraf 2015; Samuel 2004 und Randazzo et al. 2004)..... 28
Abb. 7: Kompetenzmodell der Cyberkriminellen (nach Dreyfus 2004; McGuire & Dowling 2013 sowie Holt 2013) 30
Abb. 8: Zielgruppe von Maßnahmen zur Prävention von Cyberkriminalität (auf der Grundlage der Kompetenzmodelle der Cyberkriminellen von McGuire & Dowling 2013; Holt 2013 und Dreyfus 2004) 32
Abb. 9: Informationssequenz (Frumento 2017) 35
Abb. 10: Semiotische Ebenen des Informationsbegriffes (Brönimann 1970, S. 25)..... 36
Abb. 11: Informationsdichte und Risiko (nach Brönimann 1970, S. 25)..... 37
Abb. 12: Die Top 10 der am meisten genutzten Datei-Anhänge (Selinger 2013, S. 1)..... 42
Abb. 13: Webseite der Africa University (Africa University 2019) 47
Abb. 14: Metapher der Merkmalszusammenhänge von Cyberangriffen (Riedl 2000, S. 73)..... 61
Abb. 15: IT-Komplexität-Abhängigkeitsmodell (Mocker 2009, S. 7)..... 61
Abb. 16: Persuasive Kommunikation (nach Petty & Cacioppo 1986 sowie Helisch & Pokoyski 2009) 64
Abb. 17: Wechselwirkung zwischen persönlicher Relevanz und Expertise der Quelle und der persönlichen Relevanz und Qualität der Argumente (Jonas et al. 2014, S. 242; in Anlehnung an Petty, Cacioppo & Goldman 1981)..... 65
Abb. 18: Die Wirkung von Informationsquellen auf das Verhalten (Renneberg & Hammelstein 2006, S. 37) 68
Abb. 19: Die Wirkung der Bedrohungseinschätzung und Bewältigungs-einschätzung auf die Verhaltensänderung (Witte & Allen 2000, S. 599).... 69
Abb. 20: Der Zusammenhang zwischen der Bedrohungseinschätzung und der Bewältigungskompetenzen (Renneberg & Hammelstein 2006, S. 40) 69
Abb. 21: Theorie des überlegten Handelns (Winter 2013, S. 173; in Anlehnung an Ajzen & Fisbhein 1980)..... 73
Abb. 22: Theorie des geplanten Verhaltens (Winter 2013, S. 182; in Anlehnung an Ajzen & Fishbein 1980)..... 74
Abb. 23: Ergebnisse der Strukturmodellprüfung (Bulgurcu et al. 2010, S. 540)..... 76
Abb. 24: Die SmartPLS 2.0-Ergebnisse für die getestete Beziehung (Ifinedo 2012, S. 19)..... 77
Abb. 25: Ergebnisse der PLS-Analyse (Ilfinedo 2012a, S. 6) 78
Abb. 26: Resultat der Analyse des NAME-Models (D'Arcy, Hovav & Galletta 2009, S. 89)..... 78
Abb. 27: Das theoretisches Modell von Klein & Luciano und seine Hypothesen (Klein & Luciano 2016, S. 483) 80

Abb. 28: Drei Aspekte von Medienkompetenz (Schorb 2020, S. 4) 99
Abb. 29: Das IT-Sicherheits-Lernkontinuum (Wilson & Hash 2003, S. 8) 107
Abb. 30: Security Awareness (Helisch 2009, S. 11) 108
Abb. 31: Gegenüberstellung der Kontroll- und Experimentalgruppe der präventiven Maßnahme 109
Abb. 32: Prozessmodell der präventiven Maßnahme (nach Obrecht 1996)..... 109
Abb. 33: Theorien der Verhaltensbeeinflussung als Grundlage der präventiven Maßnahme 112
Abb. 34: Didaktische Reduktion (in Anlehnung an Riedl 2000, S. 73) 113
Abb. 35: Die Beziehung zwischen Medien und Inhalten in der präventiven Maßnahme 114
Abb. 36: Ablauf der präventiven Maßnahme für die EG 116
Abb. 37: Ablauf der präventiven Maßnahme für die KG 116
Abb. 38: Faktorenanalyse des geplanten Verhaltens 121
Abb. 39: Faktorenanalyse der Beweggründe der Teilnahme..... 122
Abb. 40: Ablauf der Studie 129
Abb. 41: Pfaddiagramm des Moderatoreffekts (Urban & Mayerl 2018) 140
Abb. 42: Statistisches Diagramm des Regressionsmodells (Hayes 2018, S. 21) .. 140
Abb. 43: Häufigkeitsverteilungen des Alters in der EG und der KG zu t1 und t2.... 145
Abb. 44: Scree-Plot zum Fragenkomplex ‚geplantes Verhalten‘..... 148
Abb. 45: Optimierte Faktorladung zu FK5 151
Abb. 46: Scree-Plot zum Fragenkomplex ‚Beweggründe für die Teilnahme‘ 153
Abb. 47: Optimierte Faktorladung zu FK2 154
Abb. 48: Mittelwertvergleich der Einstellung der Teilnehmenden (EK/KG) zu t1 und t2 157
Abb. 49: Mittelwertvergleich der Einstellung der Teilnehmenden (EK/KG) zu t1, t2 und t3 158
Abb. 50: Mittelwertvergleich der Kontrollüberzeugung der Teilnehmenden (EK/KG) zu t1 und t2..... 160
Abb. 51: Mittelwertvergleich der Kontrollüberzeugung der Teilnehmenden (EK/KG) zu t1, t2 und t3..... 162
Abb. 52: Mittelwertvergleich der Selbstwirksamkeit im Kontext von IT-Sicherheit (EK/KG) zu t1 und t2..... 164
Abb. 53: Mittelwertvergleich der Selbstwirksamkeit im Kontext von IT-Sicherheit (EK/KG) zu t1, t2 und t3..... 165

Vorwort

Der Diskurs, ob Sensibilisierungsmaßnahmen im Kontext von IT-Sicherheit die beabsichtigte Wirkung haben, hat mich in meiner Tätigkeit als IT-Sicherheitsbeauftragter immer begleitet.

Um eine Antwort darauf zu finden, wurden Diskurse auf unterschiedlichen fachlichen Ebenen geführt, gingen aber letztendlich ergebnislos aus. Da durch öffentliche Gelder geförderte Veranstaltungen, in denen bundesweite Cyberangriffe thematisiert werden, bislang nach Veranstaltungsende nicht auf ihre beabsichtigte Wirkung überprüft wurden, entwickelte ich eine kritische Perspektive. Weiter sah ich als IT-Schulbetreuer die Defizite des sonderpädagogischen Personals an Berufs- und Förderschulen hinsichtlich der Informationssicherheit. Denn das Personal war teilweise überrascht, wenn auf den Rechnern der SchülerInnen mit pädagogischem Unterstützungsbedarf Schadcode vorhanden war und auch ausgeführt wurde. Um diesen für mich unbefriedigenden Zustand zu ändern, entwickelte ich den Plan, empirisch zu forschen, um mithilfe der so gewonnenen wissenschaftlich abgesicherten Ergebnisse zu weiteren (objektiven) Diskursen anzuregen.

Entstehen konnte diese Arbeit, weil viele Menschen ihren Entstehungsprozess begleitet haben. Dafür möchte ich mich ganz herzlich bedanken, denn ohne diese Begleitung wäre eine Ausarbeitung in dieser Form nicht möglich gewesen. Hervorheben möchte ich die sehr gute Zusammenarbeit mit meiner Erstbetreuerin Prof. Dr. Marie-Christine Vierbuchen und meiner Zweitbetreuerin Prof. Dr. Birgit Spies. Aufkommende Fragen wurden kompetent beantwortet, und immer wieder erhielt ich hilfreiche Tipps. Weiter möchte ich mich bei meinem Kollegen Börge Glawe bedanken, der mir den Zugang zur präventiven Arbeit ermöglichte und mich animierte, ein präventives Projekt durchzuführen. Gleichfalls gilt mein Dank Birke Sander für die Beantwortung didaktischer Fragestellungen und Daniela Keller und Dr. Björn Walter für die Beantwortung statistischer Fragen. Auch dem Team der Summer School der DGfE möchte ich meinen Dank aussprechen.

1 Einleitung

1.1 Problem- und Fragestellung

Industrialisierung, technischer Fortschritt und die globalisierte Vernetzung lassen deutlich werden, dass sich im letzten Jahrhundert die Geschwindigkeit vieler Prozesse und Vorgänge drastisch erhöht hat. Sowohl ökonomische als auch soziale Prozesse laufen deutlich schneller ab als noch vor einigen Jahrzehnten, was an sich eine positive Entwicklung darstellt: Die Produktivität ökonomischer Prozesse hat sich erhöht, neue Kommunikationswege wurden entwickelt und die Breite und Tiefe des Sortiments digitaler Medien und damit die Auswahlmöglichkeit ist für viele Menschen drastisch gestiegen. Daraus ergeben sich vielfältige Möglichkeiten der persönlichen Entwicklung, da Menschen mithilfe von neuen Kommunikationsmöglichkeiten ortsunabhängig ihren Lebensweg gestalten und auch verwirklichen können (Sauldie 2014).

Die Kompensation von Bedürfnissen, gefolgt von neuen Ideen, lässt letztendlich weitere Bedürfnisse entstehen. Dieser Zyklus, ein Wechselspiel zwischen Altem, Verändertem und Neuem, ist der Motor, der das (Wirtschafts-)Wachstum stetig antreibt. Multifunktionales Equipment, das telefoniert, Sprache erkennt und Videos verschickt, ist verfügbar und bereits in den unterschiedlichsten Zielgruppen angekommen. Die Begeisterung für neue Technologien ist teilweise so groß, dass die technologische Komplexität ignoriert wird und nur dann in den Fokus gerät, wenn (wieder) etwas nicht so wie erwartet funktioniert und deshalb Ärger produziert (Brinks 2010). Dabei richtet sich der primäre Fokus der meisten RezipientInnen nicht auf die Komplexität, sondern auf die Bedienung, auf das Mit-dabei-Sein und die Reichweite des technisch Möglichen.

Das Bedürfnis, in der Bequemlichkeit nicht gestört zu werden (Ternès & Hagemes 2018), die Unabhängigkeit und die Distanz zur technischen Komplexität lassen jedoch vermuten, dass diese Fokussierung auch als ambivalent verstanden werden kann. Denn mit der Nutzung neuer Medienprodukte, die zum Beispiel Kuscheltiere in Sprachübertragungsstationen umwandeln, oder von Kommunikationsmitteln, die Schadcode aufnehmen können, wächst auch die Gefahr des Missbrauchs sowie die Herausforderung, eine sichere Bedienung bzw. Nutzung leisten und auch fachgerecht umsetzen und bewerten zu können. Gerade für Personen über 65 Jahre, die auch an der Kommunikation teilnehmen möchten und müssen (Schorb 2009), gestalten sich diese Bedingungen bereits so komplex, dass sie die Technologien z.T. ohne eine externe Unterstützung nicht erfolgreich nutzen können (Rosenstock, Schweiger & Schubert 2016). Dieser Umstand hat Folgen und bedeutet Unwissenheit, Furcht (Dreißigacker & Riesner 2018) und Fehlverhalten, das für jedermann deutlich sichtbar wird. Mehr als jede/r Zweite, die/der (trotzdem) im Internet einkauft, schätzt die Sicherheit im Internet bereits skeptisch ein. Und

Erwachsene, die ohnehin Bedenken wegen der Datensicherheit und Internetkriminalität hegen, kaufen weit weniger online ein (24 %) als jene, die derartige Bedenken nicht teilen (von Bothmer 2017). Untermauert werden diese Bedenken, indem Cyberkriminelle durch ihre Interaktionen fast monatlich zeigen, wie Unternehmen mit Schadsoftware, Berufstätige mit sabotiertem Onlinebanking (Schneider 2019) oder KäuferInnen von Internetspielzeug mit Sicherheitslücken infiltriert (Markuson, 2019) werden können: „A vulnerability is a weakness in a device, system, application, or process that might allow an attack to take place. A threat in the world of cybersecurity is an outside force that may exploit a vulnerability“ (Chapple & Seidl 2017, S. 24). Dabei nehmen Cyberangriffe deutlich zu. So zeigen Berg und Niemeier (2019) in ihrer Studie „Wirtschaftsschutz in der digitalen Welt“, dass Cyberangriffe im Zeitraum 2017-2019 von 43 % auf 70 % gestiegen sind und im Jahr 2019 einen Schaden von 102,9 Mrd. Euro verursachten. Welche Arten von Cyberangriffen das detailliert waren, zeigt die Abbildung 1.

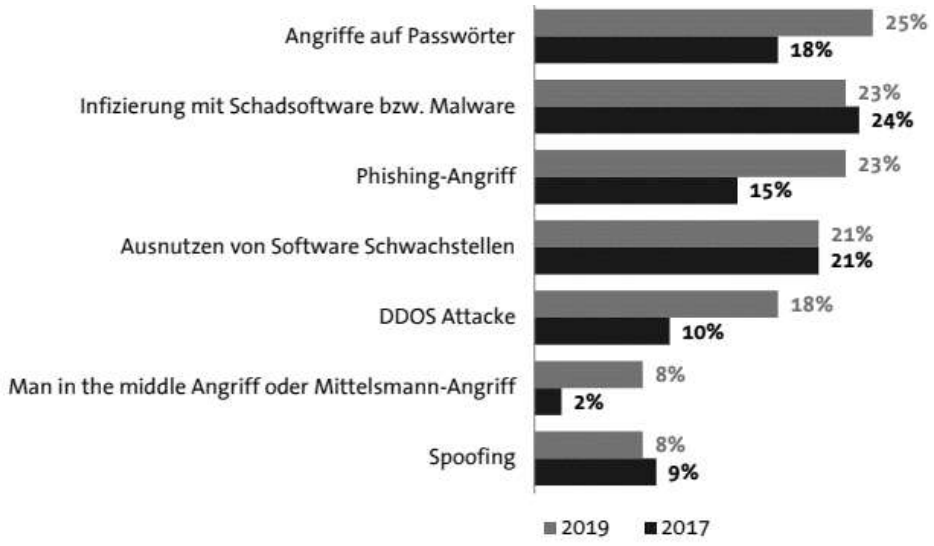


Abb. 1: Digitale Angriffe im Zeitraum 2017-2019 (Berg & Niemeier 2019, S. 3)

Das Land Mecklenburg-Vorpommern hat diese Probleme erkannt und entsprechende präventive Projekte ins Leben gerufen. Diese sogenannte Cybercrimeprojekte für Erwachsene sind derzeit also neu und kaum erforscht, da für den Wissenstransfer eine zielgruppenspezifische Auseinandersetzung mit der vorliegenden technischen Komplexität, der Expertise der Cyberkriminellen, die auch als HackerInnen bezeichnet werden, und dem bei den NutzerInnen vorhandenen Wissen erforderlich ist: „It is important that organizations not only provide training and education for awareness raising but also these trainings must be effective enough in changing behaviour both individually and collectively“ (Benson & McAlaney 2019, S. 98).

Ohne genau zu wissen, welche Faktoren in präventiven Veranstaltungen zum Thema Cybercrime, die sich an heterogene Zielgruppen wenden, dazu beitragen, dass aus Inhalten individuelles Wissen konstruiert wird, besteht allerdings die Gefahr, dass

präventive Veranstaltungen zwar gewünschte Ziele fokussieren, diese jedoch möglicherweise verfehlen. Mögliche Folgen wären kontraproduktive Lernerfolge, die nicht sensibilisieren, sondern die Lernenden in ihrer wahrgenommenen Verhaltenskontrolle bei der Anwendung von Schutzmechanismen im Kontext Cybercrime weiter destabilisieren und ihre bereits vorhandene Unsicherheit sowie ihr Ohnmachtsempfinden noch verstärken. Ziel der hier vorliegenden Arbeit ist dementsprechend die Untersuchung der Wirksamkeit einzelner Faktoren innerhalb präventiver Veranstaltungen sowie der Fragestellung, ob bzw. in welchem Maße diese Faktoren einen statistisch signifikanten Einfluss auf den Lernerfolg der Zielgruppe haben. Denn wenn eine Wirksamkeit der Veranstaltungen und deren Prädiktoren festgestellt werden kann, könnten zukünftige präventive Maßnahmen im Kontext des Cybercrime optimiert und kostengünstiger sowie evidenzbasiert konzipiert werden. Dabei sollte sich die zu analysierende Zielgruppe aus 18- bis 67-Jährigen zusammensetzen, da diese für den Arbeitsmarkt von Bedeutung sind und ihr Wissen im beruflichen Alltag zur Informationssicherheit beitragen kann.[1]

1.2 Grundlegende Vorgehensweise im Forschungsprozess und forschungsleitende Annahmen

Die in dieser Arbeit zentrale empirische Studie soll dazu beitragen, bestehende Forschungslücken bezüglich der Wirksamkeit von Präventionsmaßnahmen zum Thema Cybercrime zu schließen. Zu diesem Zweck werden im Rahmen einer quantitativen Untersuchung die Wirkungen einer Intervention erforscht, indem die Wirkungen in einer Experimentalgruppe (programmgebundene Wirkungen auf vielfältigen Ebenen) den Wirkungen in einer Kontrollgruppe (interventionsgebundene Wirkungen: reine Präsentation von HackerInnenangriffen) gegenübergestellt werden. Dabei liegt der Forschung die Annahme zugrunde, dass das didaktische Setting sowie die Vorbildung, das Geschlecht und das Alter der Untersuchungsteilnehmenden eine Wirkung auf a) die Einstellung, b) die Urteilsfähigkeit, c) die Selbstwirksamkeit und d) die Kontrollüberzeugung der in die Untersuchung eingebundenen Personen haben.

[1] „One of the dynamics that makes the one-size-fits-all awareness or education campaign ineffective is the diversity in the population“ (Erbschloe 2019, S. 181).

1.3 Aufbau der Arbeit

Die Arbeit ist, wie die folgende Abbildung 2 erkennen lässt, in acht Kapitel gegliedert.

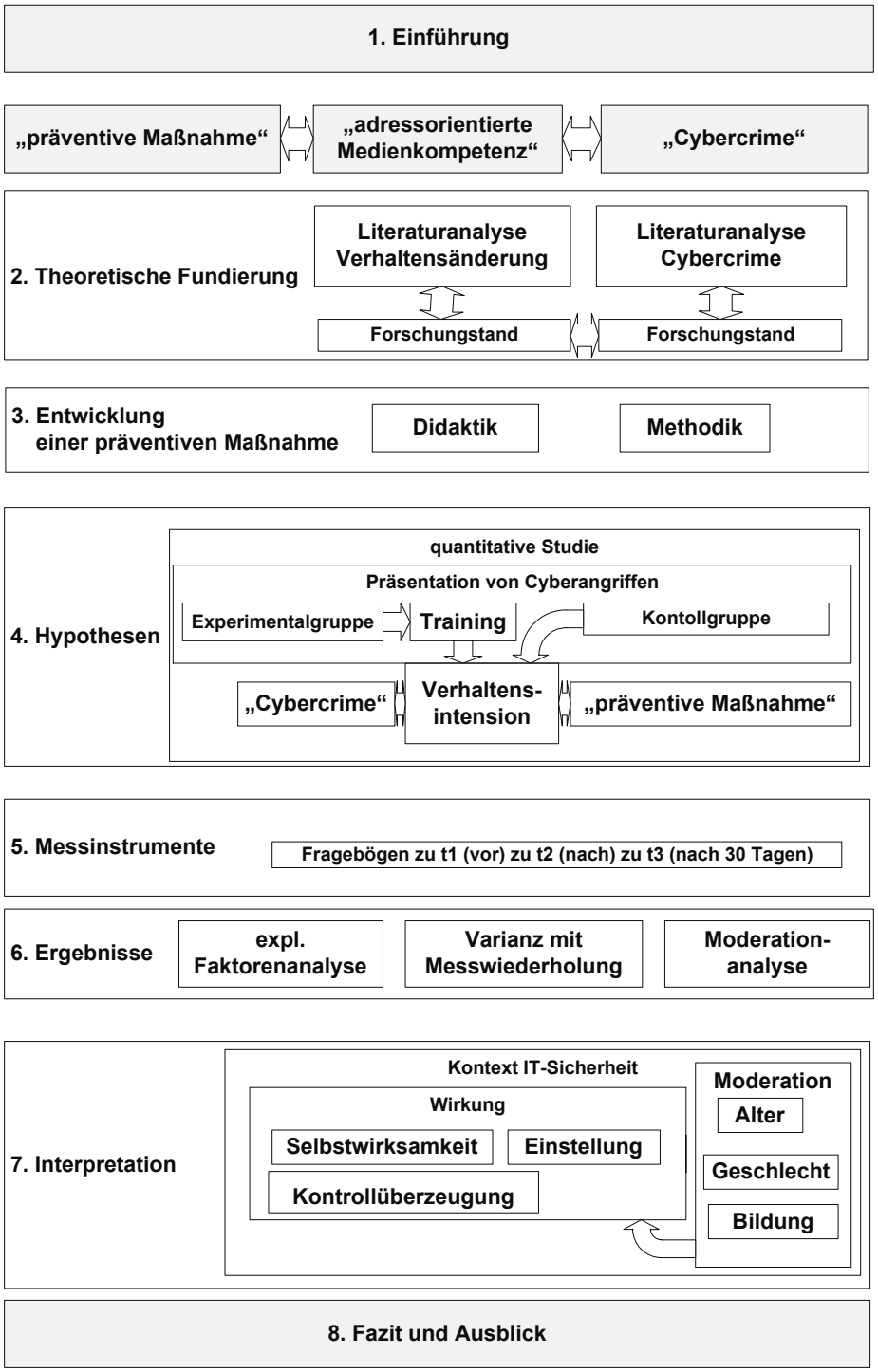


Abb. 2: Gliederung dieser Arbeit

Im Kapitel 2 werden die für die Fragestellung dieser Arbeit relevanten Theorien zu Verhaltensänderungen und Cybercrime behandelt und es wird erörtert, inwiefern diese theoretischen Überlegungen in der empirischen Untersuchung umgesetzt werden. Darauf aufbauend wird im dritten Kapitel eine präventive Maßnahme konzipiert, die laut ihrer beabsichtigten Wirkung zur Verhaltensintension beitragen soll. Im vierten Kapitel

werden Hypothesen entwickelt, die im Rahmen der empirischen Erhebung überprüft werden sollen, und im fünften Kapitel werden die in dieser Arbeit genutzten Messinstrumente vorgestellt. Das sechste Kapitel stellt die ermittelten Ergebnisse dar. Eine Interpretation dieser Ergebnisse erfolgt im siebten Kapitel. Den Abschluss dieser Arbeit bildet das achte Kapitel, das sowohl die Ergebnisse resümiert als auch weitere Forschungsaufgaben aufzeigt.

2 Theoretische Fundierung

2.1 Cybercrime

Der Begriff Cybercrime ist relativ neu und setzt sich aus den Begriffen Cyber und Crime zusammen. Der Versuch, den Terminus Cyber etymologisch zu erforschen, zeigt, dass hierzu kaum Quellen vorhanden sind. Vermutet wird, dass der Begriff auf den englischen Begriff cybernetics und den griechischen Begriff kybernetes zurückgeht. Beides kann gemäß den Wissenschaften von der Kybernetik als Steuermannskunst gedeutet werden (Bartels 1996). Zielführender und dem allgemeinen Verständnis naheliegender ist jedoch die Definition, die der Duden für diesen Begriff bereithält, denn der Begriff Cyber wird dort als „die von Computern erzeugte virtuelle Scheinwelt“ (Dudenredaktion 2019) definiert. Da „Crime“ das englische Wort für Kriminalität ist (ebd.), lässt sich Cybercrime also als Kriminalität in einer von Computern erzeugten virtuellen Scheinwelt verstehen.

Diese Komposition der Definition adressiert ihren Gegenstand jedoch unvollständig, da die kontextabhängige Rahmung nicht angegeben ist und somit die Definition anderen Kontexten zugeordnet werden kann. Denn schon ein Blick auf die Mediennutzung, wie z.B. den Fernsehkonsum, zeigt bereits allgemeinverständlich, dass diese Definition auch auf kriminelle Handlungen, die in Filmen vorgeführt, dargestellt und letztendlich von MedienkonsumentInnen bewertet werden, passt. Somit erweist sich diese etymologisch entwickelte Definition im Kontext dieser Arbeit als unzureichend, da Fehlinterpretationen möglich sind. Insofern geht es nun darum, eine für diese Arbeit geeignete Definition zu finden.

2.1.1 Definitionen und Eingrenzung

Die Definitionen von Cybercrime sind so zahlreich wie die Autorinnen und Autoren, die den Versuch unternehmen, diesen Begriff mit Real-, Nominal- oder operationalisierten Definitionen einzurahmen. Einige Autorinnen und Autoren, unter denen sich auch HerstellerInnen von Sicherheitslösungen befinden, versuchen sich dem Thema mit einer Nominaldefinition zu nähern. So versteht die Unternehmung Symantec (2019, S. 1) unter Cybercrime „jedes Verbrechen, das mit Hilfe eines Computers, Netzwerks oder Hardware-Geräts begangen wird“. Dabei wird jedoch übersehen, dass solche Definitionen den Computer als physisches Tatwerkzeug miteinschließen, sodass diese sich nicht als für diese Forschung adäquate Arbeitsdefinition erweisen. Weis (2017, S. 1), der sich in seinem Brandmauer IT-Security-Blog mit dem Thema Cybercrime beschäftigt, definiert Cybercrime hingegen mit den Worten: „Laut Definition beschreibt Cyberkriminalität eben die Straftaten, die Daten, das Internet oder IT-Systeme zum Angriffsziel haben. Ferner

umfasst Cyberkriminalität auch die Straftaten, die mithilfe dieser Technologien begangen werden“. Auch das Bundeskriminalamt wählt diese Art der Definition und kategorisiert Cybercrime im engeren und weiteren Sinne wie folgt: „Cybercrime umfasst die Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten (Cybercrime im engeren Sinne) oder die mittels dieser Informationstechnik begangen werden“ (BKA 2016, S. 2).

In seinem Bundeslagebild Cybercrime beschreibt das Bundeskriminalamt sehr ausführlich mit einer operationalisierten Definition, welche Interaktionen dem Begriff Cybercrime im engeren Sinne zuzuordnen sind (BKA-SO51 2016, S. 4):

- „Sonstiger Computerbetrug gem. § 263a Abs. 1 und 2 StGB sowie Vorbereitungshandlungen gem. § 263a Abs. 3 StGB
- Betrügerisches Erlangen von Kfz gem. § 263a StGB
- Weitere Arten des Kreditbetruges gem. § 263a StGB
- Betrug mittels rechtswidrig erlangter Daten von Zahlungskarten gem. § 263a StGB
- Betrug mittels rechtswidrig erlangter sonstiger unbarer Zahlungsmittel gem. § 263a StGB
- Leistungskreditbetrug gem. § 263a StGB
- Abrechnungsbetrug im Gesundheitswesen gem. § 263a StGB
- Überweisungsbetrug gem. § 263a StGB“.

Dass das Thema Cybercrime an Brisanz[2] nicht verloren hat, sondern eher zunimmt, lässt sich zusätzlich anhand statistischer Zahlen aus dem Bundeslagebild Cybercrime 2016 untermauern: 82649 Fälle von Cybercrime im engeren Sinne, die einer Tendenz von +80.5 % (BKA-SO51 2016) entsprechen, sind ein bedenkliches Ergebnis, das Interventionen erforderlich macht. Wobei hier verstärkend hinzukommt, dass die amerikanische Firma Fidelis im Jahr 2017 den Stand der Cybersecurity für Deutschland als besonders bedenklich einschätze, wie aus der folgenden Abbildung 3 hervorgeht.

[2] Erste Vorfälle gehen bis in die 1970er-Jahre zurück (Lempert 2018).

Abb. 3: Cybercrime im Jahr 2017 (Fidelis Cybersecurity GmbH 2017, S. 2)

Auf Basis der Eingrenzungen (im engeren Sinne) und der Operationalisierung (Messbarkeit) im Bundeslagebild Cybercrime des BKA, die praxisbezogen, aktuell und realitätsnah[3] erfolgen, liegt dieser Arbeit entsprechend die folgende, oben bereits angeführte Definition von Cybercrime des BKA zugrunde und fungiert als Ausgangsdefinition: „Cybercrime umfasst die Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten (Cybercrime im engeren Sinne) oder die mittels dieser Informationstechnik begangen werden*"* (BKA 2016, S. 2)*.*

In Abgrenzung zu anderen kriminellen Handlungen im Internet (Cybercrime im weiteren Sinne) werden in dieser Arbeit allerdings nur kriminelle Handlungen fokussiert, die im engeren Sinne als Cybercrime zu verstehen sind, da diese Formen der Kriminalität vermehrt auftreten (Wendekamm & Frevel 2017) und massive gesellschaftliche Folgen haben können (Albrecht 2018), wodurch professionelle Präventionsmaßnahmen erforderlich werden.

In der Abbildung 4 wird der Forschungsgegenstand in den Kontext von Cybercrime gesetzt und visualisiert, ohne (vorerst) auf die einzelnen Angriffsmethoden dezidiert einzugehen.

[3] Nicht alle Fälle werden erfasst.

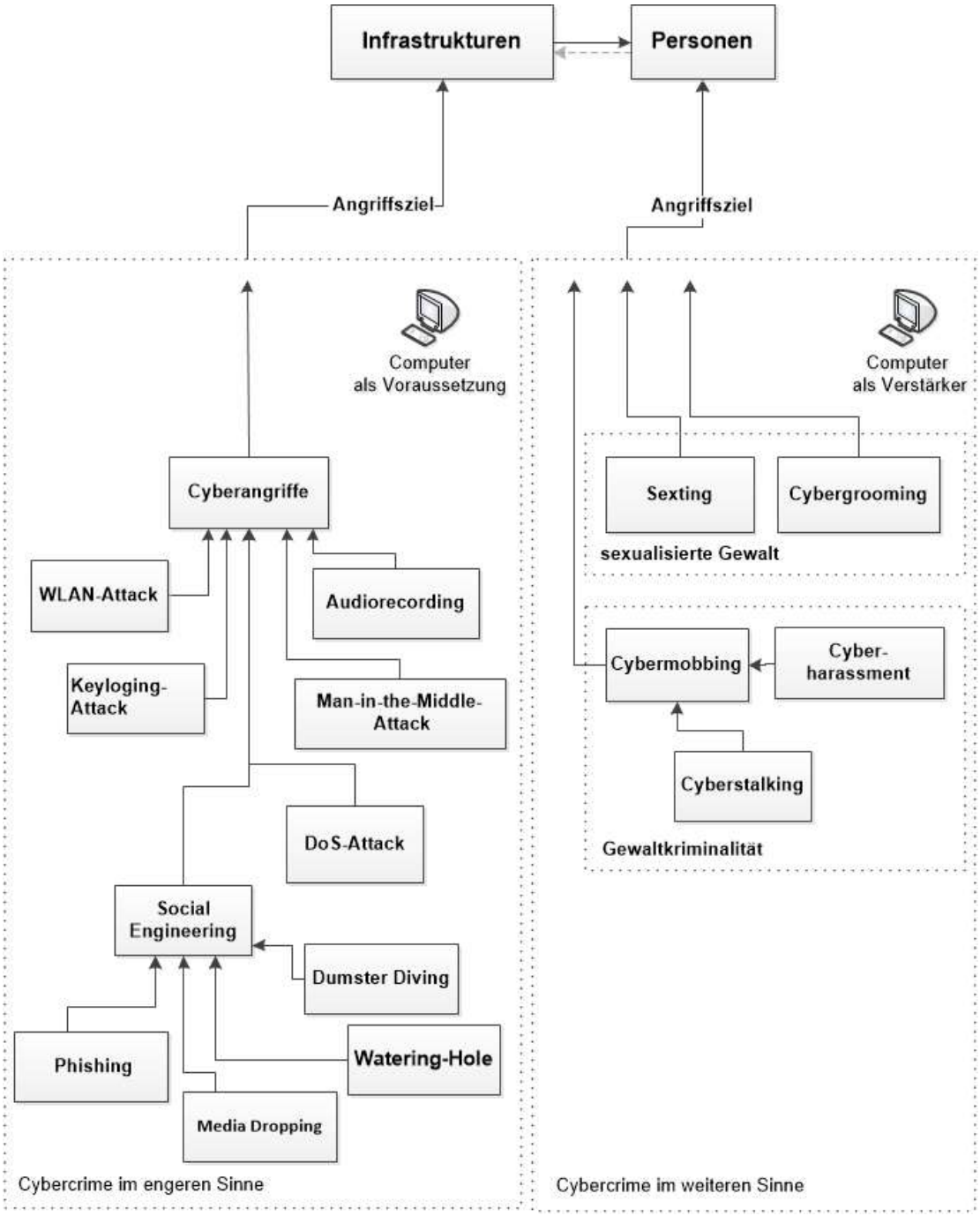


Abb. 4: Cybercrime laut der Definition des BKA mit Beispielen

2.1.2 Ist-Situation

Realitätsbezogene Perspektiven machen deutlich, dass im Jahr 2017 33 % der gegen Unternehmen gerichteten Cyberattacken erfolgreich waren. Dennoch ignorieren 61 % der Führungskräfte weltweit Schadcode wie Ransomware (der Daten verschlüsselt) und bringen damit ihr Unternehmen in Gefahr (Fidelis-Cybersecurity 2017). Eine Erklärung hierfür könnte sein, dass nur 8 % der Führungskräfte ein sehr gutes Verständnis für Informationssicherheitsprobleme besitzen, wie aus den Global Human Capital Trends von 2016 hervorgeht, in die 7000 Befragte aus 130 Ländern involviert waren (Schwartz

2016). Der Begriff Cybercrime gilt jedoch allgemein als vertraut. Narahari und Shah (2016) verweisen in ihrer indischen Studie „Cyber Crime and Security“ darauf, dass 47 % der InderInnen mit dem Begriff Cyberkriminalität vertraut sind. Laut der Studie definieren 75 % der 100 Befragten Cyberkriminalität als politisch motivierte Angriffe auf Computersysteme großer Infrastrukturen. Und 43 % sind sich bewusst, dass IT-Abteilungen mit Cyberkriminalität zu kämpfen haben. Was diese Cyberkriminalität angeht, weist das Unternehmen Kaspersky, ein Anbieter von Sicherheitssoftware, für den Zeitraum 2016-2017 in 213 Ländern 1.188.728.338 Cyberattacken nach und macht darüber hinaus (und damit auch marktwirtschaftlich) deutlich, dass die am häufigsten angegriffenen Länder im Jahr 2017 dieselben geblieben sind: die USA (33,57 %), die Niederlande (23,78 %) und Deutschland (10,94 %) (Kaspersky 2017).

Die hohe Kriminalitätsquote geht mit der Furcht, einem Cyberangriff zu erliegen, einher. So hat bereits jede/r zweite AnwenderIn (48 %) Furcht, ein Opfer von Cyberkriminalität zu werden (Ipsos 2017). Und gelingen Cyberangriffe, verdoppeln sich die affektive computerbezogene Kriminalitätsfurcht (von 6,6 % auf 12,8 %) sowie die kognitive computerbezogene Kriminalitätsfurcht (von 5,3 % auf 12,8 %), wie Dreißigacker und Riesner (2018) in einer Studie mit 2500 Befragten herausfanden. Wickert (2020) unterscheidet in diesem Kontext zwischen der affektiven und der kognitiven Kriminalitätsfurcht. Während die affektive Kriminalitätsfurcht eine gefühlsbezogene Komponente sei, die mit einem deliktunspezifischen Unsicherheitsgefühl einhergehe, Opfer eines spezifischen Deliktes zu werden, meine die kognitive Kriminalitätsfurcht die individuelle verstandesbezogene Risikoeinschätzung. Somit sind zeitnahe Interaktionsmaßnahmen erforderlich, um gesellschaftliche Errungenschaften zu schützen und technische Entwicklungen utilitaristisch fortschreiben zu können.

2.1.3 Staatliche Maßnahmen gegen Cyberangriffe

Cyberangriffe sind infrastrukturell wirksam und, wie bereits ausgeführt wurde, über Landesgrenzen hinweg (EZFF 2018) in der digitalen Welt zum Problem geworden. Die EU-Kommission hat darauf jedoch bereits reagiert und verschiedene Maßnahmen vorgestellt, deren Ziel es ist, in Europa eine solide Informationssicherheitsstruktur aufzubauen und zu etablieren. Voraussetzung hierfür sind Richtlinien, die zielführend die Informationssicherheitsstrukturen untermauern und erforderliche Prämissen transparent machen.

Die Richtlinie 2016/1148 des Europäischen Parlaments und Rates vom 6. Juli 2016 ist eine Maßnahme zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (EU 2016). Denn die EU hat erkannt, dass eine flächendeckende Informationssicherheit nur zu erreichen ist, wenn ein Staatenverbund wie die EU die gleichen Sicherheitsstandards für alle Mitglieder festlegt und

diese auch implementiert. Um diese Zielsetzung auch praktisch umsetzen zu können, werden Kooperationen vereinbart, in denen ein Austausch von Informationen sowie ein Fortschreiben von Leit- und Richtlinien erfolgt.

Eine weitere Gesetzgebung zu diesem Thema findet sich in der Datenschutz-Grundverordnung der EU, die am 25. Mai 2018 rechtskräftig geworden ist. In der letzten Fassung vom 27. April 2016 beschreibt der Artikel 32, wie AnbieterInnen von IT-Dienstleistungen, die mit personenbezogenen Daten arbeiten, zu verfahren haben. Die Rede ist hier von:

> „geeigneten technischen und organisatorischen Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem ein:
>
> a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
> b) die Fähigkeit, Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
> c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
> d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung“ (EU-DSGVO 2016, S. 51).

Die Auseinandersetzung mit dem Thema Informationssicherheit in Deutschland zeigt, dass Deutschland entsprechende Gesetze mit ähnlichem Inhalt auf den Weg gebracht hat. Hervorzuheben sind hierbei das Telemediengesetz (TMG 2007) und das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2017). Das Telemediengesetz rahmt alle elektronischen Informations- und Kommunikationsdienste und beschreibt ausführlich in § 13 Absatz 7 die Pflichten von DienstanbieterInnen:

> „Dienstanbieter haben, soweit dies technisch möglich und wirtschaftlich zumutbar ist, im Rahmen ihrer jeweiligen Verantwortlichkeit für geschäftsmäßig angebotene Telemedien durch technische und organisatorische Vorkehrungen sicherzustellen, dass kein unerlaubter Zugriff auf die für ihre Telemedienangebote genutzten technischen Einrichtungen möglich ist und diese a) gegen Verletzungen des Schutzes personenbezogener Daten und b) gegen Störungen, auch soweit sie durch äußere Angriffe bedingt sind, zu gewährleisten“ (TMG 2007).

Damit sind datenverarbeitende Organisationen, wenn personenbezogene Daten tangiert werden, verpflichtet, eine sichere Infrastruktur bereitzustellen, die technisch möglich und wirtschaftlich zumutbar ist. Und auch der Bundesverband Digitale Wirtschaft fordert eine Umsetzung gemäß dem derzeitigen technischen Stand: „Die Bezugnahme auf den

Stand der Technik bedeutet, dass die IT-Sicherheitsmaßnahmen dem aktuellen Entwicklungsstand entsprechen müssen, soweit er technisch-praktisch realisierbar ist“ (BVDW 2018, S. 104).

Somit sind aktuelle Sicherheitsarchitekturen anzuschaffen, einzusetzen und aktuell zu halten. Untermauert werden diese Forderungen mit länderspezifischen Datenschutzgesetzen. So hat Deutschland, nachdem erkannt wurde, dass Cyberangriffe ganze Wirtschaftszweige außer Betrieb setzen können, diesbezüglich ein IT-Sicherheitsgesetz (IT-Sicherheitsgesetz 2017) auf den Weg gebracht. In diesem Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme werden kritische Infrastrukturen fiskalisch und behördlich eingegrenzt sowie mit Meldepflichten versehen. Und auch die Bevölkerung sieht staatliche Maßnahmen gegen Cybercrime als Pflichtaufgaben. So sehen 81 % der durch das SINUS-Institut Befragten den Staat und 83 % die Wirtschaft in der Pflicht, für sichere Kommunikationsmöglichkeiten im Internet zu sorgen. Allerdings trauen 76 % der Gesellschaftsmitglieder und 68 % der Unternehmen dem Staat entsprechende Interaktionen nicht zu. 70 % der Befragten wünschen sich jedoch, dass der Staat konkrete Kontrollmechanismen etabliert, Sicherheitssiegel vergibt und als übergeordnete Kontrollinstanz fungiert (SINUS-Institut 2017). Um jedoch wirksam gegen Cyberkriminelle vorgehen zu können, bedarf es einer Analyse derartiger Interagierenden, um Gegenmaßnahmen täterInnenbezogen wirksam einleiten zu können.

2.1.4 Problem der Identifizierung von Cyberangriffen und deren Konsequenz

Werden Cyberattacken entdeckt, die daraus resultieren, dass Schutzmaßnahmen unzureichend implementiert worden waren, entstehen zwangsläufig bei den Geschädigten Fragen, die täterInnenbezogen fokussiert sind. Erhoffte Zuschreibungen von Cyberangriffen erweisen sich jedoch in der Praxis als problematisch: „Increasing crimes in cyberspace can be deterred and prevented through effective attribution techniques. However, attribution remains challenging because of the inherent anonymity in cyberspace and advancements in cybercriminal technologies“ (Shamsi & Flowers 2016, S. 13). Studien aus den USA belegen bereits, das 33,7 % der Befragten (n = 89) unsicher sind, wie ihre Konten kompromittiert wurden (Shay et al. 2014). Deibert und Rohozinski (2009) sehen die Gründe in der eingeschränkten Verfolgbarkeit, da digitale Interaktionen kaum noch nachverfolgt werden können. Denn Cyberkriminelle benutzen hierzu Cyberattacken mit entsprechender Hard- und Software, die weltweit zur Verfügung stehen und deren Kommunikationswege kaum noch einsehbar sind (Graves 2010). Deshalb gilt: „The distributive nature of cyber-crime and cyber-terrorism makes tracing the perpetrators, the victims, and the technology used to execute the attack or crime difficult“ (Hosmer 2014,

S. 305). Verstärkend kommt hinzu, dass selbst IT-ExpertInnen (n = 1083) einschätzen, dass 35 % aller Cyberattacken in einem Jahr unentdeckt bleiben und ein weiteres Jahr vergeht, um die Ursache eines Cyberangriffes zu identifizieren (Ponemon-Institute 2014).

Wird dieses Risiko missachtet oder ignoriert, besteht nicht nur die Gefahr, einem Sicherheitsvorfall und dessen Zuordnung ausgesetzt zu sein, sondern auch, dass unwissentlich eigene Infrastrukturen unbekannten Cyberkriminellen zur Verfügung gestellt werden (Lange & Bötticher 2015). Werden aus diesen Infrastrukturen heraus kriminelle Handlungen begangen,[4] reicht es nicht aus, darauf zu verweisen, dass begründeter Verdacht besteht, dass Cyberkriminelle unrechtmäßig interagierten. Vielmehr hat die Betreiberin bzw. der Betreiber selbst den Beweis zu erbringen, dass es sich um eine unautorisierte Nutzung handelte (AG Frankfurt/Main 17.02.2016 - 380 C 2838/15 (75)). Diese Entscheidung der AG Frankfurt/Main zeigt zudem sehr deutlich, dass der Gesetzgeber erwartet, dass der „Stand der Technik“ von BetreiberInnen, auch privaten, eingehalten wird. Und auch wenn Interaktionen wie z.B. betrügerische Überweisungen mittels Phishing der oder dem Nutzenden unbekannt waren, geht der Schadensfall zu Lasten der/des Betreibenden (AG Frankfurt/Main 24.03.2016 - 32 C 3377/15 (72)). Damit wird transparent, dass Sicherheitsvorfälle unbedingt zu verhindern sind, da die Beweislast bei einem Cyberangriff bei der/dem Betreibenden von IT-Infrastrukturen liegt und somit Kompetenzen im Umgang mit IT-Technik vorausgesetzt werden.

Um eine Identifizierung trotzdem möglich werden zu lassen, so beschreiben es Rid und Buchanan (2015) in ihrer Abhandlung „Attributing Cyber Attacks“, bedürfte es Taktiken und Strategien, um eine Operationalisierung von TäterInnen durchführen zu können. Wie diese aussehen können, beschreibt Lin (2016) in seiner Publikation „Attribution of Malicious Cyber Incidents“ und verweist detailliert auf die technische Forensik als Mittel der Identifizierung, die jedoch laut Årnes (2018) SpezialistInnen vorbehalten ist. Präventive Interaktionen zum gleichen Kontext zeigt Saalbach (2017) in der Publikation „Attribution of Cyber Attacks Methods and Practice” auf und empfiehlt die Implementierung vorgetäuschter Infrastruktur als Angriffsziel für Cyberkriminelle, um anschließend die Delikte TäterInnen zuschreiben zu können. Diese Vorgehensweise lässt eine Asymmetrie des vorhandenen Wissens vermuten, die auch in der Publikation „Public Attribution of Cyber Incidents“ (Egloff & Wenger 2019) aufgenommen und behandelt wird.

Im privaten Kontext sind diese Identifizierungsmöglichkeiten allerdings wenig hilfreich und nur Dienstleistenden anzuraten, die dies bereits tun und auch bekanntmachen, wie dies Boddy (2019) anhand der Unternehmung Sophos zeigt (siehe Abbildung 5).

[4] Bspw. durch die Nutzung fremder WLAN-Verbindungen oder Netzwerke in (Förder-)Schulen.

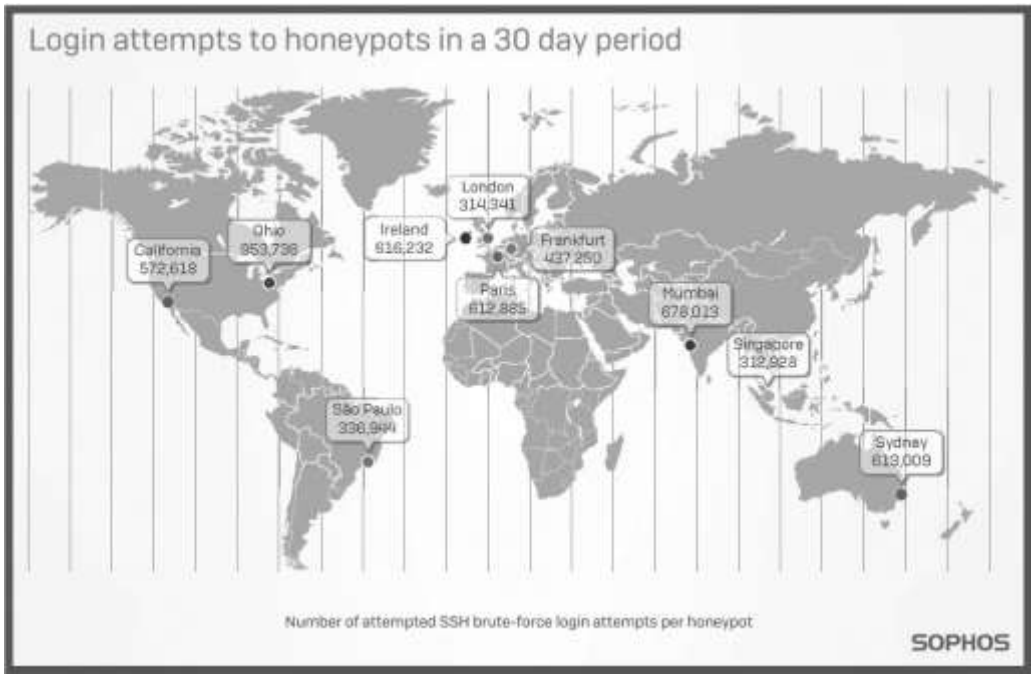


Abb. 5: Cyberangriffe auf Scheinrechnern (Boddy 2019, S. 3)

Der Schutz der privaten AnwenderInnen vor Cyberangriffen bleibt jedoch weiter schwierig und kaum lösbar, da Fachwissen und zusätzliche Infrastrukturen erforderlich sind. Um trotzdem einen wirksamen Schutz aufbauen und wirksame Schutzmaßnahmen implementieren zu können, ist es hilfreich, Cyberkriminelle auf ein mögliches Schadenspotential zu reduzieren.

2.1.5 Cyberkriminelle: eine Kategorisierung

Präventive Maßnahmen im Kontext von Cybercrime zielen darauf ab, IT-Sicherheitsrisiken zu mindern, um schädliche Folgen von Cyberangriffen abzuwehren. Um dies realisieren zu können, bedarf es nicht nur einer Auseinandersetzung mit Schutzmaßnahmen und möglichen Opfern, sondern auch einer analytischen Betrachtung der TäterInnen (van Elsbergen 2005). Und was den schulischen Kontext anbelangt, so haben gerade PädagogInnen nicht nur die Aufgabe, eine sichere Infrastruktur für die Internet(be)nutzung bereitzustellen, sondern auch die bewahrpädagogische Aufgabe, darauf zu achten, dass Jugendliche nicht zu kriminellen Handlungen verleitet werden.

Im Zeitalter der Digitalisierung, die eine ständige Bereitstellung von verständlichen Informationen für jede Zielgruppe möglich macht, ist es nicht zwingend, für einen Cyberangriff ein bestimmtes Alter zu haben, eine Programmiersprache zu beherrschen oder Maschinencode lesen und interpretieren zu können. So kam in der Studie „High Volume Cyber Crime and the Organization of the Police“ aus den Niederlanden (n = 47) heraus, dass 12- bis 24-Jährige zu 21,3 %, 25- bis 34-Jährige zu 17 %, 35- bis 44-Jäh-

rige zu 25,5 % sowie 45- bis 54-Jährige zu 10,6 % unter den identifizierten Cyberkriminellen vertreten waren (Leukfeldt, Veenstra & Stol 2013). Forschungsergebnisse der Studie „Account-Missbrauch im Internet“ (n = 599) verweisen hingegen auf ein Durchschnittsalter von 22 Jahren (Vick & Roters 2003). Und amerikanische Forschungsergebnisse zeigen, dass sich 26,6 % der befragten Cyberkriminellen in einer vierjährigen Collegeausbildung befanden, 13,6 % in einer zweijährigen Collegeausbildung, 11,8 % in der Mittelschule und 15 % in der Grundschule. Auch wissenschaftliche Abschlüsse waren mit dem Graduate school-master’s degree (4,7 %) und dem Graduate school-Ph. D. (2,6 %) vertreten (Woo 2003). Das heißt: Je höher der Bildungsgrad, desto geringer waren Cyberkriminelle in den Stichproben vertreten. Zu gegenteiligen Ergebnissen kommt allerdings der The Black Report 2018 (n =112), der auf 43 % Cyberkriminelle mit College-Graduates-Ausbildung, 32 % mit Postgraduate-Degree-Ausbildung und 19 % mit Programmierausbildung verweist (Pogue 2018). Ebenfalls bemerkenswert ist das Bundeslagebild Cybercrime 2016 (n = 20920), das nachweist, dass 14 % der Tatverdächtigen unter 21 Jahre alt waren, während der Gruppe der 21- bis 29-Jährigen 32 % zugeordnet werden konnten, aber auch nachweist, dass der Anteil von Personen höheren Alters (40- bis 49-Jährige: 16 %; 50- bis 59-Jährige: 9 %) geringer ist (BKA-SO51 2016). Ähnliche Bedingungen weist das Bundeslagebild 2017 (n = 22296) aus. Hier waren die unter 21-Jährigen mit 13 %, die 21- bis 29-Jährigen mit 32 %, die 30- bis 39-Jährigen mit 26 %, die 40- bis 49-Jährigen mit 16 % und die 50- bis 59-Jährigen mit 8,7 % vertreten (BKA 2017).

Cyberkriminelle sind sich der Unrechtmäßigkeit ihrer Interaktionen meistens bewusst und nutzen daher Verschlüsselungen und Verschleierungstechnologien für den Austausch von Informationen und Dokumenten. 92 % von ihnen nutzen dafür jedoch auch persönliche Zusammenkünfte, wobei 74 % der Befragten (n = 2000) diesen Weg des Informationsaustausches für sehr sicher halten (SINUS-Institut 2017), während sie (anscheinend) den digitalen Weg als zu unsicher einschätzen. Die indische Studie „Crisis and Collective Problem Solving in Dark Web“ von Kwon et al. (2017) zeigt, dass die akute Schließung von Web-Plattformen eine große Anzahl von direktiven Nachrichten „Interessierter“ nach sich zieht und dass Mitglieder hochmotiviert sind, neue Wege zu finden, um den Austausch weiter stattfinden zu lassen.

Das zunehmende Alter der NutzerInnen digitaler Technik und die damit verbundene Distanzierung von der Cyberkriminalität könnte auf menschliche Reife, beeinflusst durch Milieuveränderungen, wirtschaftliche Selbstständigkeit oder moralische Entwicklung (Harenski et al. 2011), hinweisen.

Cyberkriminell zu werden, erfordert ein Interesse an technischen Problemlösungen (Förtsch 2012), Selbstlernkompetenz (Bässmann 2015), kriminelle Energien, Zugang zu

Informationen (UBM 2018) und Technik sowie eine zielführende Motivation. Diesbezüglich sind im Rahmen dieser Arbeit folgende Aspekte von zentralem Interesse, die aufgrund dessen im Folgenden nacheinander beschrieben werden:

- Spaß an der Technik,
- Bedürfnis nach Herausforderungen,
- Selbstlernfähigkeit,
- Bedürfnis nach Aufmerksamkeit,
- finanzielle Vorteile.

Spaß an der Technik (Kilger, Arkin & Stutzman 2004)

Cyberkriminelle haben Spaß daran, Sicherheitsbarrieren zu überwinden. Die Studie von Tufin (2010) „Technologies“ in den USA zeigt, das 39 % der 1.000 befragten Jugendlichen Hacken „cool“ finden und 26 % in Großbritannien Spaß daran haben. Damit wird deutlich, dass der Spaß im Umgang mit der Technik möglicherweise einer legalen Kanalisierung bedarf. Hier sind pädagogische Hilfsangebote sinnvoll und erfordern von den Lehrkräften eine Expertise, die über derjenigen der Heranwachsenden liegen muss, damit unter anderem keine unautorisierten Zugänge genutzt werden und Cyberangriffe aus Infrastrukturen, die der allgemeinen Bildung zugeordnet sind, ausprobiert werden, deren Konsequenzen im Kapitel 2.1.4 beschrieben wurden.

Bedürfnis nach Herausforderungen (Pollino et al. 2006)

Unautorisierte Zugänge herzustellen ist für Cyberkriminelle ein mit Spannung verbundenes Erlebnis, wenn es bisher noch nicht bzw. auch anderen nicht gelungen ist. Gelingt es, die erste Sicherheitsbarriere zu überwinden, sorgt das für weitere Motivation. Kriminelle Handlungen werden so zu einer Art Sport (Vogelgesang, Wetzstein & Winter 2017), mit dem Ziel, auch die letzte Sicherheitsmaßnahme (last game level) aufzubrechen. Ist dies geschafft, verliert das ‚gesicherte‘ System seine Attraktivität und wird ‚nur noch‘ benutzt, um kriminelle Handlungen zu begehen (Fischer 1988). Insgesamt sehen 86 % der Cyberkriminellen die Herausforderung als Stimulus, sich Wissen anzureichern (Pogue 2018), wobei es auch motivational wirkt, dass der Erfolg mit Aufmerksamkeit verbunden ist (vgl. den Aspekt „Bedürfnis nach Aufmerksamkeit“).

Selbstlernfähigkeit (Newman 2009)

Sollen Systeme zweckentfremdet werden, müssen neue Informationen gesammelt, bewertet und zu vorhandenem Wissen hinzugetragen werden. Deshalb gilt: „A hacker is someone who enjoys exploring and learning about computer systems“ (Newman 2009, S. 28). Einfache Suchanfragen mit der Begriffskombination „darknet hacker forum“ bieten bereits einen ersten Einstieg in eine Netzwerktopologie, die im Verborgenen liegt

und bei der Suche nach Information im Internet Anonymität verspricht (Pfajfar 2019). Grimes (2017, S. 231) merkt hierzu an: „Ask all the arrested criminals who thought Tor or their anonymity service was providing absolute anonymity“. Sekundär entsteht so subjektives oder kollektives Wissen über ein IT-System, das für weitere Angriffe genutzt, adaptiert und auch zeitnah – als Ware – ausgetauscht werden kann (Pogue 2018). Neben Informationsquellen wie Datenbanken, die technische Schwachstellen hosten und auch aktualisieren (bspw. die Exploit Database), stehen den Cyberkriminellen eine Vielzahl von allgemein zugänglichen Hackerwebseiten zur Verfügung. “The Exploit Database is maintained by Offensive Security, an information security training company that provides various Information Security Certifications as well as high end penetration testing services. The Exploit Database is a non-profit project that is provided as a public service by Offensive Security” (Vitalwerks Internet Solutions 2018, S. 1).

Bedürfnis nach Aufmerksamkeit (Flenov 2005)

Jede in der Community von Cyberkriminellen gezeigte Zweckentfremdung, die noch unbekannt ist, bringt den AkteurInnen Aufmerksamkeit und Bewunderung, die auch durch die Öffentlichkeit durch die Zuschreibung von Innovativität reflektiert wird (Yar 2006). Etwas zu können, was andere nicht können, wird auch hier zum Alleinstellungsmerkmal (Steffens 2018), das jedoch durch die Weitergabe von InsiderInneninformationen und deren Veröffentlichung sehr schnell aufgelöst werden kann, da die Information auf diese Weise schnell an Verwertbarkeit verliert (Steinhaus 2018). Cyberkriminelle geben jedoch auch deshalb nur ungern Informationen weiter, da die Gefahr besteht, dass gefundene Sicherheitslücken von HerstellerInnen reflektiert und geschlossen werden. Bemerkenswert ist ebenfalls, dass selbst AnbieterInnen spezieller Sicherheitslösungen eigene Rankinglisten von Cyberkriminellen publizieren und damit für Aufmerksamkeit und Anerkennung sorgen (Kaspersky-Lab 2018).

Finanzielle Vorteile (Krah 2017)

Cyberkriminelle besitzen auch finanzielle Interessen (Pogue 2018; Matrosov, Rodionov & Bratus 2019): „Money has motivated criminals for longer than computers have been around, but the current state of computer security allows large sums of money to be stolen more easily and with far less risk than traditional, non-computer related crime“ (Grimes 2017, S. 213). Andere Analysen zeigen weiter auf, dass die Zahl der Cyberangriffe in der Finanzbranche um 65 % höher ist als der Durchschnitt über alle Sektoren hinweg, und bezieht sich damit auf den X-Force Financial Services Report 2017 des Software-Hauses IBM (IBM 2018b).

Neben den genannten Eigenschaften sind moralische Aspekte relevant (Chiesa, Ducci & Ciappi 2009), die durch eine Vermischung unterschiedlicher Motivationen und deren Bewertungen geprägt sind. So benennt Chantler (1996) unter anderen „Lamers“ und „Losers“, die kaum Anzeichen für intellektuelle Fähigkeiten besitzen und den Wunsch nach Profit, Rache, Diebstahl sowie Spionage haben. Hollinger (1988) weist zudem auf „Cracker“ hin, die teilweise von Zerstörungsabsichten getrieben sind. Rodgers (2000) nennt den Begriff „Information Warriors“, und Füllgraf (2015) und Samuel (2004) subsummieren unter dem Begriff Hacktivismus AkteurInnen, die meist aus politischen Intentionen heraus handeln (siehe Abbildung 6).

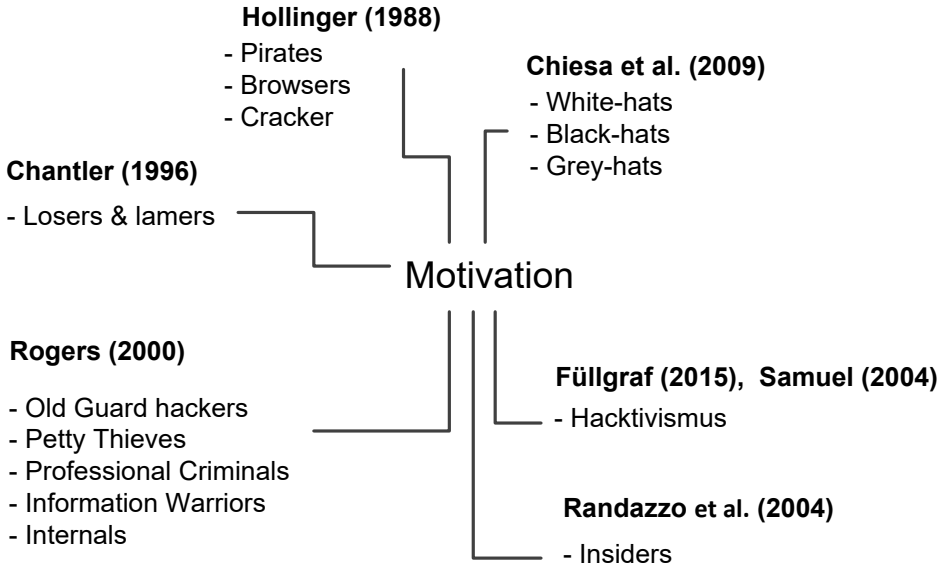


Abb. 6: Kategorisierung von Cyberkriminellen (nach Rodgers 2000; Chantler 1996; Hollinger 1988; Chiesa et al. 2009; Füllgraf 2015; Samuel 2004 und Randazzo et al. 2004)

Interaktionen aus der moralischen Perspektive als tadelnswerte Handlungen zu klassifizieren, ist jedoch kaum zielführend und „verschwimmt“ in der gesellschaftlichen Konformität, wie die Studie Norton Cyber Security Insights Report (2017) der Unternehmung Symantec Corporation im Kontext von Cybercrime zeigt. Im Rahmen dieser Studie wurden 21.549 Erwachsene in den Ländern Kanada, USA, Niederlande, Hong Kong, Frankreich, Italien, Großbritannien, Indien, Deutschland, Schweden, Österreich, Indonesien, Neuseeland, Singapur, Latein Amerika, Brasilien, Spanien, die Vereinigten Arabischen Emirate, China, Japan und Mexiko befragt, und es konnte aufgezeigt werden, dass 43 % der Befragten es für akzeptabel hielten, in bestimmten Fällen Gesetzesüberschreitungen zu begehen: „43% believe at least one type of cybercrime is always or sometimes acceptable“ (Symantec Corporation 2018).

Weitere für akzeptabel gehaltene Grenzüberschreitungen sind (ebd., S. 23):

- reading someone else's email without their permission (26 %),

- sharing things you know are not true on social media (21 %),
- using a false email or someone else's email to identify yourself online (21 %),
- using a false photo or someone else's photo to identify yourself online (20 %),
- putting software on someone's machine that allows you to spy and/or track them (20%),
- changing someone's status, posts or comments on social media without permission (19 %),
- posting inflammatory, threatening or sexually explicit comments or photos online (17 %),
- accessing someone's financial accounts without their permission (15 %),
- using someone else's credit card without permission to shop or book Online (15 %),
- stealing someone's personally identifiable information (15 %),
- allowing your device to be used to send spam, malware or attack other Computers (15 %),
- sending emails that trick people into giving out personal, financial or sensitive details (14 %).

Erfolgsversprechender als eine moralische TäterInnen-Kategorisierung ist im Sinne einer Optimierung der Sicherheit, transparent zu machen, über welche fachlichen Kompetenzen Cyberkriminelle verfügen. Denn nur so können wirksame Barrieren aufgebaut werden, die moralunabhängig Cyberangriffe verhindern können: „On the other hand, a defender needs to know the way of an attacker thinking and methodology, as well as about the tools, which attacker can use“ (Cekerevac et al. 2018, S. 86).

Hilfreich hierzu ist es, auf die Abstufungen von Dreyfus, McGuire und Dowling zurückzugreifen, die auf Arbeiten von Holt (2013) aufbauen und sich mit dem Kompetenzmodell von Dreyfus (2004) überlagern lassen, wie in der folgenden Abbildung 7 veranschaulicht wird.

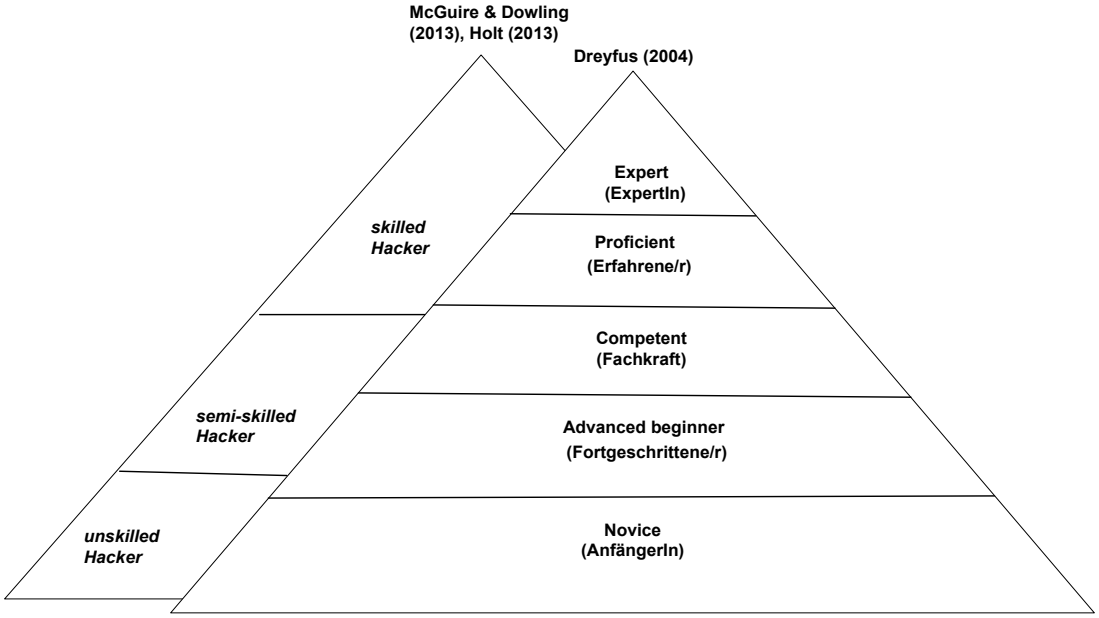


Abb. 7: Kompetenzmodell der Cyberkriminellen (nach Dreyfus 2004; McGuire & Dowling 2013 sowie Holt 2013)

Auf der Basis beider Modelle lassen sich drei formal unterschiedliche Niveaustufen der Kompetenz herausstellen, die den AkteurInnen zugeordnet werden können.

Stufe 1: unskilled Hacker - Novice

Eine Zuordnung nach dem Modell von Dreyfus sieht für die erste Gruppierung die Bezeichnung Novice (AnfängerInnen) vor, da hier erste Grundlagen für das Verständnis geschaffen werden. „The student automobile driver learns to recognize such domain-independent features as speed (indicated by the speedometer) and is given rules such as shift to 2nd gear when the speedometer needle points to 10“ (Dreyfus 2004, S. 177). Für McGuire und Dowling sind diese am wenigsten kompetenten Cyberkriminellen „unskilled hacker“ sowie auch „skript-kiddies“, deren Taxonomie von Rodgers (2000) übernommen wurde: „Newbies (who have limited skills and experience, and are reliant on tools developed by others, also known as ‚script-kiddies‘)“ (McGuire & Dowling 2013, S. 24).

Ein Beispiel hierfür liefern Biermann und Polke-Majewski (2020): Ein Schüler stellte aus dem Elternhaus heraus Politiker bloß, indem er durch Cyberangriffe erworbene private Informationen im Netz veröffentlichte und damit sein Rechtsbewusstsein plakatierte.

Die Gefahr, einem Angriff durch Skript-Kiddies zu erliegen, kann jedoch mit den meisten pragmatischen Sicherheitseinstellungen abgewendet werden. So verweist

Flenov (2005) darauf, dass bekannte technische Standards abgeändert werden können,[5] um Angriffe durch Skript-Kiddies zu vermeiden. Dass es dem Schüler trotzdem gelungen ist, derartige Informationen zu gewinnen, zeigt allerdings, dass Kenntnisse im Umgang mit digitalen Medien unabdingbar sind und teilweise einer Korrektur bedürfen.

Stufe 2: semi-skilled Hacker – Advanced beginner/Competent

Cyberkriminelle, die bereits Programme fertigen und/oder ändern und vorhandene Werkzeuge für andere Sicherheitsprobleme nutzen, können einer zweiten Kategorie, den „semi-skilled hackers“ (McGuire & Dowling 2013) oder „advanced beginners“ und „competent“ (Dreyfus 2004) zugeordnet werden. AkteurInnen dieser Kompetenzstufe können bereits die richtigen Methoden auswählen und Angriffsmethoden auf andere Angriffsobjekte adaptieren. Dazu erfolgt nicht nur ein Rückgriff auf konditioniertes Wissen, sondern es bedarf auch einer kognitiven Auseinandersetzung mit dem vorhandenen (unzureichenden) Wissen und der neuen Problemstellung.

Stufe 3: skilled Hacker – Proficient/Expert

Die dritte und für die Opfer von Cyberkriminalität gefährlichste Gruppe sind die „skilled hackers“ (McGuire & Dowling 2013) bzw. die AkteurInnen auf der Stufe „proficient/ expert“ (Dreyfus 2004). Diese Cyberkriminellen sind in der Lage, sich in neue technische Systeme einzuloggen, eigene Entwicklungen zu fertigen, unbekannte Sicherheitslücken zu finden und dadurch Ziele weltweit massiv angreifen zu können. Gemeint sind hier organisierte Cyberkriminelle, die auch im Auftrag anderer Regierungen arbeiten und ganze Infrastrukturen infiltrieren können. Auch Cyberangriffe, die von fachkundigen MitarbeiterInnen oder Systemverantwortlichen der angegriffenen Organisation auf den Weg gebracht werden, gehören hierzu. Eine Umfrage des Unternehmens PwC (2016) zum globalen Stand der Informationssicherheit zeigte, dass im Jahr 2015 34 % der Sicherheitsvorfälle von beschäftigten MitarbeiterInnen und 29 % der Vorfälle von ehemaligen Angestellten verursacht wurden. Dabei verweist die Studie „Complexity of Insider Attacks to Databases“ bezüglich der Komplexität von Cyberangriffen darauf, dass die Gefährlichkeit dieser AkteurInnen in dem InsiderInnenwissen über die Organisation und die vorhandene Sicherheitsinfrastruktur liegt und darin, dass ein Vertrauen nicht erst erarbeitet werden muss (Kul, Upadhyaya & Hughes 2016): „ We are dealing with trusted employees who have inside knowledge about the organization, security infrastructure, and information flow“ (Kul et al. 2016, S. 1).

[5] Ein Beispiel hierzu ist ein Portwechsel. Website-Aufrufe werden standardisiert auf dem Port 80 erwartet. Wird dieser Port verändert, kann die Website ohne Kenntnis des neuen Ports nicht aufgerufen werden.

Diese Darstellung macht deutlich, dass zwar nur eine grobe Einteilung der Cyberkriminellen möglich ist, diese jedoch unabdingbar wird, wenn Sicherheitsmaßnahmen zuschreibungsbezogen implementiert werden müssen.

Präventive Maßnahmen im Kontext von Cybercrime, die der Allgemeinheit zugänglich sind, sollten Schutzmaßnamen für die TäterInnenprofile eins und zwei bereithalten. Schutzmaßnahmen gegen Cyberangriffe von Skilled Hackers bedürfen hingegen umfangreichere Sicherheitsstrategien (Schumacher, Roedig & Moschgath 2003) und sind ohne entsprechendes Vorwissen in kürzester Zeit schwer vermittelbar. Deshalb wird im Folgenden auf die beiden ersten TäterInnenprofile fokussiert, da die Informationsquellen dieser HackerInnen ohne erheblichen Aufwand auch für AnwenderInnen zugänglich und mit deren Vorwissen nachvollziehbar sind (siehe Abbildung 8).

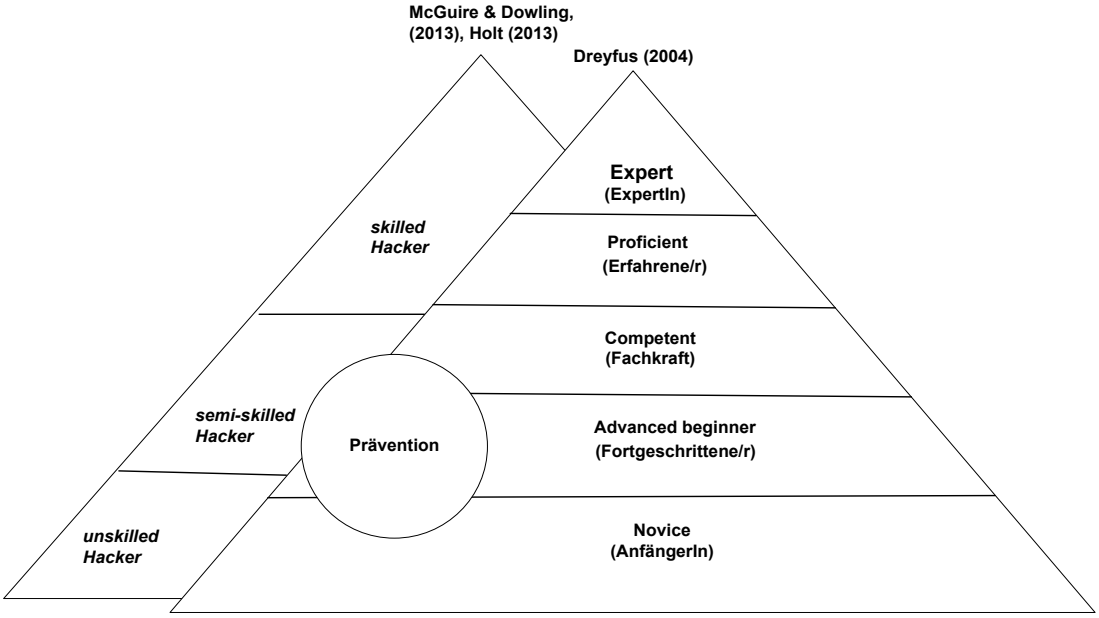


Abb. 8: Zielgruppe von Maßnahmen zur Prävention von Cyberkriminalität (auf der Grundlage der Kompetenzmodelle der Cyberkriminellen von McGuire & Dowling 2013; Holt 2013 und Dreyfus 2004)

Welche Cyberangriffe der unskilled bzw. semi-skilled HackerInnen (also der AnfängerInnen, Fortgeschrittenen und Fachkräfte) möglich werden und aktuell gesellschaftlich von Bedeutung sind (vgl. dazu Abbildung 1), wird im Folgenden ausführlich behandelt.

2.2 Arten von Cyberangriffen

Cyberangriffe lassen sich dem Bundesamt für Sicherheit in der Informationstechnik zufolge zum einen nach dem Angriffszweck und zum anderen nach dem Angriffsziel kategorisieren. Der Angriffszweck tangiert die Sicherheitsziele Vertraulichkeit, Integrität

und Verfügbarkeit (BSI 2012). Das Angriffsziel kann singulär, partikulär[6] oder generalisiert ausgerichtet sein. Nachfolgend werden Beispiele von Angriffstechniken aufgeführt, die singulär, partikulär oder generalisiert eingesetzt werden können, um die Verfügbarkeit, die Integrität oder die Vertraulichkeit von Information zu schädigen. Da der Umgang des Menschen mit der IT-Technik bei Cyberangriffen eine zentrale Rolle spielt, wird der Blick zunächst auf den Menschen als Angriffsziel gerichtet.

2.2.1 Angriffsziel: Der Mensch als Informationsträger (Social Engineering)

Social Engineering

Technische, durch Hard- oder Software implementierte Sicherheitsmaßnahmen dienen zwar dem Versuch, Systeme und Infrastrukturen langfristig vor Cyberkriminellen zu schützen, unterliegen jedoch letztendlich vermehrt der Interaktionen am Endgerät der Bewertung und Benutzung jeder/jedes einzelnen Nutzenden, sodass festzuhalten ist: „Information Security can no longer be protected through physical and technical means alone“ (Solms & Solms 2009, S. 126). Oder, wie es Bunker (2020, S. 17) ausdrückt: „A simple lapse in concentration and confidential data is sent to ‘the wrong Dave.’ With human error accounting for such a large proportion of data breaches, investment in technology to protect against this is vital“. Der Mensch wird damit selbst zu einem unkalkulierbaren Sicherheitsrisiko (Lipski 2009). Denn mangelndes Wissen, biogene Triebe[7] und konditionierte Verhaltensweisen[8] können von Cyberkriminellen ausgenutzt werden, um Cyberangriffe umzusetzen. Aufgrund dessen ist Social Engineering zu einem zentralen Aspekt geworden, wenn es um präventive Maßnahmen im Bereich Cybercrime geht (ebd.).

Um den Begriff Social Engineering einführend zu definieren, ist zunächst darauf hinzuweisen, dass es unterschiedliche Versuche gibt, den Begriff intersubjektiv zu definieren. Konstrukt-Definitionen der hier ausgewählten Autorinnen und Autoren zeigen, dass unterschiedliche Formulierungen genutzt werden, um den Begriff einzugrenzen. Hierzu einige Beispiele:

Lipski (2009, S. 1) definiert Social Engineering anhand der dabei eingesetzten Methoden: „Social Engineering benutzt Techniken der Beeinflussung und Überredungskunst zur Manipulation oder zur Vortäuschung falscher Tatsachen, über die sich ein

[6] Diese Form wird auch als targeted attacks (Rocha & Guarda 2018) bezeichnet.

[7] Gemeint sind Triebe mit lebenserhaltender Funktion.

[8] Dies sind Verhaltensweisen, deren Ablauf nicht mehr wahrgenommen wird.

Social Engineer eine gefälschte Identität aneignet“. Rouse (2018, S. 1) hingegen definiert Social Engineering aus dem Blickwinkel der Vorgehensweise: „Der Begriff ‚Social Engineering‘ bezeichnet eine Vorgehensweise, bei der die Schwachstelle Mensch ausgenutzt wird. Oft werden dabei Mitarbeiter eines Unternehmens mit einem Trick überredet, die normalen Sicherheitsvorkehrungen zu umgehen und sensible Informationen preiszugeben“. Und das Bundesamt für Informationssicherheit definiert Social Engineering als Methode wie folgt:

> „Social Engineering ist eine Methode, um unberechtigten Zugang zu Informationen oder IT-Systemen durch ‚Aushorchen‘ zu erlangen. Beim Social Engineering werden menschliche Eigenschaften wie z. B. Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität ausgenutzt. Dadurch können Mitarbeiter so manipuliert werden, dass sie unzulässig handeln. Ein typischer Fall von Angriffen mit Hilfe von Social Engineering ist das Manipulieren von Mitarbeitern per Telefonanruf, bei dem sich der Angreifer z. B. ausgibt als [Administrator]“ (BSI 2019, S. 1).

Social Engineering im Kontext von Cybercrime wird somit in dieser Arbeit definiert als eine kriminelle Strategie, die soziale und psychologische Eigenschaften sowie die Anfälligkeit für Manipulationsmöglichkeiten von Menschen unter Anwendung digitaler Technologien nutzt, um Menschen zu unautorisiertem und schädigendem Handeln zu veranlassen, sodass diese zu Opfern werden. Wie diese Definition im Detail taktikbezogen analysiert werden kann und welche Transformationen von Daten in Informationen eine beeinflussende Rolle einnehmen, wird nachfolgend aufgeführt und an dem Vektorenmodell von Frumento hervorgehoben (siehe Abbildung 9).

Die Angriffsvektoren nach Frumento (2017)

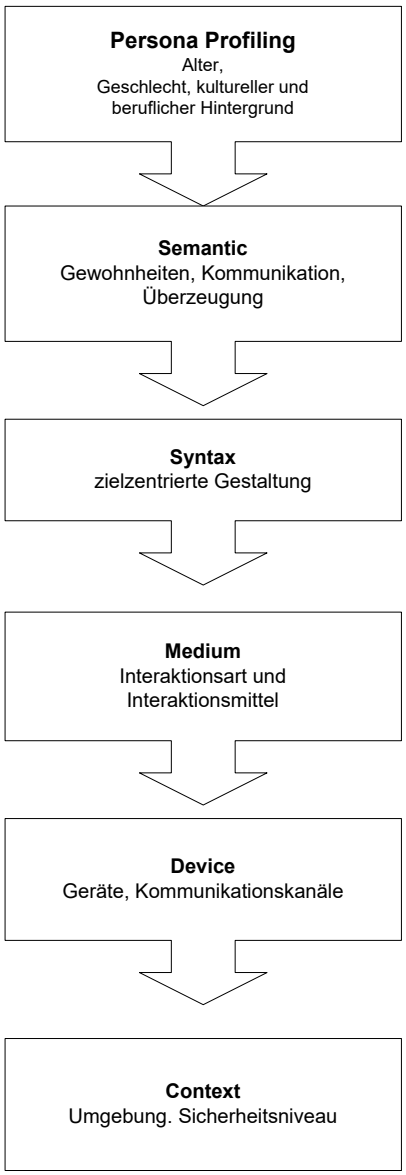


Abb. 9: Informationssequenz (Frumento 2017)

Frumento (2017) schlägt, wie in der Abbildung aufgezeigt wird, sechs Angriffsvektoren vor, die aufeinander aufbauen und jeweils erfüllt sein müssen, damit Social Engineering erfolgreich von Cyberkriminellen eingesetzt werden kann. Hierzu werden in den Angriffsvektoren eins und zwei gemäß Brönimann (1970) ermittelte Daten in Informationen gewandelt, um eine Erweiterung des Wissens vornehmen zu können (siehe Abbildung 10).

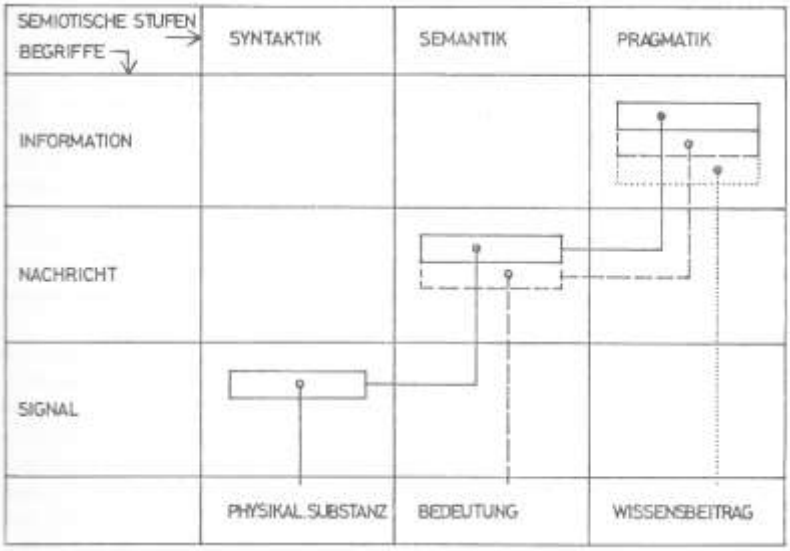


Abb. 10: Semiotische Ebenen des Informationsbegriffes (Brönimann 1970, S. 25)

Die von Datenschutzbeauftragten postulierte Definition von Information[9] ist im Kontext von Cybercrime unzureichend, da der Wissensbeitrag, den Brönimann beschreibt, unbeachtet bleibt. Watson, Mason und Ackroyd (2014, S. 205) beschreiben dies wie folgt: „This activity will enhance the previously acquired intelligence, enabling more educated and targeted attacks“, was Ozkaya (2018) als „information gathering“ bezeichnet. Biografische Daten wie Alter und Geschlecht, die soziale Rolle sowie der kulturelle Hintergrund werden von Cyberkriminellen gesammelt, um aus Daten Informationen zu generieren, sodass diese letztlich zielführend zum Social Engineering eingesetzt werden können (Frumento 2017). Das Individuum wird damit „sozial verortet“, indem es mit bestimmten „sozialen Substantiven“ adressiert wird (Stone & Hagoel 1978). Und damit werden bestimmte Prozesse sozialer Einbettung durch Zugehörigkeits-, Anerkennungs- und Vertrauenskonstruktionen in verschiedene Lebenswelten gesetzt (Höfer & Kraus 2005). Je mehr Informationen vorhanden sind, desto höher ist das Risiko, einen Cyberangriff zu erleiden, wie die folgende Abbildung 11 veranschaulicht.

[9] „Durch eine Kombination verschiedener Daten wird eine Beziehung hergestellt, die interpretiert werden kann. Die Daten werden zu einer Information“ (Czernik 2016).

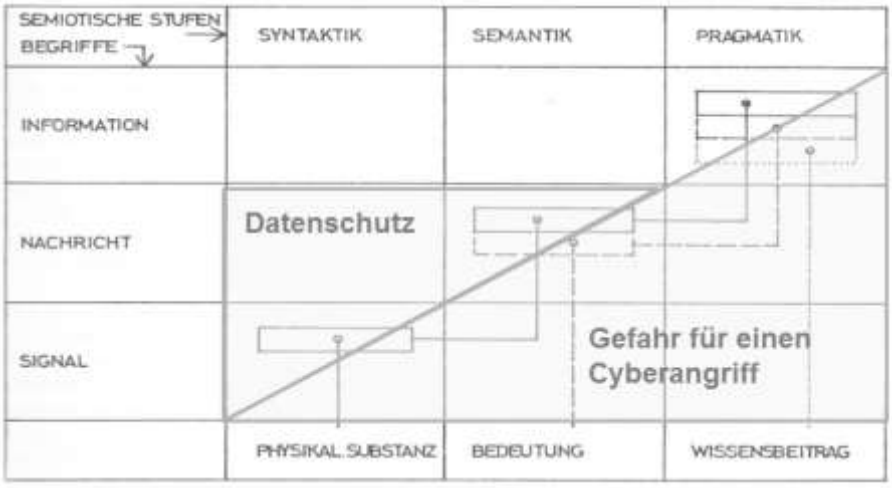


Abb. 11: Informationsdichte und Risiko (nach Brönimann 1970, S. 25)

Diese Differenzierung ist essentiell, da einige AutorInnen wie Ternès und Hagemes (2018) Daten zwar als Waren für die Wirtschaft, Geheimdienste und Kriminelle bezeichnen, damit jedoch im Sinne von Brönimann (1970) Informationen im abgehandelten Kontext fokussieren.

In der Praxis dürfte sich jedoch der Zugang zu persönlichen Daten der anvisierten Angriffsopfer schwierig gestalten, da Angaben zur Persönlichkeit, die primär von Interesse für Cyberkriminelle sind, kaum bereitwillig abgegeben werden und daher durch andere Erhebungsinstrumente wie zum Beispiel durch informelle Beobachtungen und Befragungen erhoben werden müssen.

Fileccia (2008) veranschaulicht hierzu anhand unterschiedlicher Beispiele, wie aus Daten zweckentfremdete Informationen abgeleitet werden können, indem Intelligenztests, Prognosen zur eigenen Lebenserwartung oder die Teilnahme an Gewinnspielen oder Warenprobentests angeboten werden. Aktuellere Entwicklungen zeigen Laufer und Meineck (2020) auf und verweisen auf den freizugänglichen Service(s) PimEyes[10], der bereits auf der Grundlage hochgeladener Fotos 900 Millionen Gesichter erkennt.

Einen zweiten Vektor stellt die *Semantik* dar, die sukzessiv zum ersten Vektor zu kontextualisieren ist. Dieser Analyserahmen schließt neben der Kommunikation und den Gewohnheiten der potenziellen Angriffsopfer deren Einstellungen mit ein. Hierzu lassen sich, so Cialdini (2017), Grundprinzipen des menschlichen Handelns wie Reziprozität, Commitment und Konsistenz, soziale Bewährtheit, Sympathie, Autorität und Knappheit den ausgewählten Opfern zuordnen und anschließend ausnutzen.

Die Reziprozität beschrieb Gouldner bereits im Jahr 1960 in drei Punkten:

- gegenseitiger Austausch von Befriedigungen,
- der Glaube an Gegenseitigkeit,

[10] https://pimeyes.com/en/

- die Gegenseitigkeit als moralische Norm.

Ajzen und Fishbein (1980, S. 25) merken hierzu im Kontext der Sympathie an: „We tend to like people who agree with us, to associate positive properties with objects or people we value, to attribute negative motives to people we despise, to help people we admire, and so on“.

Eine Transformierung von Daten in Informationen kann auch hier durch unterschiedliche Methoden erfolgen, mögliche Beispiele sind in der Tabelle 1 dargestellt.

Tab. 1: Beispiele für die Semantik mit Quellen und Ableitungen

Semantik	Reziprozität	Sympathie	Knappheit
Quelle	Eröffnungsgabe	Halo-Effekt[11]	künstliche Verknappung
Bedingung	Annahme der Gabe	Resonanz	fehlende Substituierbarkeit
Ableitungen	Gegengabe	Verhaltensänderung	Verhaltensänderung

Für den Kontext der Cybersicherheit kann dies aus der Tabelle 1 theoretisch entnommen und praktisch adaptiert werden. Ein Beispiel ist in der Tabelle 2 dargestellt.

Tab. 2: Künstliche Verknappung im Kontext von Cybercrime

Knappheit	Beispiele
künstliche Verknappung	Abschalten von WLAN-Netzen und Bereitstellen von kompromittierten WLAN-Netzen
Bedingung	WLAN-Netz ist nicht substituierbar und muss diesbezüglich genutzt werden.
Ableitungen	Übernahme der Kommunikation durch Cyberkriminelle, siehe Man-in-the-Middle Angriff, dargestellt in den Angriffsvektoren vier und fünf.

Einen dritten Angriffsvektor sieht Frumento (2017) in der *Syntax* und impliziert damit den Inhalt und die Gestaltung der Kommunikationsmedien. Bezüglich der verbalen Kommunikation verweist der Autor auf die zu wählende Stimmlage, die auch Mitnick und Simon (2003) adressieren und die Thomas (2014, S. 47) wie folgt weiter ausführt: „One must also be able to speak the lingo of the organization and know its key players“. Eine detaillierte Beschreibung legt Ozkaya vor, der zu diesem Angriffsvektor schreibt:

> „Learn how to ask the right questions. Make sure your body language is in sync with your words. Building rapport is not what you say; it’s how you say it. Rapport is established by matching and mirroring. Humans are the weakest point of any organization; the more you understand humans, their behaviors, and their history, the better you can hack them” (Ozkaya 2018, S. 64).

Dies kann gleichfalls für die Gestaltung und Implementierung von Inhalten in digitalen Medien adaptiert werden (siehe Tabelle 3).

[11] Der Halo-Effekt ist ein Überstrahlungseffekt, der auf Thorndike (1920) zurückgeht.

Tab. 3: Medien und deren Syntax

Medien	**Syntax**
E-Mails	vertraute Ansprache, Wortwahl und Inhalt
Medien	**Syntax**
Website	vertraute Ansicht der Website

Die Angriffsvektoren vier und fünf (*Medium* und *Device*) thematisieren die Wahl des Mediums und die technischen Voraussetzungen, um den Angriff ausführen zu können. Hierzu bedarf es der Kenntnis, über welches Medium (E-Mail, Internet) das Angriffsziel kommuniziert. Anhand des Alters kann beispielsweise probabilistisch die Techniknutzung abgeleitet werden, wie Huber (2012) es für E-Mails, SMS und Chats von Cyberstalking-Opfern ermittelt hat und wie es in der Tabelle 4 dargestellt ist.

Tab. 4: Alter von Cyberstalking-Opfern (Huber 2012, S. 148; Angaben in Prozent)

Alter	E-Mail (n = 248)	SMS (n = 127)	Chats (n = 41)	Verbreitung von Inhalten auf Websites (n = 20)
18–25 Jahre	15.2	16.1	34.4	30.3
26–35 Jahre	20.8	19.6	22.4	21
36–45 Jahre	23.6	26.6	27.6	24.3
46–55 Jahre	21.5	21.5	8.5	21.4
56–65 Jahre	11.8	10.8	7	3
> 66 Jahre	7	6.3	0	0

Sind die genutzten digitalen Medien bekannt, können von Cyberkriminellen unterschiedliche Methoden genutzt werden, wie nachfolgend beschrieben wird.

Verschiedene Formen des Social Engineerings und Schutzmaßnahmen gegen diese Angriffsmethoden

Im Folgenden werden folgende Formen des Social Engineerings behandelt, bevor auf weitere Angriffsmethoden eingegangen wird:

1. Phishing und Spear-Phising,
2. Watering-Hole-Angriff,
3. Media Dropping,
4. Dumpster Diving.

Methode 1: Phishing

Den Ursprung des Wortes Phishing sieht Purpura (2018) in dem Zeitpunkt, als HackerInnen in den USA Passwörter von ahnungslosen AOL-KundInnen scannten. Denn Phishing beschreibt eine Methode des Social Engineerings (Ioannou 2019), die gefälschte Inhalte zugänglich macht, um Zugangsdaten unautorisiert „abzufischen“ oder

Systeme zu kompromittieren. Phishing kann generalisiert (E-Mail an alle NutzerInnen im Internet) oder partikular (E-Mail an alle MitarbeiterInnen einer Organisation) eingesetzt werden.[12] Einen möglichen Ablauf beschreiben Roper, Grau und Fischer (2006, S. 215) wie folgt: „First of all, it provides confirmation that the account exists and that somebody is using it". Dabei machen digitale Verfahren, die die versandten E-Mails auf Gültigkeit prüfen und bei Unzustellbarkeit zurück schicken, ambivalent transparent, dass die E-Mail-Adresse nicht vorhanden ist, und zeigen weiter auf, welcher E-Mail-Server bei der Empfängerin bzw. dem Empfänger genutzt wird. Weiter führen die AutorInnen aus (ebd.): „The next, and probably most useful piece of information in the response, will be the signature". Interessant sind hier für Cyberkriminelle z.B. Abwesenheitsnachrichten, denn in diesen werden meistens Telefonnummern, Websites und Kontaktdaten von MitarbeiterInnen bekanntgegeben. Ebenfalls kann, wenn angegeben, die komplette Signatur kopiert und für weitere Kommunikationen, mit einem der/dem EmpfängerIn bekannten Namen, verwendet werden.

Indische Studien von Narahari und Shah befassen sich mit dieser Art des Social Engineering und zeigen auf, dass 67 % der Befragten häufig Phishing-E-Mails bekamen, in denen auch nach sensiblen Informationen wie Handynummern oder Bankdaten gefragt wurde. Studien wie die Untersuchung „Unpacking Spear Phishing Susceptibility", in die 1.200 Teilnehmende involviert waren, zeigen, dass 56 % der Teilnehmenden bei der Adressierung mit dem Vornamen als E-Mail-Empfangende und 38 % der Facebook-Nutzenden mit bereitgestellten Links auf gefälschte E-Mails interagierten (Benenson, Gassmann & Landwirth 2016). Und Narahari und Shah (2016) zeigten anhand ihrer Studie mit 100 Befragten, dass 48 % der Befragten ihre persönlichen Daten mit anderen Personen teilten, auch wenn sie diese nicht genau kannten. Weiter belegen die Autoren Benenson, Landwirth und Gassmann (2016) in der Studie „Exploiting Curiosity and Context" (n = 1600), dass 51 % der Studierenden, die dieser Form des Social Engineerings nicht folgten, angaben, die Absenderin bzw. den Absender nicht zu kennen, und dass 36 % erkannten, dass Inhalt und Kontext nicht zusammenpassten. Und Majlinda (2018) weist in ihrer kanadischen Studie „Cybersecurity Awareness and Beyond" nach, dass 78 % der Befragten sich der Risiken unbekannter Links bewusst sind, die E-Mails jedoch trotzdem anklicken. Majlindas Studienergebnisse belegen damit die von Barnes (2006) entwickelte Privacy Paradox Theorie, die dysfunktionales Verhalten transparent macht (Witteck 2011).

Welche Medien für derartige Cyberangriffe genutzt werden, fasst Schmitz (2020) im Blog „Phishing setzt auf den Leichtsinn der Opfer" wie folgt zusammen:

[12] Dies setzt natürlich voraus, dass die E-Mail-Adressen bekannt sind.

- die getarnte Rechnung,
- die Paketzustellung,
- die Dokument- oder Dateianlieferung,
- das gefälschte Fax,
- die gefälschte Sprachnachricht und
- die Online-Kontoüberprüfung/Aktualisierung“.

Erschwerend kommt hinzu, dass die Informationsüberflutung mittels der digitalen Medien am Arbeitsplatz durch die E-Mail-Kommunikation zugenommen hat.

> „Deutlich wird, dass nicht nur die Quantität, sondern vielmehr die Qualität der Informationen sowie die sich daraus ergebende Menge an Aufgaben von Bedeutung für das Erleben einer Informationsüberflutung sind. Auch das Wissen um den Einsatz effizienter E-Mail-Tools und Medienkompetenz spielen eine wichtige Rolle“ (Drössler et al. 2018, S. 79).

Spear-Phishing

Neuere Entwicklungen, aufgezeigt in der Studie „Unpacking Spear Phishing Susceptibility“ (Benenson et al. 2016), zeigen, dass Phishing verstärkt kontextbezogen zugeschnitten wird, sodass sich der Begriff Spear-Phishing etabliert hat (Ciampa 2011). Das Spear-Phishing zeichnet sich durch die Verwendung kontextspezifischer gefälschter Nachrichten aus, die auf spezifischem Wissen über Einzelpersonen und ihre Organisationen basieren. Hierzu werden E-Mails speziell auf die Inhalte einer Organisation zugeschnitten, damit Vertrauen entsteht und auch ausgenutzt werden kann (Gardner & Thomas 2014). Damit ist Spear-Phishing sowohl ein singulärer als auch ein partikulärer Cyberangriff auf die Vertraulichkeit, die Verfügbarkeit und die Integrität der zu schützenden Daten.

Schutzmaßnahmen gegen Phishing und Spear-Phishing

Um gegen Spear-Phishing und Phishing vorzugehen, bedarf es gezielter Sensibilisierungsmaßnahmen, in denen ein “gesundes“ Misstrauen aufgebaut und gefestigt wird. Beispiele können nur einen ersten Eindruck vermitteln, da Angriffe multivalent gestaltet werden können: „Often, phishing e-mails create a sense of urgency, claiming that the recipient’s account will be disabled if immediate action isn’t taken“ (Gardner & Thomas 2014, S. 95). Die Nutzenden müssen daher idealerweise jede gefälschte E-Mail erkennen und wissen, welche Schäden durch eine aktive Reaktion auf gefälschte E-Mails möglich werden. Simple Schutzmaßnahmen können eine telefonische Nachfrage bei der/dem „richtigen“ AbsenderIn oder die Bewertung der E-Mail-Adresse sein (Blass 2019). Pragmatischere Schutzmaßnahmen beschreibt Andric (2017, S. 192f.) wie folgt:

> „1 If you didn’t request it – don’t click on it!
>
> 2 Never download and run any file you don’t 100% trust!

3 Never enter sensitive information after following a link or popup.

4 Validate the link.“

Die Unternehmung AV-TEST zeigt hierzu auf der Grundlage einer im Zeitraum 2003-2013 durchgeführten Studie unterschiedliche Datentypen auf, die von Cyberkriminellen besondere Beachtung finden (Selinger 2013) und von den Anwendenden auch weiterhin misstrauisch als Anhang betrachtet werden sollten (siehe Abbildung 12).

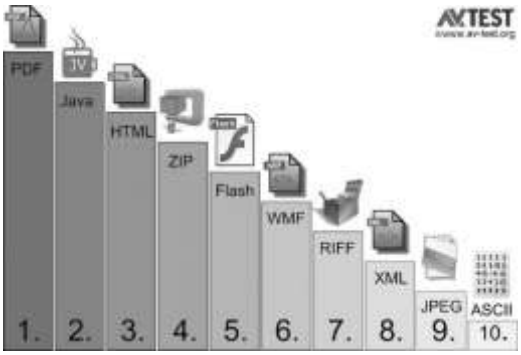


Abb. 12: Die Top 10 der am meisten genutzten Datei-Anhänge (Selinger 2013, S. 1)

Das Besondere hierbei ist, dass Anhänge wie pdf-Dateien, die vielfach genutzt werden, als besonders bedenklich eingestuft wurden.

Methode 2: Der Watering-Hole-Angriff

Ein Watering-Hole-Angriff beschreibt eine gezielte Attacke, bei dem die/der Angreifende eine kompromittierte Webseite (Ernst 2015), die das Interesse des gewählten Opfers fokussiert, implementiert (Krombholz et al. 2014). Gardner (2014, S. 31) beschreibt dies wie folgt: „Watering Hole attacks, while not as popular as phishing attacks, have increased in number over the past few years as users get better at spotting phishing attacks“. Dabei zeigt Ozkaya (2018, S. 419) auf, dass sensibilisierte Personen zwar einer gefälschten E-Mail misstrauen, einem gefälschten Link auf einer vertrauten Website jedoch nicht: „A wary person might, for example, purposefully avoid clicking a link in an unsolicited email, but the same person would not hesitate to follow a link on a website he or she often visits“.

Um Watering-Hole-Angriffe zu implementieren, werden meistgenutzte Webseiten ausfindig gemacht, durch Schadcode infiziert und dem Opfer als vertraute Webseite weiter zugänglich gemacht. Damit sind Watering-Hole-Angriffe besonders gefährlich (Rouse 2016). Erforderlich, um Watering-Hole-Angriffe möglich werden zu lassen, sind detaillierte Kenntnisse darüber, welche Websites genutzt werden und welche Sicherheitslücken der Webpräsenz vorhanden sind. Diese Informationen können durch den ersten Angriffsvektor gemäß Frumento (2017) für den Besuch vertrauter Webseiten

ermittelt werden. Inwieweit hierzu jedoch Websites[13] durch Schadcode infiziert werden können, hängt von den aktuell eingesetzten Technologien und deren Verwundbarkeit durch Sicherheitslücken ab.

Schutzmaßnahmen gegen Watering-Hole-Angriffe

Ein Schutz gegen Watering-Hole-Angriffe erfolgt primär, indem Daten, die das persönliche Surfverhalten beinhalten, geschützt werden und damit nicht zu Informationen für Cyberkriminelle werden können. Die ADV-Arbeitsgemeinschaft des Landes Nordrhein-Westfalen rät in ihrem Leitfaden zur Prüfung eines Internetauftritts deshalb, das persönliche Surfverhalten nach Benutzung des Browsers zu löschen, was durch gezielte Einstellungen im Browser leicht möglich sei (ADV-Arbeitsgemeinschaft 2016). Weiterhin können Zusatzprogramme für Browser installiert werden, die ein Behavioral Targeting[14] erschweren können (Moser 2017). Das Benutzen von infizierten Webseiten kann damit jedoch nicht verhindert werden. Eine Prüfung, ob die Webseite infiziert ist, kann jedoch mit entsprechender installierter Sicherheitssoftware erfolgen (Bradley 2013). Viele Sicherheitslösungen bieten eine Prüfung, bevor eine Website benutzt wird.

Methode 3: Media dropping

Media dropping, ebenfalls eine Methode des Social Engineerings, fokussiert menschliche Eigenschaften wie Neugier (Merten 2008) oder Hilfsbereitschaft (Pokoyski & Pütz 2014). Hierzu werden Datenträger mit entsprechendem Schadcode als Köder ausgelegt, in der Hoffnung, dass diese in vorhandene Systeme implementiert werden (Debo & Earley 2015). Cyberkriminelle hoffen darauf, dass die Finderin oder der Finder die erforderliche Neugier bzw. das Verlangen besitzt, den Datenträger zu nutzen (Willems 2015) oder seiner Besitzerin/seinem Besitzer zurückzugeben (Reimann 2015).

Media dropping ist damit eine partikulare Cyberangriffsform, die eine lokale[15] Wirkung haben kann. Tischer et al. (2013) zeigten in den USA, dass 297 USB-Sticks, die auf dem Campus der University of Illinois ausgelegt worden waren, von 87 % der Studierenden aufgenommen und von 45 % auch eingelesen wurden. Als Argumentation gaben 18 % Neugier an, und 68 % meinten, helfen gewollt zu haben. Dieser Argumentation kann durchaus gefolgt werden, da beschriftete USB-Sticks weniger (17 von 59) eingelesen wurden als beschriftete USB-Sticks mit Rücksendeadressenetiketten.

[13] Websites sind alle Webseiten des Internetauftritts, Webseiten sind einzelne Seiten (Reimann 2015).

[14] Behavioral Targeting ist eine Methode, um aus der Beobachtung des Serverhaltens Rückschlüsse auf die Interessen der Internetbenutzenden zu ziehen.

[15] Begrenzt ist dieser spezifische Angriff durch die Anzahl der Datenträger und die Zugangsautorisierung zum Auslegungsort.

Media Dropping ist eine Form des Social Engineerings (Debo & Earley 2015), die selten spezifische Angriffsopfer fokussiert. Vielmehr geht es hier vermehrt darum, eine breite (unbekannte) partikuläre Masse zu erreichen, die mit entsprechenden technischen Voraussetzungen, wie die eines freigeschalteten USB-Anschlusses, ausgestattet ist (Shackleford 2019).

Schutzmaßnahmen gegen Media Dropping

Um Angriffe durch Media Dropping zu verhindern, wenden viele Organisationen administrative Methoden an. Hierbei werden USB-Zugänge gesperrt oder durch Sicherheitsmaßnahmen überwacht (Reimann, 2018). Diese Maßnahmen behindern jedoch den Datenaustausch und erschweren damit die Ablauforganisation (Gut & Kammermann 2016). Denn da die Kompatibilität unterschiedlicher Systeme weitgehend abgesichert ist (Raulff & Lepper 2016), werden USB-Datenträger von den Anwendenden intensiv genutzt (Immler 2007) und diesbezüglich auch gefordert. Die Benutzung fremder USB-Speichermedien, ohne genau zu wissen, welche Inhalte auf dem Speichermedium vorhanden sind, bedarf jedoch einer kritischen Bewertung durch die jeweiligen Anwendenden und sollte vermieden werden.

Methode 4: Dumpster Diving

Dumpster Diving, ebenfalls eine Methode des Social Engineerings, fokussiert die Achtlosigkeit im Umgang mit Daten und Informationen in schriftlicher und digitaler Form. Cyberkriminelle untersuchen bspw. Papierkörbe auf verwertbare Inhalte, um an wichtige Informationen zu gelangen (Long, Wiles & Mitnick 2008). Das Fehlen von Vertraulichkeitsstufen auf ausgedruckten Dokumenten wird zu einem weiteren Risiko, wenn Dokumente entsorgt werden müssen, da sich die Vertraulichkeit des Inhaltes nicht immer aus dem gedruckten Text ableiten lässt (Reiss & Reiss 2009).

Eine andere kaum beleuchtete Methode ist das Auslesen alter Speichermedien[16], die letztendlich unachtsam entsorgt wurden und sich meist, für jedermann zugänglich (Computerhilfen.de 2012), auf Schrottplätzen befinden. Diese Art eines „junkyard looking“ bietet die Möglichkeit, umfangreiche Daten abzuschöpfen, die nicht mehr konvertiert werden müssen, da sie bereits im digitalen Format vorliegen (Abts & Mülder 2017).

Schutzmaßnahmen gegen Dumpster Diving

Der einfachste Schutz ist die Vernichtung der nicht weiter genutzten Speichermedien mit vertraulichen Daten durch Verfahren, die eine reversible Rekonstruktion unmöglich

[16] Gemeint sind bspw. Festplatten.

machen. Hierzu gibt es bereits entsprechende Standards für Papier[17] und digitale Medien[18], die berücksichtigt und eingehalten werden müssen, um ein Dumpster Diving abzuwenden.

Andere Formen des Social Engineerings

Social Engineering ist kein Phänomen allein der digitalen Welt, denn auch analoge Kommunikationsmittel wurden und werden genutzt, um Informationen unautorisiert abzugreifen. So glauben 67 % der Bevölkerung in den USA und Großbritannien[19], dass Cyberkriminelle durch das Beantworten von Fragen am Telefon an Informationen herankommen (Technologies Wombat Security 2017). Und 51 % der Teilnehmenden an einer Befragung in Indien (n = 100) gaben an, Phishing-Telefonanrufe zu erhalten (Narahari & Shah 2016). Darüber hinaus ist auch im Jahr 2019 jene Form des Social Engineerings immer noch aktuell, bei der Smartphonenutzende über Warnanrufe von angeblichen Supportmitarbeitenden mit tatsächlicher US-Support-Nummer berichten (Becker 2019). Diese Form, an sensible Daten von NutzerInnen zu gelangen, wird als Vishing bezeichnet (Gardner & Thomas 2014).

Resümee: Schutzmaßnahmen gegen Social Engineering

Angriffe durch Social Engineering nutzen mit vielfältigen Methoden menschliche Eigenschaften, Bedürfnisse, Vorlieben oder Verhaltensweisen aus und werden damit im Zeitalter des digitalen Wandels und in einer globalisierten, digitalen Welt zum Risiko. Technische Schutzmöglichkeiten gegen Social Engineering existieren kaum,[20] sodass die Medienkompetenz mit darüber entscheidet, ob riskante Interaktionen stattfinden oder nicht. Untersuchungen wie die „Study on the effectiveness of the security countermeasures against spear phishing“ schlagen diesbezüglich vor, die Simulation von Cyberangriffen als beste Interventionsmöglichkeit einzusetzen (Song, Seo & Lee 2015), und unterstreichen damit auch die Empfehlungen des BSI (2019) sowie der ISO 27001 (iso.org 2005) und damit letztendlich auch die Erforderlichkeit präventiver Interventionen. Dieser Empfehlung ist jedoch nicht bedingungslos zu folgen, wie das im Kapitel 2.3.7 angesprochene Privacy Paradox von Barnes (2006) zum Thema Phishing zeigt.

[17] DIN 66399

[18] US DoD 5220.22-M ECE

[19] Die Stichprobe bestand jeweils aus 1.000 Personen.

[20] Aufgrund dessen wurden sie hier auch nicht thematisiert.

2.2.2 Angriffsziel: Infrastruktur

Da Cyberangriffe auch ohne Social Engineering gegen technische Infrastrukturen gerichtet werden können, wird nachfolgend der Cyberangriff mit dem Angriffsziel Infrastruktur in seinen möglichen Angriffsformen thematisiert und dezidiert anhand von einzelnen Phasen behandelt.

Erste Phase: Informationsgewinnung (Singer 2019)

In der Phase der Informationsgewinnung werden alle Daten gesammelt, die verfügbar sind. Methoden des Social Engineerings wie Dumpster Diving, Water-Holing oder Phishing können genutzt werden, um unautorisiert an Daten zu gelangen, die für Cyberkriminelle im Bedeutungskontext zu Informationen werden (information gathering).

Suchmaschinen wie Google erlauben bereits mit zusätzlichen Suchparametern einen ersten digitalen Einstieg in die Datenerhebung (Dornfest, Rausch & Calishain 2003). Ein einfaches Beispiel hierfür ist die Eingabe bei Google: *allinurl: login site:XYZ.de*, die zur Folge hätte, dass alle Login-Webseiten der Webseite XYZ anzeigt werden.[21]

Piotrowski (2005) liefert in seiner Abhandlung: „Dangerous Google – Searching for Secrets“ eine umfangreiche Sammlung von möglichen Sucheingaben, die auch in der Abhandlung „No Tech Hacking A Guide to Social Engineering Dumpster Diving & Shoulder Surfing“ von Long et al. (2008) zu finden sind.

Einfacher ist es jedoch, Webseiten-Aufrufe im Hyperlink einfach zu kürzen, um an Informationen zu gelangen. Praktische Beispiele sind schnell umsetzbar, auch ohne spezielle Software oder Sachkenntnis. Folgendes Beispiel soll dies verdeutlichen: Auf der Website der Africa University wird der Hyperlink einer pdf-Datei: „http://www.africau.edu/images/default/sample.pdf“ wie folgt gekürzt: „http://www.africau.edu/images/“. Wird diesem Link gefolgt, zeigt die Website jedoch nicht nur ein Verzeichnis der Website an, sondern liefert gleichzeitig auch detaillierte Informationen wie die Webserver-Software Apache/2.4.29, das Betriebssystem Unix und die Verschlüsselungsversion OpenSSL/1.0 (siehe Abbildung 13).

[21] Dies wird als Google-Hacking bezeichnet (Goyal 2017).

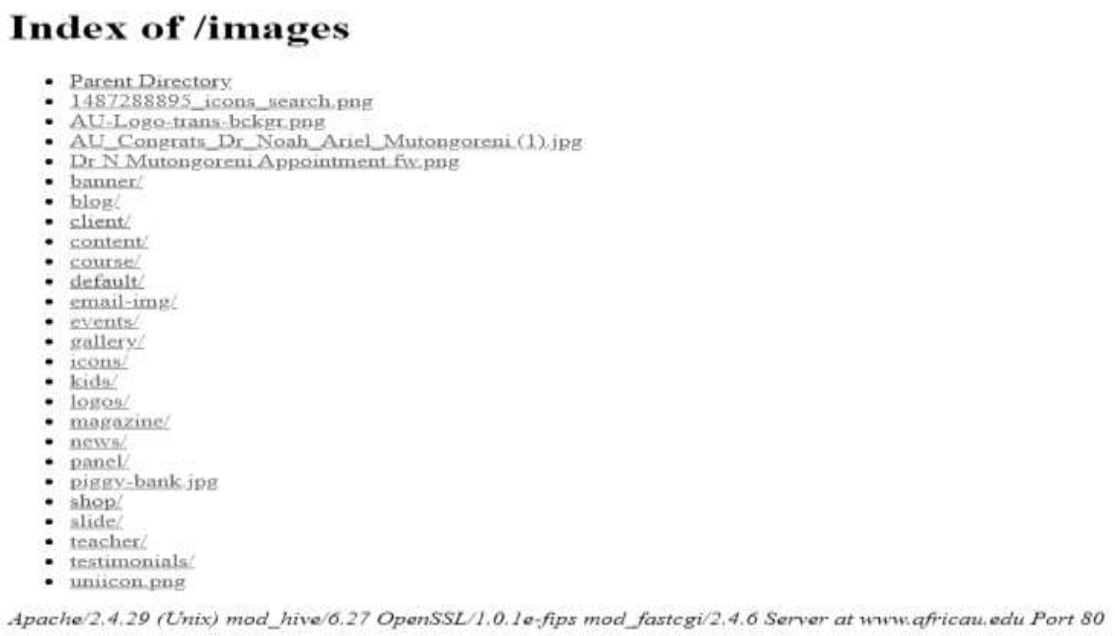


Abb. 13: Webseite der Africa University (Africa University 2019)

Andere Suchmöglichkeiten, generalisiert oder partikular, lassen sich durch besondere Suchmaschinen ermitteln, die darauf spezialisiert sind, sicherheitsrelevante Informationen herauszufiltern und transparent zu machen. Suchmaschinen wie Shodan (Matherly 2019) oder Censys (Durumeric et al. 2019) sind bereits in der Lage, digitale Daten von Infrastrukturen für jede/n Interessierte/n bereitzustellen. Und die Software SearchDiggity (Brown & Ragan 2019) bietet, komfortabel aufgeführt, eine Zusammenstellung der unterschiedlichsten Suchmaschinen. Dies alles findet im rechtskonformen Bereich statt, da die Suche nach (technischen!) Daten straffrei ist (Kuketz 2018).

Zweite Phase: Toolgebundene Informationsgewinnung

In der Phase der toolgebundenen Informationsgewinnung erfolgt der Einsatz von diversen Analysewerkzeugen. Aufbauend auf vorhandenen Informationen, wird die unterschiedlichste Software eingesetzt, die meist frei verfügbar ist und unter dem “Deckmantel“ des Penetrationstests als Ethical Hacking Tool von allen Gesellschaftsmitgliedern bereitgestellt und genutzt werden darf (EC-Council 2010). Sind Schwachstellen gefunden, können diese genutzt werden, um einen Angriff zu starten (Messner 2009).

In dieser Phase befinden sich die AkteurInnen noch immer im rechtskonformen Bereich, da keine Beeinflussung stattfindet. Denn: „Portscans und Pings sind nach Auffassung der Forschungsstelle Recht sowohl bei eigenen als auch an fremden Systemen aus rechtlicher Sicht zulässig, da hier kein Zugang zu besonders gesicherten Daten verschafft wird“ (Welp & Kaufmann 2018, S. 3).

Dritte Phase: Cyberangriff

In der Phase des Cyberangriffs wird der Versuch unternommen, ein System zu kompromittieren oder einen unautorisierten Zugang zu erwirken. In dieser Phase haben die AkteurInnen den rechtskonformen Bereich gemäß § 303b StGB verlassen.

Vierte Phase: Spuren verwischen

In der vierten Phase geht es darum, die Spuren zu verwischen. Dies ist nicht nur erforderlich, um als Verursachende/r nicht identifiziert werden zu können, sondern dient auch dazu, das kompromittierte System so lange wie möglich illegal nutzen zu können (Vladimirovich 2018).

Beispiele dieser Cyberangriffsform

Wie technische Umsetzungen von Cyberangriffen im Detail aussehen können, wird im Folgenden an mehreren Beispielen aufgezeigt, da diese auch Bestandteile der betrachteten Sensibilisierungsmaßnahme sind und als Simulation von Cyberangriffen fungieren. Denn: „To protect a computer and/or a computer system from hacker attacks, a defender needs to know the way of an attacker thinking and methodology, as well as about the tools, which attacker can use“ (Cekerevac et al. 2018, S. 86).

Im Folgenden werden daher relevante Cyberangriffe aus dem Zeitraum 2017-2020 vorgestellt, die in der Abbildung 1 bereits vorgestellt worden waren, da diese in präventiven Maßnahmen auf einer privaten Infrastruktur mit geringen Mitteln umgesetzt werden können. Als Beispiele dienen konkret:

1. Cyberangriffe gegen Passwort-Authentifizierungen,
2. Cyberangriffe nach der Erlangung des physischen Zugangs,
3. Cyberangriffe gegen WLAN-Infrastrukturen,
4. Cyberangriffe durch Man-in-the-Middle-Strategien,
5. Cyberangriffe durch Voice-Recording,
6. Cyberangriffe durch DDoS.

Beispiel 1: Cyberangriffe gegen Passwort-Authentifizierungen

Um Rechentechnik vor einem unautorisierten Zugriff zu schützen und die Benutzerin oder den Benutzer zu identifizieren, gibt es unterschiedliche Verfahren. Die Passwort-Authentifizierung ist eine der ältesten Authentifizierungsverfahren in der Computertechnik und umfasst unterschiedlichste Umsetzungsmöglichkeiten (Tsolkas & Schmidt 2017). Eine der einfachsten technischen Umsetzungen des Zugangs ist die Vergabe und Anwendung von Zugangskennungen (Accounts). Dabei setzt sich die Zugangskennung aus dem Benutzendennamen und dem (meist selbstgewählten) Passwort zusammen. Studien wie „On The Ecological Validity of a Password Study“ (n = 645) zeigen allerdings

auf, dass, je mehr Passworte genutzt werden, desto mehr Ähnlichkeiten dieser Worte zu bereits vorhandenen Passwörtern auftreten. 26,5 % der Teilnehmenden dieser Studie benutzten sogar gleiche Passwörter für IT-Zugriffe (Fahl et al. 2013). Und eine andere Erhebung, in die jeweils 1.000 US-AmerikanerInnen und EngländerInnen involviert waren, verweist darauf, dass nur 29 % der Teilnehmenden dieser Studie unterschiedliche Passwörter für unterschiedliche Anwendungen verwendeten (Technologies Wombat Security 2017). Zudem verweisen Shepherd und Archibald in ihrer auf Schottland bezogenen Studie darauf, dass BenutzerInnen zwar verneinen, für Passwörter Wörter aus dem Sprachgebrauch zu benutzen, es aber trotzdem tun.

> „During the experimental process, when participants were asked if they had used a dictionary password, the majority of those asked stated ‚no'. However, after analysing the requisite log files, there was a noted statistical significance which indicated that the majority of the participants had a common element in their password" (Shepherd & Archibald 2017, S. 4).

Das Länge des gewählten Passworts sowie die Wahl seiner alphanumerischen und symbolischen Zusammensetzung ist jedoch entscheidend, um nicht unautorisiert entschlüsselt zu werden (Grillenberger 2017). Denn wie Kelley et al. (2012) in den USA durch die Untersuchung von 12.000 Passwörtern auf ihre Widerstandsfähigkeit gegenüber unterschiedlichsten Passwort-Cracking-Algorithmen feststellten, lassen sich die Algorithmen zur unautorisierten Passwortentschlüsselung durch „technisches Training" stets verbessern. Damit wird es erforderlich, auf ein immer längeres und kryptisches Passwort zu achten. Werden allerdings durch digitale oder analoge Sicherheitsrichtlinien, und latent durch den Stand der Forschung, kryptische Passwörter vorgegeben, erzeugen diese meist Schwierigkeiten bei der Verwendung und produzieren diesbezüglich Missverständnisse. Gefundene Kompromisse (mehrstufige Passworterstellungsprozesse), wie in der Studie „A Spoonful of Sugar?" dargestellt, beeinflussen jedoch wiederum die Risiken der IT-Sicherheit (Shay et al. 2015) in Bezug auf die Vertraulichkeit.

Die Darstellung einer unzureichenden Passwort-Authentifizierung in präventiven Maßnahmen ist mit der Software Passware Kit Forensic möglich, die professionell in der Forensik eingesetzt wird (Reiber 2019). Dokumente der unterschiedlichsten Typologien, verschlüsselt mit unterschiedlichen Passwortstärken, können genutzt werden, um eine Brauchbarkeit der Passwortstärke mit dieser Software aufzuzeigen. Da die Software in der Lage ist, Rechenkapazitäten aus spezifischer Hardware wie Grafikkarten zu nutzen, ist sie ideal dazu geeignet, schwache Passwortstärken in kürzester Zeit aufzuzeigen.

Schutzmaßnahmen gegen Cyberangriffe gegen Passwort-Authentifizierungen

Das gewählte Passwort ist entscheidend für die Absicherung eines Systems. Diesbezüglich sind Passwörter so lang und so kryptisch wie möglich zu gestalten. Da jedoch

die Länge und die eingesetzte Kryptologie mit der Behaltensleistung der Nutzenden korreliert, wird empfohlen, Anfangsbuchstaben oder Zeichen von gelernten Sätzen als Passwort zu instrumentalisieren. Wichtig im Umgang mit sensiblen Daten ist weiterhin das Setzen eines Ablaufdatums der Passwort-Authentifizierung. Je sensibler die gespeicherten Daten sind, desto kürzer sollte der Authentifizierungs-Zeitraum gesetzt sein, wobei dies bei unterschiedlichen Anwendungen zeitlich differenziert zu gestalten ist. Die Passwort-Authentifizierung allein ist jedoch unzureichend, wenn der Zugang zur Rechentechnik nicht eingeschränkt ist, wie nun aufgezeigt wird.

Beispiel 2: Cyberangriffe nach der Erlangung des physischen Zugangs

Gelingt es Cyberkriminellen, einen physischen Zugang zur Rechentechnik herzustellen, haben diese die Möglichkeit, auf einem ungeschützten System jegliche Interaktionen durchzuführen. Bspw. können sie Schadsoftware installieren, die nicht nur das Passwort protokolliert, sondern alle Tastatureingaben abspeichert und damit der/dem Cyberkriminellen verfügbar macht. Der dafür notwendige Sourcecode ist in einschlägigen Programmiersprachen vorhanden (Khrais 2018) und im Internet frei verfügbar (Balci 2016). Beispiele in den unterschiedlichen Programmiersprachen sind:

- a simple Keylogger Program in C++ (Brighton 2010),
- a Keylogger Application Program in C# (Gul 2016),
- a Keylogger Java Source Code - Program Creek (Lampert 2017).

Weitere Möglichkeiten ergeben sich durch Implementierungen von unterschiedlicher HackerInnenhardware, die frei erwerbbar ist. Hierzu benutzen Cyberkriminelle sogenannte Keylogger, die per USB zwischen Rechner und Tastatur gesteckt werden, oder sie kompromittieren die Tastatur mit entsprechenden Bauteilen (Darms, Haßfeld & Fedtke 2019). Neuere Geräte wie der KeyGrabber Wi-Fi Premium sind sogar bereits in der Lage, diese Daten per WLAN zu übertragen (Schumacher & Barczok 2017).

Um Cyberangriffe nach der Erlangung eines physischen Zugangs in präventiven Maßnahmen vorzuführen, bietet es sich an, frei verfügbaren Sourcecode zu kompilieren und die Funktionalität vorzuführen. Eine weitere Möglichkeit besteht darin, Tastatureingaben mit dem KeyGrabber USB KeyLogger[22] zu tracken. Beide Simulationen können in präventiven Maßnahmen vorgeführt werden, da die Beschaffung durch Download und Kauf einfach umsetzbar und der Vorbereitungsaufwand gering ist.

Schutzmaßnahmen gegen Cyberangriffe durch die Erlangung des Zugangs

In unserer Gesellschaft sind viele Schutzmaßnahmen gegen Zugang bekannt, da viele Güter durch Verschluss gegen Diebstahl geschützt werden können. Gleiches gilt für die

[22] Diese Software ist im Handel frei erhältlich.

Rechentechnik, die diesbezüglich zu verschließen und nur einem autorisierten Kreis von Berechtigten zugänglich zu machen ist. Allerdings verwies Hallahan bereits im Jahr 2007 darauf, dass diese grundlegenden Schutzmaßnahmen Schwächen aufweisen: „Access control is the fundamental basis of computer security, but still remains a relative weakness in dealing with everyday threats, especially those posed by insiders“ (Hallahan 2007, S. 1). So zeigen Cyberangriffe aus dem Jahr 2019, dass der Zugangsschutz an Aktualität kaum verloren hat. Denn Jackpotting-Attacken, bei denen mithilfe von USB-Anschlüssen physisch geschaffene Zugänge zu Geldautomaten geschaffen wurden, führten zu unautorisierter Geldauszahlung (Cox 2019).

Beispiel 3: Cyberangriffe auf WLAN-Infrastrukturen

Digitale Erreichbarkeit wird bestimmt durch Digitalisierung, die eine Vernetzung, Verfügbarkeit und Kommunikation zu jeder Zeit und an fast jedem Ort möglich macht. Neue Technologien erlauben eine immer schnellere Datenübertragung, die genutzt wird, um immer größere Datenmengen unter mehreren NutzerInnen auszutauschen. Drahtlose Anbindungen sind zur Selbstverständlichkeit geworden und vereinfachen das Handling und verbessern die Wirtschaftlichkeit digitaler Produkte im Gegensatz zu punktuellen kabelgebundenen Anbindungen. Der Begriff WLAN ist zu einem Symbol für Freiheit, kabelloser Internetverfügbarkeit und Geräteunabhängigkeit geworden. Diese Technologie ist heute in fast jedem Haushalt in Deutschland vorhanden (Glos & Seemann 2013), besitzt jedoch eine meist unbekannte Ambivalenz, die sich in der Verfügbarkeit, der Sicherheit und der Informationsweitergabe zeigt. Denn um technische Informationen (im Rahmen der ersten und zweiten Phase eines Cyberangriffs) über vorhandene WLAN-Netze zu generieren, genügt bereits ein einfaches WLAN-Tracking (Wright & Cache 2015).

Dieses WLAN-Tracking ist eine Methode, die bereits marktwirtschaftlich genutzt wird, um Personenbewegungen und damit letztendlich das Kaufverhalten auf einfachem Weg operationalisieren zu können (Büring 2019). Hierzu werden WLAN-Signale genutzt, die (soweit das WLAN eingeschaltet ist) ständig auf der Suche nach WLAN-Verbindungen sind. Die Besitzerin/der Besitzer wird zwar nicht nach ihrem/seinem Namen getrackt, jedoch ist die Netzwerkadresse ihres/seines Gerätes (Mac-Adresse) für jede Person, die über entsprechendes Equipment verfügt, sichtbar. Auf diese Weise können beim wiederholten Eintritt in die Verkaufseinrichtung Werbeangebote „gerätebezogen“ zugeschnitten werden (Roeske 2018).

Für Cyberkriminelle kann WLAN-Tracking hingegen dazu dienen, erste Informationen zu erhalten, da Mac-Adressen meist herstellerInnenspezifisch sind und sich diesbezüglich mithilfe des Web-Services der Unternehmung[23] Coffer Group (2018) einem Gerätetyp zuordnen lassen. Im Kontext präventiver Maßnahmen kann die Funktionalität von Cyberangriffen gegen WLAN-Infrastrukturen mit der Open-Source-Software Kismet aufgezeigt werden, denn diese Software bietet umfangreiche Diagnosemöglichkeiten, die ein WLAN-Tracking der Handys der Teilnehmenden anzeigen, die WLAN aktiviert haben (Kershaw 2016).

Eindrucksvoller und auf WLAN-Tracking aufsetzend sind Karma-Attacken, die nicht nur Handys tracken, sondern darüber hinaus auch auslesen können, mit welchen WLAN-Netzen das Handy bereits verbunden war (Tiongson & Ryan 2015). Eine andere Methode, um sich einen Überblick über öffentlich sichtbare WLAN-Netze zu verschaffen, ist die Software Airdump-ng (Devine & Otreppe de Bouvette 2018). Mithilfe dieser Software können sich Cyberkriminelle (innerhalb der ersten und zweiten Phase des Angriffs) einen Überblick darüber verschaffen, welche WLAN-Netze vorhanden sind und welche Datenverbindungen in einem bestimmten Moment genutzt werden. Eine weitere Möglichkeit besteht darin, in der dritten Phase des Cyberangriffs den gesichteten WLAN-Datenverkehr zu stören, um primär WLAN-Kommunikationen zu blockieren und somit eine Neuverbindung[24] zu provozieren (Sorge, Lo Iacono & Gruschka 2013). Sekundär kann damit versucht werden, den Verbindungsaufbau (Vier-Wege-Handshake) abzuspeichern, um das beinhaltete Passwort entschlüsseln zu können (Reibold 2015). Gelingt es den Cyberkriminellen, die Daten (etwa aufgrund eines zu einfachen Passworts) zu entschlüsseln, kann die WLAN-Verbindung (Internet) später unautorisiert kontaktiert und der Internetanschluss unrechtmäßig genutzt werden. Auch dies kann im Rahmen präventiver Maßnahmen gut veranschaulicht werden, denn die Distribution Kali-Linux[25] bietet eine umfangreiche Sammlung unterschiedlicher Software an, die im Internet frei verfügbar ist und für die Darstellung genutzt werden kann.

Schutzmaßnahmen gegen Cyberangriffe auf WLAN-Infrastrukturen

Cyberangriffe auf WLAN-Infrastrukturen können gelingen, wenn die genutzte Passwortstärke sich als unzureichend erweist. Dieses Thema wurde bereits hervorgehoben, als die Passwortstärke thematisiert wurde, und trifft gleichfalls für die Implementierung von Passwort-Authentifizierungen in WLAN-Netze zu. Soll ein Tracking verhindert werden,

[23] Mit der Website http://www.coffer.com/mac_find/ kann anhand der Mac-Adresse der Hersteller bzw. die Herstellerin identifiziert werden.

[24] Diese Angriffe werden auch Deauthentication Attack-Angriffe genannt (Dickey 2015).

[25] Die Distribution ist verfügbar unter: https://www.kali.org.

ist es erforderlich, ein empfangsbereites WLAN am Endgerät abzuschalten. Störungen durch Deauthentication Attack-Angriffe können zwar erkannt und ihnen kann durch entsprechende Konfigurationen begegnet werden, für eine Störung durch Störsender gibt es jedoch keine Schutzmaßnahmen.

Diese Konstellation ist beachtenswert, wenn Infrastrukturen oder Videoüberwachung implementiert und digitale Medien (bspw. in Schulen) eingesetzt werden sollen. Eine Benutzung von freien Hotspots, die „WLAN für Alle“ bereitstellen, sollte kritisch betrachtet und auf ein Minimum beschränkt werden. Zudem sollten die Nutzenden wissen, dass durch die Nutzung von Hotspots die Erstellung von Bewegungsprofilen für jedermann möglich wird (Detken & Eren 2006). Daher sollten Hotspots nur mit Technologien genutzt werden, die eine hohe Verschlüsselung gewährleisten (Klau 2002) und Änderungen der Mac-Adressen zulassen.[26] Novelli (2019, S. 106) fasst dies wie folgt zusammen:

> „Regardless of the use of TOR, you should always use VPNs not just to be anonymous, but rather to protect yourself when you use an unsafe hotspot (like airports, hotels, bars etc.) or if you’re afraid your home router is monitored. All networks, and especially the public ones, may be traffic-monitored“.

Damit besteht auch die Gefahr, dass kopierte Websites unbemerkt durch Man-in-the-Middle-Strategien genutzt werden, auf die nun eingegangen wird.

Beispiel 4: Cyberangriffe durch Man-in-the-Middle -Strategien

Der Man-in-the-Middle-Angriff (MITM) ist eine Methode, in der zwei KommunikationspartnerInnen durch eine/n böswillige/n Dritte/n infiltriert werden (Young & Aitel 2004), sodass die Integrität der Daten gefährdet ist. Dabei ist beiden KommunikationspartnerInnen die Anwesenheit der/des böswilligen Dritten meist nicht bekannt bzw. bewusst.

Man-in-the-Middle-Angriffe benutzen unter anderem die Strategie des Social Engineerings, um Internetnutzende auf eigene Webseiten zu locken. Die Nutzenden gehen davon aus, dass die vorgefundene Webseite die ausgewählte Webseite (erste Phase) ist und geben daraufhin ihre persönlichen Daten ein, die dann von Dritten abgefangen werden. Die Implementierung ist einfach und mit wenigem Equipment herstellbar. Hierzu spannen die Angreifenden einen eigenen Hotspot auf (zweite und dritte Phase), der mit einem bekannten Namen eines anderen Hotspots des Opfers assoziiert werden kann. Das können Namen von Cafés oder Telekommunikationsanbietenden sein oder ausgelesene bereits verwendete Hotspots. Weiter klinken sich die Angreifenden zwischen dem eigenen Hotspot und der Internetverbindung ein, um die Nutzenden auf gefälschte Webseiten (Water-Holing) umzuleiten. Die Nutzenden glauben, auf der richtigen Webseite zu sein – sind es aber nicht. Kostenlose, fast überall verfügbare Hotspots bergen somit

[26] Dazu eignet sich bspw. die Software MAC Address Changer oder Pry-Fi.

auch hier ein deutliches Sicherheitsrisiko. Wirsing (2017) veranschaulicht dies anhand der besonderen Gefahr in Konferenzen, wenn “stimmige“ Namen wie Offiziell_Kongress2017 gewählt werden, und stützt sich dabei auf das Experiment der Unternehmung Avast (2016) im Flughafen von Barcelona im Jahr 2016, in das 2.000 Studienteilnehmenden involviert waren. Hier hatten Nutzende gefälschte Hotspots unwissentlich genutzt, um Informationen oder E-Mails abzurufen (siehe auch Tabelle 5).

Tab. 5: Interaktionen auf gefälschten Hotspots (Avast 2016, S. 1)

Anteil	Interaktion
61,70 %	searched information on Google or checked their emails on Gmail
14,90 %	percent visited Yahoo
2 %	visited Spotify

Oppliger (2016, S. 232) schlägt diesbezüglich die Benutzung von verschlüsselten SSL-Verbindungen als Schutzmaßnahme vor: „The best way to think about an MITM attack in an SSL/TLS setting is to consider an adversary that represents an SSL/TLS proxy server (or relay) between the user and the server“.

Leider sind selbst verschlüsselte Verbindungen gegen Man-in-the-Middle-Angriffe nicht immer immun und können, wie in der Studie von Marlinspike (2016) gezeigt wurde, mit Methoden wie SSLStrip oder SSLSniff sabotiert werden. Wie genau SSL-Verbindungen kompromittiert werden können, beschreiben AutorInnen wie Ristic (2014), Opplinger (2016) oder O’Leary (2019).

> „When Ettercap is used to perform a MitM attack against SSL/TLS-encrypted traffic, it replaces the site's original certificate with one generated by Ettercap. For the attack to succeed, the target is going to need to accept the presented certificate as valid, and so some effort needs to be paid to make the certificate realistic. The process of generating a certificate and a key for Ettercap is the same as the process for generating a certificate for a legitimate service. Start by creating a key for Ettercap“ (O’Leary 2019, S. 828).

Die Darstellung eines Man-in-the-Middle-Angriffs in präventiven Maßnahmen kann mit einer kompromittierten Website erfolgen, genauso wie durch ein „Aufspannen“ eines eigenen Hotspots mit allgemein bekanntem Namen oder dadurch, dass bereits genutzte Hostspots von den Teilnehmenden ausgelesen werden (Tiongson & Ryan 2015).

Schutzmaßnahmen gegen Cyberangriffe durch Man-in-the-Middle-Strategien

InternetbenutzerInnen sollten sich bewusst sein, dass Mobilität mit einer Netzinanspruchnahme Unbekannter verbunden ist. Ein Schutz gegen MITM ist die Verfolgung von Verbindungen anhand von IP-Adressen. Dieses Monitoring ist jedoch kompliziert und für viele AnwenderInnen kaum durchführbar. Ein weiterer Schutz liegt darin, präventiv aufzuklären, um die IT-Sicherheitsrisiken einschätzbar zu machen. Dabei ist nicht nur aufzuzeigen, wie die Daten übertragen werden können, sondern auch, welche Daten

übertragen werden können. Das können nicht nur Informationen in textueller Form, sondern auch in Form von Audio- und Videodaten sein, die im Homeoffice genutzt werden.

Beispiel 5: Cyberangriffe durch Voice-Recording

> „Suggestively, with the growing trend of software applications and the relatively poor user education, cybercrime through malicious software will continue to increase“ (Singh, Adeyemi & Venter 2019, S. 92).

Geräte, die analoge Sprache in digitale Daten synthetisieren können, besitzen die Funktionalität, Umgebungsgeräusche wahrzunehmen und zu verarbeiten. Das ist den Nutzenden zwar meistens bekannt und wird von diesen mitunter auch akzeptiert (Schillerhof 2018), allerdings besteht somit die Gefahr, dass Gespräche permanent übertragen und mitgehört werden (Day, Turner & Drozdiak 2019). Bemerkenswert ist jedoch, dass Informationseinrichtungen, die signalisieren, dass gerade eine digitale Aufnahme erstellt wird (LED), nur teilweise vorhanden sind und von den Nutzenden kaum wahrgenommen werden. So zeigt die kalifornische Studie „Somebody's Watching Me?“, dass nur 27,6 % der 98 befragten Nutzenden eine leuchtende LED, die eine aufnehmende Kamera signalisierte, registrierten (Portnoff et al. 2015).

Mobile Technik, die in die Lage versetzt wird, Umgebungsgeräusche zu verarbeiten, besitzt zudem kaum Vorrichtungen, die den Anwendenden eine Verarbeitung von Audiosignalen signalisieren. Eben dieser Umstand stellt jedoch ein Sicherheitsproblem dar. Denn bei einer genaueren Betrachtung mobiler Technik wird deutlich, dass heutige Notebooks in der Lage sind, Audiosignale aufzunehmen, da Empfangseinrichtungen wie Mikrofone bereits implementiert sind und in der Regel auch von den Betriebssystemen unterstützt werden. Diese Funktionalität ist latent und tritt erst in Erscheinung, wenn sie gebraucht wird.

Zur Darstellung von Cyberangriffen durch Voice-Recording in präventiven Maßnahmen bedarf es weniger Zeilen Sourcecode, um dies technisch realisieren und demonstrieren zu können. Cyberangriffe dieser Art werden durch entsprechende Programmschnittstellen zu Aufnahmegeräten möglich, weil das Betriebssystem (wie Windows) den Softwareentwickelnden derartige Programmbibliotheken (wie die winmm.dll) zur Verfügung stellt. Eine Implementierung eines Cyberangriffs durch Voice-Recording ist somit ebenfalls möglich, wie der hierzu von mir in Anlehnung an Kapfer (2014) entwickelte Programcode zeigt.

```
public partial class Form1 : Form
  {
    public Form1()
    {
      InitializeComponent();
```

```
        } [DllImport("winmm.dll", EntryPoint = "mciSendStringA", CharSet = Char-
Set.Ansi, SetLastError = true, ExactSpelling = true)]
          private static extern int mciSendString(string lpstrCommand, string lpstrRe-
turnString, int uReturnLength, int hwndCallback);
          private void Form1_Load(object sender, EventArgs e)
        {
          mciSendString("open new Type waveaudio Alias recsound", "", 0, 0);
          mciSendString("record recsound", "", 0, 0);
        }
        private void timer1_Tick(object sender, EventArgs e)
        {mciSendString("save recsound D:\\" + DateTime.Now.Hour.ToString() + "_" +
DateTime.Now.Minute.ToString() + "_" + DateTime.Now.Millisecond.ToString() +
".wav", "", 0, 0);
          mciSendString("close recsound ", "", 0, 0);
          mciSendString("open new Type waveaudio Alias recsound", "", 0, 0);
          mciSendString("record recsound", "", 0, 0);
        }
      }
```

Wird der hier abgebildete Code durch E-Mail übertragen (weil das Medium Text in einer E-Mail von der Firewall aufgrund der Praktikabilität nicht geblockt werden kann), auf einem Rechner gespeichert und kompiliert (weil der Compiler, der im Framework standardisiert vorhanden ist, nicht gelöscht wurde) und anschließend gestartet, schreibt das Programm bei vorhandenem Mikrofon alle aufgenommenen Umgebungsgeräusche so lange in eine Datei, bis das Programm beendet wird. Eine Signalisierung der Aufnahme durch das Betriebssystem oder die Hardware wie bei einer Webcam gibt es jedoch (bis heute) nicht.

Schutzmaßnahmen gegen Cyberangriffe durch Voice-Recording

Empfangseinrichtungen, die audiovisuelle Signale übertragen können, sind IT-Sicherheitsrisiken, die einer Beachtung bedürfen. Mechanische Abschaltmöglichkeiten sind kaum vorhanden, sodass das komplette Entfernen der Empfangsbauteile wie der Mikrofone erforderlich würde. Diese Entfernung ist jedoch nur teilweise möglich, sodass den Nutzenden evtl. nur radikale physische Maßnahmen wie Überkleben bleiben. Auch Überklebungen, z.B. von Kameras, gestalten sich jedoch schwierig, da der Ort der Implementierung nicht immer ersichtlich ist und das Eruieren des Orts eine intensive Auseinandersetzung mit der Hardware erfordert. Andere Schutzmöglichkeiten bestehen in bestimmten Einstellungen seitens des Betriebssystems oder in Spezialsoftware, der dann vertraut werden muss. Ausreichende Schutzmaßnahmen sind daher i.d.R. nicht vorhanden.

Beispiel 6: Cyberangriffe durch DDoS

Ein DDoS-Angriff ist eine weitere Angriffsform von Cyberkriminellen, die die Verfügbarkeit beeinflusst (Brenner 2010). Die Abkürzung DDoS steht für den Begriff Distributed-Denial-of-Service, der einen verteilten Angriff durch viele Cyberkriminelle auf ein dezidiertes Zielobjekt bezeichnet (Yu 2014). Ziel der Angreifenden ist es, einen bereitgestellten Dienst zu attackieren, um dessen Funktionalität einzuschränken oder – im Idealfall – den Dienst unautorisiert auszuschalten. Edwards (2020, S. 19) beschreibt dies so: „Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks are technical attacks to overload the website and server, restricting customers and staff from accessing the Internet“. Zielobjekte können Webpräsenzen wie Onlineshops, Online-Banking-Portale oder Informationsportale sein. Wie genau DDoS-Angriffe funktionieren, beschreiben Malik und Singh (2015) in ihrer Dokumentation „A Review: DoS and DDoS Attacks“. Aktuelle Betrachtungen dieser Angriffsform zeigen, wie präsent diese Bedrohung auch heute noch ist. Einen der bisher größten öffentlich bekannten DDoS-Angriffe hat die Online-EntwicklerInnenplattform GitHub seit dem Jahr 2018 zu verzeichnen: „Im Höhepunkt des Angriffs wurden laut einem Blogeintrag der GitHub-Macher 1,35 Terabit pro Sekunde gemessen[27], ein zweiter Angriff, nur kurze Zeit später, erreichte immer noch einmal 400 Gigabit pro Sekunde“ (Brien 2018). Damit zeigen derartige Entwicklungen, dass DDoS-Angriffe Angriffsformen sind, die noch immer funktionieren und auch genutzt werden. Husáket et al. (2018) beschreiben diese Situation ebenfalls und verweisen darauf, dass sowohl unkritische als auch kritische Infrastrukturen (siehe Tabellen 6 und 7) durch DDoS-Angriffe betroffen sein können, wenn Angriffsziele durch Scheininfrastrukturen (wie durch honeypots[28]) simuliert werden (Rist et al. 2018).

Tab. 6: Unkritische Systeme (Husák et al. 2018, S. 5)

Top-10 non-critical sectors			
Sector	**Scans (%)**	**DDoS (%)**	**Ratio**
Telecommunications	47.668	33.049	1.442
Internet Service Provider	43.404	40.583	1.069
(unknown)	7.717	22.505	0.343
Private Service	0.224	0.134	0.538
Internet Colocation Service	0.157	0.292	0.538
Education	0.154	0.388	0.397

[27] Ein Vergleich: Das Hochschulnetz des Rechenzentrums der Universität Würzburg verfügt über eine Bandbreite von zwei Gigabit pro Sekunde (Funken 2020).

[28] Honeypots sind Computersysteme, die gezielt AngreiferInnen anlocken können (Luber & Schmitz 2018).

Tab. 7: Kritische Systeme (Husák et al. 2018, S. 5)

Top-10 critical sectors			
Sector	**Scans (%)**	**DDoS (%)**	**Ratio**
Manufacturing	.053	.139	0.383
Government	.044	.064	0.693
Health	.024	.032	0.736
Finance	.014	.056	0.247

Diese Angriffsform ist nicht neu und kann, wie Khanal, Lynton und Dean (2013) in einer dokumentierten Simulation zu diesem Thema deutlich machen, mit einfachen Mitteln umgesetzt werden.

Private NutzerInnen, die sich im digitalen Netz bewegen, haben allerdings kaum Angriffsformen wie DDoS-Angriffe zu befürchten. Denn da diese Angriffe eine dauerhafte Präsenz mit statischen Adressbereichen (IP-Adressen) voraussetzen, meistens jedoch nur ein temporärer Zutritt zum Internet oder Ortsunabhängigkeit gewünscht wird, machen statische Adressbereiche bei privaten Nutzenden wenig Sinn.

Trotzdem bedarf es im Kontext von präventiven Maßnahmen einer Fokussierung auf dieses Thema. Denn erstens ist die für einen solchen Angriff geeignete Software (z.B. X4U Doser) frei verfügbar und auch downloadbar (Oliver 2018). Und zweitens kommen, wie Studien zeigen, gerade junge Leute einfach aus Interesse auf die Idee, DDoS-Angriffe auszuprobieren (Refsdal, Solhaug & Stølen 2015) und machen sich damit bereits gemäß § 303, Abs. 1 Nr. 2, Abs. 2 StGB strafbar (Haesen 2014). Ein Beispiel hierfür, das 2.000 PCs betroffen hat, führt Clough (2010) an. Und Spring (2005) verweist darauf, dass im Jahr 2004 ein 16-Jähriger mittels seines heimischen Computers diverse Computer angegriffen hat. Diesbezüglich sind also primär Eltern angesprochen, auf durch ihre Kinder bzw. Jugendlichen installierte Software zu achten und entsprechende Interaktionen ihrer Kinder zu überwachen. Um dies gewährleisten zu können, müssen sie jedoch IT-Sicherheitsrisiken kennen und eine Gewichtung eines möglichen Schadenpotentials vornehmen können.

In präventiven Maßnahmen kann durch die benannte Software X4U Doser diese Art von Cyberangriffen auf private Infrastruktur gezeigt und sogar ausgeführt werden, wenn sich die Betroffenheit auf die eigene Infrastruktur beschränkt.

Zusammenfassung

Cyberangriffe können unterschiedlich initiiert und ausgeführt werden. Die hier vorgestellten Varianten sind ein kleiner Ausschnitt der Angriffsformen, die im Zeitraum 2018-2020 besonders relevant waren (IBM 2018a; siehe auch Abbildung 1) und ohne detailliertes technisches Wissen nachvollzogen werden können. Denn bei der Darstellung von Angriffsmöglichkeiten in dieser Arbeit geht es nicht darum, technisch im Detail zu

beschreiben, wie Kriminelle einzelne Nutzende oder Systeme angreifen können, sondern darum, die Einfachheit, Kopierbarkeit und Abänderungsfähigkeit von Schadsoftware und die Lückenhaftigkeit von Technologien darzustellen, die im digitalen Zeitalter vorhanden sind und einen Schutz erforderlich machen. Herausgehoben werden soll auch, dass die Information im Kontext aller Schutzmaßnahmen ein essentiell zu schützendes Gut ist. Denn nur durch die Verletzung der Vertraulichkeit, Verfügbarkeit und Integrität der Informationen zu einem Zielsystem[29] ist ein Cyberangriff, wie oben beschrieben, überhaupt möglich. Alle Schutzmaßnahmen müssen somit darauf ausgerichtet sein, dass Informationen weitestgehend unzugänglich bleiben und nicht aus Daten generiert werden können. Diese Schutzmaßnahmen können metaphorisch als Zwiebelmodell betrachtet werden, das sich aus unterschiedlichen Schutzschichten zusammensetzt (Becker & Mahler 2019). Falsches Verhalten, das Informationen zugänglich macht, kann als ein Durchbruch der ersten Sicherheitsschicht betrachtet werden, und dieses wird durch eine zweite Sicherheitsschicht abzufangen versucht. Bunker beschreibt dies wie folgt: „The phrase that your security is 'only as strong as your weakest link' applies in either case“ (Bunker 2020, S. 19). „However, technology on its own is not enough to mitigate today's cyber risks "(ebd., S. 17). Damit zeigt sich die Komplexität von Cyberangriffen, die weiter zunimmt (Bhardwaj & Goundar 2020) und aufgrund dessen den Nutzenden dynamisch aktualisiertes deklaratorisches und prozedurales Wissen abverlangt.

2.2.3 Begünstigung von Cybercrime durch Komplexität

Die Digitalisierung schreitet voran, sodass sich alle Nutzenden digitaler Medien zwangsläufig mit Sicherheitsfragestellungen auseinandersetzen müssen. Sie bedürfen daher einer technischen Medienkompetenz, die das Thema IT-Sicherheit verbunden mit Schutzmaßnahmen ausreichend allokiert. Diese Kompetenz zu erwerben, ist jedoch mit Hindernissen verbunden, denn: „Die Komplexität global vernetzter Systeme zu beschreiben und die Gleichzeitigkeit ihrer Veränderungsdynamik in Worte zu fassen, ist ebenso schwierig, wie mit Sprache eine Beethovensymphonie zu vermitteln“ (Malik & Singh 2015, S. 12).

Schwierig scheint der sicherheitskonforme Umgang mit Computer- und Kommunikationssystemen zu sein, da diese bereits so komplex technisiert sind, dass das Verständnis der dahintersteckenden Technologie zunehmend schwer aufzubringen ist (Köhntopp, Pfitzmann & Fox 2001). Diese Komplexität äußert sich dabei nicht nur in der Vielzahl und Vielfalt der Elemente und Beziehungen eines abgegrenzten Systems, wie

[29] Mensch oder Technik

Vieweg (2015) es beschreibt, sondern umfasst auch die Beziehung zu anderen Systemen (Reichardt 2011). Kirchhof (2003) gliedert sie in a) Wahrnehmungskomplexität, b) Entscheidungskomplexität und c) Handlungskomplexität, stellt jedoch heraus, dass diese Formen aus unterschiedlichen Gründen ineinanderfließen und Cybercrime begünstigen können. Gestillte mediale Bedürfnisse, die sich nach Bonfadelli und Friemel (2017) in kognitive, affektive und soziale Bedürfnisse einteilen lassen, lassen wiederum neue Bedürfnisse entstehen, die durch Technologien zeitnah umzusetzen sind. Damit entsteht eine Verzahnung, die Kirchhof (2003) als Relationenkomplexität bezeichnet, da unterschiedlichste Medien zu multimedialen Endgeräten transformiert werden. Andere AutorInnen wie Gandolfi (2001) sehen die Komplexität als gering kontrollierbar, da diese bereits ausgelöste Eigendynamiken entwickeln würden, sodass Weyer (2009) und Vieweg (2015) lediglich die Kompliziertheit als auflösbar ansehen.

Komplexität besitzt jedoch auch marktwirtschaftliche Vorteile. Denn die von vielen Nutzenden unerwünschte technische Transparenz ist für einige Herstellenden unabdingbar geworden, um Produkte entwickeln zu können, die nicht mehr durch Reengineering verstanden und diesbezüglich nicht mehr zu kopieren sind, und in diesem Sinne Marktvorteile zu erhalten: „Without obfuscation, an attacker would search for the copy protection code inside the software and then remove it“ (Schrittwieser & Katzenbeisser 2011).

Weiterhin ist die Entwicklung derart rasant, dass sie kaum noch adäquat dokumentiert werden kann (Guggenberger 2010). Erfolgen diese Dokumentationen aber doch, sind sie nur noch den Entwickelnden vorbehalten (Warren 2017; Dittmar & Lörch 2018), denn alle Anbietenden möchten ihr Produkt so schnell wie möglich auf dem Markt platzieren, damit der Markt konkurrenzlos abgeschöpft werden kann (Keegan, Schlegelmilch & Stöttinger 2002). Glas, Pieler und Rosenstiel (2004, S. 17) konstatieren das wie folgt: „Parallel zur Optimierung des Geschäfts-Portfolios müssen alle Hebel angesetzt werden, um die operative Effizienz des Unternehmens auf das Niveau der besten Wettbewerber zu bringen“. Dazu werden vorhandene Ressourcen dezidiert verwendet, um die von den KundInnen gewünschte Funktionalität zu erreichen. Ressourcen, um sichere Systeme zu erhalten, sind jedoch wenig vorhanden und werden von den KundInnen auch kaum vor einem Kauf reflektiert. Implementiert wird im Bereich der Sicherheit also nur das Nötigste, wenn überhaupt (Bitkom 2017).

Die steigende Komplexität und die damit verbundene, aufgrund einer Eigendynamik bestehende Unübersichtlichkeit bergen zudem die Gefahr, unbewusst Sicherheitslücken in Systemen zu verankern. So zeigt das BSI (2012) auf, dass sich bei der heutigen Komplexität der IT Schwächen prinzipiell nicht vollständig vermeiden lassen. Kommerzielle AnbieterInnen von Sicherheitslösungen nutzen diese Situation und entwickeln unterschiedliche Sicherheitsarchitekturen (Scheer 2000), die durchaus einen Grundschutz

darstellen, mit dem sich 45 % der von Narahari und Shah (2016) in Indien Befragten sicher fühlen. Das Durchdringen der Komplexität wird damit jedoch nicht erreicht, sondern lediglich, wenn überhaupt möglich, delegiert.[30] Um sich wirksam schützen zu können, ist es jedoch wichtiger, die Kompliziertheit von Cyberangriffen durch eigene Erkenntnisprozesse aufzulösen, die Riedl (2000) in einer stilisierten Metapher darstellt (siehe Abbildung 14).

Abb. 14: Metapher der Merkmalszusammenhänge von Cyberangriffen (Riedl 2000, S. 73)

Und die Mocker (2009) wiederum in einem IT-Komplexität-Abhängigkeitsmodell (siehe Abbildung 15) visualisiert.

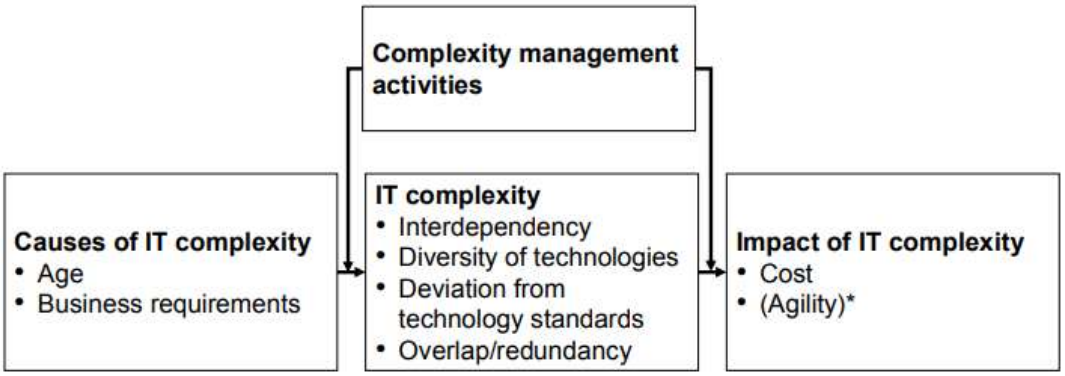


Abb. 15: IT-Komplexität-Abhängigkeitsmodell (Mocker 2009, S. 7)

Bei der Vermittlung dieser Sachverhalte im Rahmen von Präsentationen ist laut Long et al. (2008) Folgendes zu beachten:

- Es sollte eine einfache Sprache mit Vokabular von Nicht-IT-Mitarbeitenden verwendet werden, sodass auf Akronyme verzichtet wird.
- Pro Folie sollen nicht mehr als 15 Wörter verwendet werden.
- Da das Thema IT-Sicherheit trockener Unterrichtsstoff ist, ist Humor wichtig.

[30] Um die Komplexität aufzulösen zu können, werden Heuristiken eingesetzt (Meier 2008), die auch zur Bekämpfung von Cyberangriffen genutzt werden (Sowa 2017).

Damit ist allerdings, wenn überhaupt, eher die Kompliziertheit allokiert als die Komplexität.

Das Erkennen der Komplexität und der damit verbundenen Kompliziertheit ist bereits in der prädezisionalen und präaktionalen Phase essentiell, damit bereits vor dem Kauf über mögliche Ambivalenzen nachgedacht werden kann. Denn gekaufte Produkte (aktionale Phase) wie Spielzeuge wie die Puppe Cayla, die durch die Bundesnetzagentur als unautorisierte Sendeeinrichtung klassifiziert wurde (Kühl 2017), oder Fernseher, die Gespräche ins Internet übertragen (Gruenwald 2017), zeigen, dass in der Kaufentscheidung i.d.R. der Mehrwert digitaler Produkte im Fokus steht und eine mögliche erkennbare Ambivalenz durch Komplexität und Kompliziertheit verdeckt ist.

> „Die Uneinsehbarkeit der komplexen Datenverarbeitungs- und Datenverbreitungsprozesse innerhalb vernetzter informationstechnischer Systeme begünstigt eine Situation, in welcher für Endnutzerinnen und Endnutzer digitaler Medien gänzlich undurchsichtig wird, welche persönlichen Daten erhoben, wie sie verarbeitet und an wen sie weitergegeben werden“ (Hagendorff 2019, S. 97).

Dabei hat sicherheitskonformes Verhalten im Umgang mit digitalen Medien einen entscheidenden Einfluss auf den Mehr- und Kehrwert digitaler Produkte. Korrekturbedürftiges Verhalten bedarf jedoch nicht nur einer Reduktion der Kompliziertheit, sondern gleichfalls einer Auseinandersetzung mit den vorhandenen theoretischen Modellen, die eine Verhaltensänderung in Aussicht stellen. Das alleinige Vertrauen in technische Systeme und Infrastrukturen, wie Weissinger (2017) es im Kontext von Cybercrime beschreibt, ist somit unzureichend und keine Lösung.

Diesbezüglich ist die nachfolgende Abhandlung der unterschiedlichsten Theorien und Forschungsergebnisse im Kontext Cybercrime hilfreich.

2.3 Erklärung von sicherheitskonformem Verhalten im Kontext von Cybercrime

Präventive Interaktionen erheben idealerweise den Anspruch, erforderliche Verhaltensänderungen zu bewirken, wenn das Verhalten bislang nicht sicherheitskonform[31] war. Diesbezüglich bedarf es einer Fokussierung auf vorhandene Theorien, deren Prädiktoren eine solche Verhaltensänderung in Aussicht stellen. Diese Prädiktoren sind in den unterschiedlichsten Theorien zu finden, von denen einige im Folgenden behandelt werden, da diese in der Konzipierung der in dieser Studie auf ihre Wirksamkeit evaluierten präventiven Maßnahme eine essentielle Rolle spielten. Konkret werden die folgenden Modelle nacheinander ausführlich vorgestellt:

- das Elaboration-Likelihood-Modell (ELM),

[31] Normen ergeben sich auf dem Grundschutz des BSI oder der ISO 27001. Einige AutorInnen sprechen auch von der Cyber-Hygiene (Neigel et al. 2020).

- das heuristisch-systematische Modell (HSM),
- die Theorie der Schutzmotivation (PMT),
- die Theorie der Selbstwirksamkeitserwartung (SET),
- das Konstrukt der Kontrollüberzeugung (LoC),
- die Einstellungstheorie (FAT),
- die Theorie des überlegten Handelns (TRA),
- die Theorie des geplanten Verhaltens (TPB),
- das transtheoretische Modell der Verhaltensänderung (TTM).

Anschließend werden diese Erklärungsmodelle im Kontext von Cybercrime mit Bezug zum aktuellen Forschungsstand empirisch unterfüttert.

2.3.1 Das Elaboration-Likelihood-Modell (ELM)

Der zentrale Begriff im Elaboration-Likelihood-Modell ist die Persuasion (in diesem Fall im Sinne von Überzeugung gemeint). Persuasion bezieht sich auf Konstrukte, in denen Verhalten durch Botschaften modifiziert wird (von Roehl 2005). Petty und Cacioppo implizieren hierzu zwei mögliche Wege, die sie als Routen bezeichnen:

> „This theory, which we have called the Elaboration Likelihood Model (ELM), outlines two ‚routes to persuasion'. One route is based on a careful and thoughtful assessment of the central merits of the position advocated (central route). The other is based on some cognitive, affective, or behavioral Preface cue in the persuasion context which becomes attached to the advocacy or allows a relatively simple inference as to the merits of the position advocated (peripheral route)" (Petty & Cacioppo 1986, S. 7f.).

Je höher die Motivation und je eingehender die Informationsverarbeitung ist, desto wahrscheinlicher erfolgt die Zuordnung zur zentralen Route. Je höher die Motivation und je flüchtiger die Informationsverarbeitung ist, desto wahrscheinlicher erfolgt die Zuordnung zur peripheren Route. Wobei Felser (2015) darauf hinweist, dass Petty und Cacioppo beide Routen auch als Wege der Überredung beschreiben, wobei jeweils zentral und peripher zu unterscheiden ist.

Helisch und Pokoyski (2009) fassen in Anlehnung an Petty und Cacioppo im Kontext der Security Awareness die zentrale und die periphere Route, hier auch als Wege bezeichnet, grafisch zusammen (siehe Abbildung 16) und verweisen darauf, dass die zentrale Route in bestimmten Situationen zu einer dauerhaften und stabilen Einstellungsänderung, die periphere Route hingegen nur zu einer instabilen Veränderung der Einstellung führt.

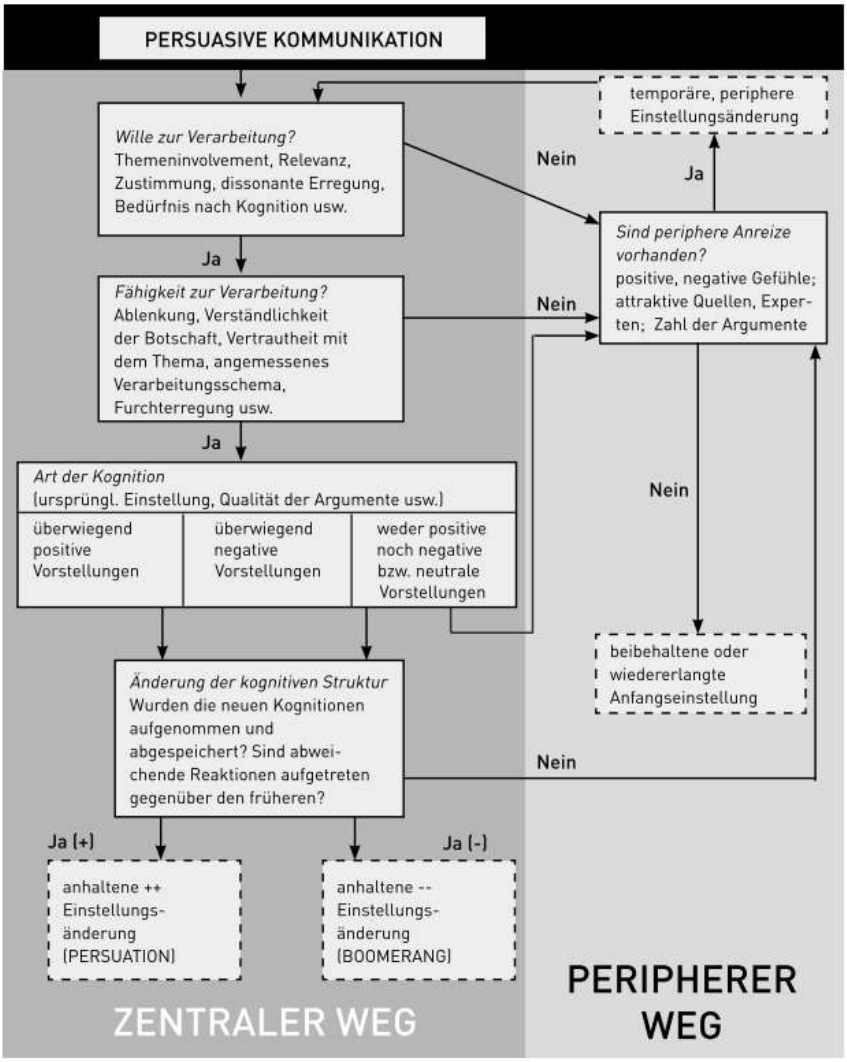


Abb. 16: Persuasive Kommunikation (nach Petty & Cacioppo 1986 aus Helisch & Pokoyski 2009, S. 67)

Auffällig in der Abbildung ist jedoch, dass der Begriff Persuasion durch ‚Persuation' und die Formulierung ‚anhaltende Einstellungsänderung' durch ‚anhaltene Einstellungsänderung' ersetzt wurde, sodass hier von Rechtschreibfehlern ausgegangen werden muss. Wichtiger ist es jedoch, hervorzuheben, dass, wie Jonas, Stroebe und Hewstone (2014) konstatieren, die RezipientInnen die Argumente, die in einer Botschaft enthalten sind, kritisch überprüfen, was sowohl eine Verarbeitungsmotivation als auch eine Verarbeitungsfähigkeit voraussetzt. Ist eine gründlichere Auseinandersetzung mithilfe kognitiver Prozesse möglich, erfolgt die Wegzuschreibung einer zentralen Route. Ambivalent hierzu adressiert die periphere Route der Persuasion eine geringere Motivation, sich mit Botschaften eingehender zu befassen. Petty und Cacioppo weisen in diesem Zusammenhang darauf hin, dass Einstellungsänderungen, die auf einer umfassenden Ausarbeitung von problemrelevanten Argumenten beruhen, beständiger, widerstandsfähiger und verhaltensprädiktiver sind als Einstellungsänderungen, die auf einfachen Hinweisen beruhen: „Attitude changes based on extensive elaboration of issue-relevant arguments

(central route) are postulated to be more persistent, resistant, and predictive of behavior than attitude changes based on simple cues (peripheral route)“ (Petty & Cacioppo 1986, S. 24).

Detailliert bezogen auf Argumente und Expertise ist die Studie von Petty, Cacioppo und Goldman (1981) (siehe Abbildung 17), welche die Wechselwirkung zwischen a) der persönlichen Relevanz und Expertise sowie b) der persönlichen Relevanz und Qualität der Argumente auf die Einstellung nach der Kommunikation aufzeigt.

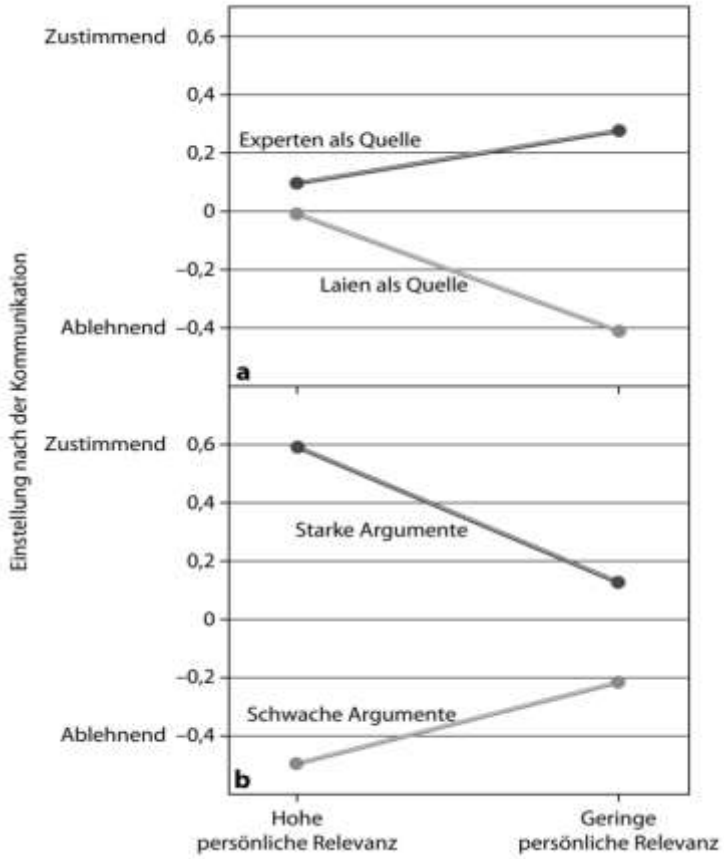


Abb. 17: Wechselwirkung zwischen persönlicher Relevanz und Expertise der Quelle und der persönlichen Relevanz und Qualität der Argumente (Jonas et al. 2014, S. 242; in Anlehnung an Petty, Cacioppo & Goldman 1981)

In dieser Studie wird deutlich, dass ExpertInnen in Interaktionsprozessen eher zustimmend begegnet wird, während dies für LaiInnen nicht gilt, die eher auf Ablehnung stoßen. Weiterhin führen starke Argumente, die von ExpertInnen präsentiert werden, zu einer Verstärkung der Einstellungsänderung. Damit wird deutlich, dass Wirkungen, die eine Verhaltensänderung fokussieren, verstärkt werden können, wenn die Dozierenden eine Expertise präsentieren, die auch wahrgenommen wird, und in der Präsentation überzeugende Argumente benutzen.

2.3.2 Das heuristisch-systematische Modell (HSM)

Das Heuristic Systematic Model (HSM) von Eagly und Chaiken (1993) impliziert, ähnlich wie das ELM-Modell, Hauptannahmen über die Determinanten der Persuasion und hinsichtlich der Vorhersagen über den Einfluss, den diese Variablen auf die Persuasion haben (Jonas et al. 2014). Den Kern dieser Theorie bildet die Unterscheidung zwischen heuristischer und systematischer Informationsverarbeitung (Betsch, Funke & Plessner 2011). In der Gegenüberstellung beider Persuasionsrichtungen offenbaren sich der kognitive Aufwand sowie die Methodik der Informationsverarbeitung (siehe Tabelle 8).

Tab. 8: Das heuristisch-systematische Modell (nach Betsch, Funke & Plessner 2011)

heuristisch	**systematisch**
analysearm	analysereich
geringer kognitiver Aufwand	hoher kognitiver Aufwand
theoriegeleitet	datengeleitet
automatisch, unbewusst	kontrolliert, bewusst
Anwendung von: Kategorien, Schemata, Stereotypen, Heuristiken	Anwendung von: Logik, Bayes-Theorem, Varianzanalyse, Kosten-Nutzen-Analyse etc.

Die Modelle der Elaborationswahrscheinlichkeit sagen voraus, dass die Verhaltensänderung, die auf einer systematischen Verarbeitung (d.h. auf der zentralen Route) beruht, beständiger ist als die Verhaltensänderung, die durch eine periphere oder heuristische Verarbeitung induziert wird (Jonas et al. 2014). Geuß (2018) weist darauf hin, dass kognitive Informationsverarbeitungsmodelle zur Erforschung der Urteilsfähigkeit von RezipientInnen geeignet sind, wie etwa das Elaboration-Likelihood-Modell (ELM) oder das heuristisch-systematische Modell (HSM). Und Helisch und Pokoyski (2009) weisen im Kontext der Security-Awareness (präventive Maßnahmen) auf ein „low involvement“ (periphere/heuristische Route) der Belegschaft von Organisationen hin, sofern kein akuter und für die Belegschaft sichtbarer Sicherheitsvorfall vorliegt. Damit postulieren die beiden, dass ohne sichtbare Sicherheitsvorfälle keine kognitive Auseinandersetzung mit dem Thema Security stattfindet, die Einzelnen nicht von der Erforderlichkeit von Maßnahmen überzeugt sind bzw. ein völliges Desinteresse bzgl. dieser Maßnahmen herrscht.

Betrachtet werden sollte jedoch, dass inzidierte Cyberangriffe furchtbehaftet sein können (Clark, Beck & Campisi 2014) und unerwünschte Nebeneffekte mit sich bringen können wie eine falschen Attribution und die damit verbundene nicht intendierte Konfliktpotenzierung (Harnisch & Zettl 2020). Aufgrund dessen wird im Folgenden theoriebasiert auf die Funktion von Furcht im Kontext von (Präventionsmaßnahmen gegen) Cybercrime eingegangen.

2.3.3 Die Theorie der Schutzmotivation (PMT)

Die „Protection Motivation Theory“ (PMT) dient der Erklärung der Wirkung von Furchtappellen auf gesundheitsbezogene Einstellungen und Verhaltensweisen (Hayden 2019). Rogers zieht damit die Wirkung von Furchtappellen in den Fokus einer möglichen Verhaltensänderung und betrachtet dabei einerseits das Wissen über Gesundheitsgefahren aus internen Informationsquellen (Persönlichkeitseigenschaften und vorherige Erfahrungen mit ähnlichen Bedrohungen) und andererseits das Wissen aus externen Informationsquellen (z.B. Überzeugung durch andere, Beobachtungslernen). Welche Wirkungen dieses Wissen hat, ist laut Glaser (2009) jedoch von Bewertungsprozessen abhängig, nämlich von der Bewertung der Gefahr und der Bewertung des Copingverhaltens.

Copingstrategien (COP) sind Bewältigungsstrategien, die subjektiv genutzt werden, um Gefahren abzuwenden, und die zur Stabilisierung des inneren Gleichgewichts beitragen können (Lazarus & Folkman 1984). Lazarus und Lazarus (2006) untergliedern Copingstrategien in problemfokussierendes Coping und emotionsfokussierendes Coping. Das problemfokussierende Coping („problem-focused coping“) adressiert direkte Handlungen, um ein partikulares Problem lösen zu können. Darunter fallen Handlungen, die zur Problemlösung führen, aber auch Handlungen, die es zu unterlassen gilt. Beim emotionsfokussierenden Coping geht es hingegen um die Regulation negativer Emotionen wie Angst, Wut oder Trauer. Beide Bewältigungsstrategien sind in jeden Problemlösungsprozess involviert und nie voneinander getrennt: „Most difficult stressful situations depend on both functions, regulating feelings and trying to change the stressful conditions that are about to be faced“ (ebd., S. 58). Der Prozess der Problemlösung wird somit immer von beiden Copingstrategien geprägt.

In Hinblick auf die Wirkung von Angstappellen und deren Konsequenzen zeigt sich die Erweiterung der PMT im Jahr 2000 durch zwei Metaanalysen (Floyd, Prentice-Dunn & Rogers 2000; Milne, Sheeran & Orbell 2000) als hilfreich. Denn hier wird berücksichtigt, dass Informationsquellen wie Beobachtungslernen, verbale Überzeugungen, Persönlichkeitsvariablen und Erfahrungen die subjektive Bedrohungseinschätzung beeinflussen (Renneberg & Hammelstein 2006) (siehe Abbildung 18).

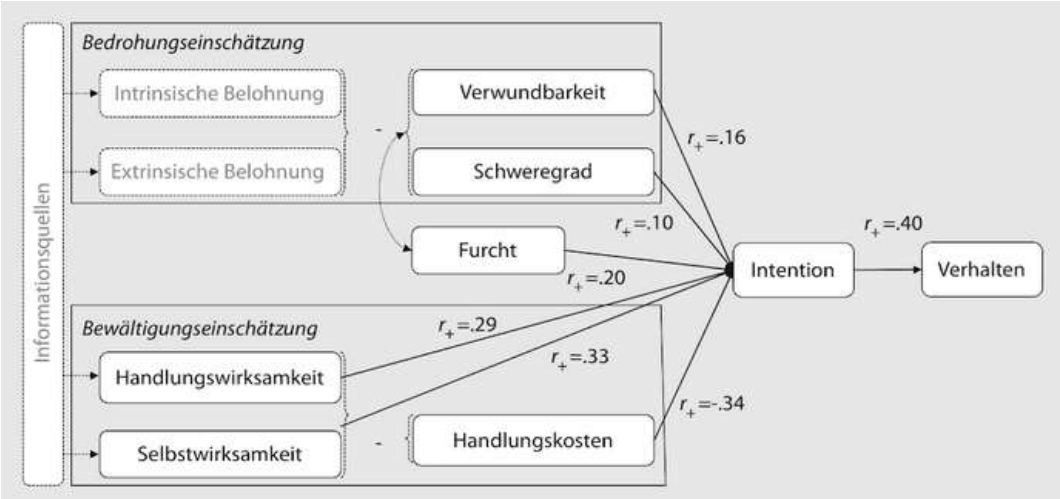


Abb. 18: Die Wirkung von Informationsquellen auf das Verhalten (Renneberg & Hammelstein 2006, S. 37)

Witte und Allen (2000, S. 606) weisen darauf hin, dass die erlebte Selbstwirksamkeit sich jedoch nur vergrößern läßt, wenn subjektive Barrieren identifiziert und auch abgebaut werden: „To increase perceptions of self-efficacy, practitioners should identify barriers that inhibit one's perceived ability to perform a recommended action and directly address these in a message (i.e., skills, costs, beliefs, emotions, etc.)". In ihren Metaanalysen kommen die beiden abschließend zu dem Ergebnis (siehe Abbildungen 19 und 20), dass Furchtappelle nur motivierend wirksam sind, wenn Maßnahmen gleichzeitig Bewältigungskompetenzen unterstützen.

Table 2. Effects of Message Feature on Attitudes, Intentions, and Behaviors

	Fear	Severity	Susceptibility	Response Efficacy	Self-Efficacy
Attitudes					
k	34	14	11	11	8
N	7,514	2,195	1,606	1,849	1,348
r	.147	.149	.119	.139	.116
95% confidence interval	.022	.041	.048	.044	.052
χ^2	79.99*	49.23*	50.86*	40.72*	44.85*
Intention					
k	43	26	27	24	21
N	9,686	3,923	3,948	4,348	3,873
r	.126	.142	.171	.166	.173
95% confidence interval	.020	.030	.030	.029	.030
χ^2	212.95*	81.80*	105.08*	99.29*	82.10*
Behavior					
k	28	16	11	12	11
N	4,666	2,528	1,797	1,608	1,475
r	.158	.132	.138	.129	.126
95% confidence interval	.028	.038	.045	.048	.050
χ^2	142.69*	34.28*	22.23*	16.74	20.46

NOTE: *k* = number of studies, *N* = number of research participants.
*$p < .05$.

Abb. 19: Die Wirkung der Bedrohungseinschätzung und Bewältigungseinschätzung auf die Verhaltensänderung (Witte & Allen 2000, S. 599)

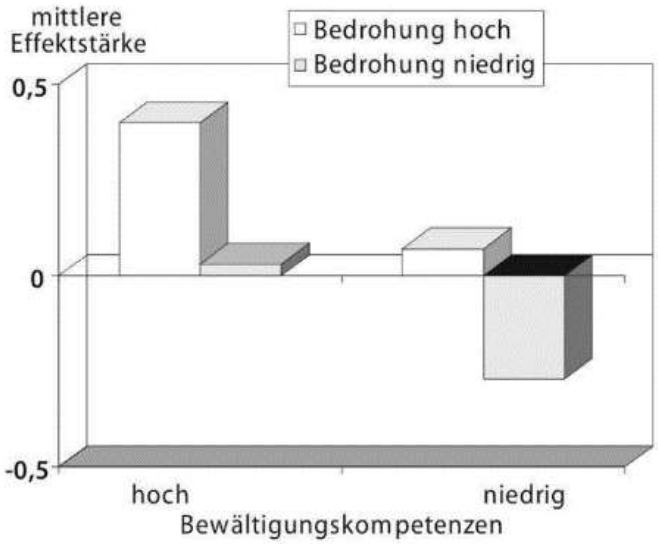


Abb. 20: Der Zusammenhang zwischen der Bedrohungseinschätzung und der Bewältigungskompetenzen (Renneberg & Hammelstein 2006, S. 40)

Damit wird deutlich, dass Furchtappelle eine Verhaltensänderung bewirken können, diese jedoch durch Bewältigungsstrategien zu untersetzen sind. McLuhan, Fiore und Agel merkten hierzu bereits im Jahr 1967 an: „Our "Age of Anxiety" is, in great part, the result of trying to do today's job with yesterday's tools-with yesterday's concepts“ (ebd., S. 8f.).

Hilfreich ist es somit, bereits im Vorfeld vorhandene Bewältigungsstrategien zu identifizieren, um verhaltens- und auch emotionsbeeinflussende Bewältigungsstrategien aufbauen zu können (Borković 2010). Das trifft gleichfalls auf präventive Maßnahmen zu, in denen Furcht entstehen kann, weil die Selbstwirksamkeitserwartung oder Kontrollüberzeugung nicht vorhanden oder unzureichend ist.

2.3.4 Die Theorie der Selbstwirksamkeitserwartung (SET)

In der sozial-kognitiven Theorie Banduras zur Selbstwirksamkeit (Self-Efficacy Theory, SET) wird unter anderem angenommen, dass das Verhalten sowie die Verhaltensänderungen einer Person maßgeblich durch subjektive Überzeugungen (wie die Konsequenz- und die Selbstwirksamkeitserwartung einer Person) bedingt werden (Urton 2017). Damit kann auch dieser Ansatz in den Kontext von sicherheitskonformem Verhalten gesetzt werden. Die Konsequenzerwartung fokussiert primär auf die Abschätzung der potenziellen Folgen der Intention einer Person (Handlungsfolgenabschätzung), während die Selbstwirksamkeitserwartung die subjektiv zur Verfügung stehenden Handlungsoptionen zu einer speziellen Problemlage adressiert. Wobei Bandura (1997) hier nicht die allgemeine Selbstwirksamkeit (vgl. dazu z.B. Schwarzer & Jerusalem 2002) im Blick hat, sondern die spezifischeren Selbstwirksamkeitsüberzeugungen einer Person im Hinblick auf spezielle Situationen oder Lebensbereiche. Des Weiteren beschreibt

Bandura vier Einflussfaktoren und deren Einflussstärke auf die Selbstwirksamkeit. Als stärkste Einflussgröße benennt Bandura (1994, S. 6) die eigenen Erfolgserfahrungen („mastery experience“). Neben den eigenen Erfahrungen bestimmt ihm zufolge die stellvertretende Erfahrung („vicarious experience“) als zweitstärkste Einflussgröße die Selbstwirksamkeit. Dies verdeutlicht Bandura anhand der Beobachtung, die die Beobachtende bzw. den Beobachtenden glauben lässt, dass auch sie/er selbst die Fähigkeiten besitze:

> „The second way of creating and strengthening self-beliefs of efficacy is through the vicarious experiences provided by social models. Seeing people similar to oneself succeed by sustained effort raises observers' beliefs that they too possess the capabilities to master comparable activities to succeed“ (Bandura 1994, S. 3).
>
> „Tue second class of motivators operates through social incentives. In the course of development, physically positive experiences often occur in conjunction with expressions of others' interest and approval, whereas unpleasant experiences are associated with disapproval or censure“ (ebd. 1991, S. 70).

Die drittstärkste Einflussgröße ist gemäß Banduras Ansatz die verbale Überzeugung („verbal persuasion“). Das können persönliche Gespräche sein, in denen der jeweiligen Person ihre Kompetenzen verdeutlicht werden. „They anticipate likely outcomes of prospective actions, they set goals for themselves, and they plan courses of action designed to realize valued futures“ (ebd., S. 71). Die vierte Einflussgröße ist die Wahrnehmung eigener Gefühle, die situationsbedingt auftreten und die Selbstwirksamkeit beeinflussen können.

Für präventive Maßnahmen heißt dies: Erforderliche Schutzmaßnahmen können anhand von real erfolgten oder fiktiven Cyberangriffen diskutiert und ausprobiert werden. Den Lernenden kann so ein Lernsetting mit Bewältigungsstrategien in Aussicht gestellt werden, in dem die Selbstreflexion der eigenen Medienkompetenz sichtbar wird und vorhandene Fähigkeiten und Erfahrungen überprüft werden können. Der Grad an interner Kontrolle wird so zum Korrelat der Selbstwirksamkeit (Lindner 2002).

Um sich näher mit der Veränderung des Verhaltens in präventiven Maßnahmen zu beschäftigen, werden nun weitere Theorien, und insbesondere Einstellungstheorien, erörtert, da auch sicherheitskonformes Verhalten unter anderem von der Einstellung der Benutzenden abhängt.

2.3.5 Das Konstrukt der Kontrollüberzeugung (LoC)

Ein ähnliches Konstrukt wie das der Selbstwirksamkeit von Bandura ist die Kontrollüberzeugung von Rotter. Rotter (1975) legt hierzu ein Theorem vor, das den Umfang einer Konsequenz auf das eigene Verhalten bezieht und dabei primär die Rolle von Kontrollüberzeugungen beleuchtet. Diese Überzeugungen sind, so Stanjek (2020), abhängig von dem Umfeld und den Einschätzungen der eigenen Leistungsfähigkeit. Damit lässt

sich eine Überschneidung zu der bereits behandelten Selbstwirksamkeit erahnen, die Ammon (2006) auch so beschreibt. Wichtig ist jedoch, dass das Kontrollüberzeugungskonstrukt nach Rotter von der Selbstwirksamkeit Banduras zu differenzieren ist, denn „jemand kann der Meinung sein, große Fähigkeiten zu besitzen (self-efficacy), aber dennoch der Überzeugung sein, das mächtige Andere die Ereignisse kontrollieren“ (Ammon 2006, S. 105). Was nun konkret digitale Medien angeht, so ist auch zu berücksichtigen, dass gesellschaftliche Entwicklungen und Positionierungen nicht immer dazu beitragen, dass digitale Medien so eingesetzt werden, dass diese von allen (potentiellen und realen) Nutzenden als bereichernd erlebt werden: „Technology can be extremely complex, and although the evidence presented may be very relevant, the party presenting it needs to ensure its value is highlighted and not lost in the complexity of the underlying technology“ (Edwards 2020, S. 268). – Eine ausführliche Beschreibung dessen erfolgt im Kapitel 2.5.

2.3.6 Die Einstellungstheorie (FAT)

Eine positive Einstellung zur Informationssicherheit ist kein Garant für die tatsächliche Umsetzung von sicherheitsschaffenden Maßnahmen, die sich im sicherheitskonformen Verhalten widerspiegelt. Bereits im Jahr 1934 unternahm La Piere Forschungen, um einen Zusammenhang zwischen Einstellungen[32] und tatsächlichem Verhalten herzustellen. Und Ende der 1960er-Jahre erforschte Wicker in mehreren empirischen Untersuchungen die Beziehung zwischen Einstellungen und Verhalten, um eine gemeinsame Varianz nachzuweisen (Mummendey 1988), die sich jedoch nur auf 10 % zwischen Einstellungs- und Verhaltensmaßen einstellte (Wicker 1971). Im Jahr 1963 entwickelte Fishbein die Einstellungstheorie (Functional Attitude Theory, FAT), die auch als Attitüdentheorie bezeichnet wird, um Einstellungen zu erklären. Auf der Grundlage der vorausgegangenen Forschung wird die FAT auch als Erwartungs-Wert-Modell bezeichnet, bei dem die subjektive Einstellung gegenüber Objekten einem subjektiven Wert oder Nutzen gegenübergestellt wird (Ajzen 2015). Einstellungsobjekte können Themen wie das in dieser Arbeit interessierende Thema „Informationssicherheit“ sein.

2.3.7 Die Theorie des überlegten Handelns (TRA)

Eine Erweiterung der Einstellungstheorie stellt die Theorie des überlegten Handelns (Theory of Reasoned Action, TRA) dar, mit der Ajzen und Fishbein Einstellung und Verhaltensintention in Relation setzen. Die Theorie des überlegten Handelns basiert auf der

[32] Einstellungen sind positive oder negative Bewertungen von Objekten, Ereignissen oder Vorstellungen (Zimbardo & Gerrig 2008).

Annahme, dass das Verhalten durch die eigene (positive) Bewertung und die Bewertung positiv bewerteter Personen beeinflusst wird. Einstellungen („attitudes“) zu erlernten Handlungen, aus denen bestimmte Handlungsoptionen abgeleitet werden, ergeben sich aus der Bewertung der erwarteten Konsequenzen.

Mathematisch lässt sich die Einstellungstheorie nach Fishbeln, Ajzen und Landy (1970, S. 2) wie folgt formalisieren:

$$A_B \propto \sum_{i=1}^{n} b_i e_i$$

Die Einstellung zum Verhalten (A_B) lässt sich herleiten aus der Überzeugung, dass die Verhaltensintention B zur Konsequenz i führen wird (b_i). Die Variable e_i setzt sich aus der Bewertung e und dem Verhaltensergebnis i zusammen. Erweiternd kommt hinzu, dass normative Einflussfaktoren ebenfalls einstellungsbestimmend sind. Der soziale Druck („social pressure“) wird dabei als Erwartung anderer AkteurInnen bezüglich der Durchführung der Handlung bzw. als „nonnative beliefs“ bezeichnet und zugleich als Motivation der Akteurin bzw. des Akteurs, diesen Normen zu folgen, definiert (Stern 2002). Neben den Variablen aus der Einstellungstheorie wirken jedoch noch weitere Variablen als Hintergrundfaktoren, ohne dabei einen direkten Beitrag zur Vorhersage eines möglichen Verhaltens zu leisten: „However, these various indexes of attitude strength were found to correlate differentially with education, gender, and race, challenging the notion that attitude strength is a unitary construct“ (Ajzen 2001, S. 37). Winter (2013) stellt hierzu die in die Forschungen von Ajzen und Fishbein involvierten Variablen grafisch wie folgt zusammen:

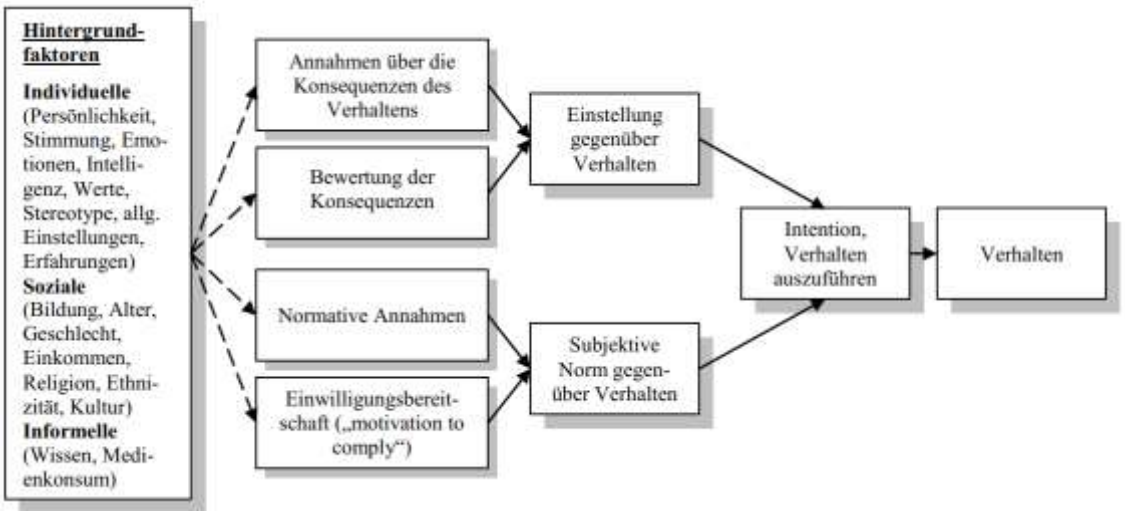


Abb. 21: Theorie des überlegten Handelns (Winter 2013, S. 173; in Anlehnung an Ajzen & Fisbhein 1980)

Verhalten im Kontext der Informationssicherheit ist konsequenzbehaftet und beeinflusst damit die Einstellung gegenüber dem Verhalten. Das setzt jedoch voraus, dass Risiken bekannt sein müssen, um Konsequenzen einschätzen zu können. Gleichzeitig muss die

Bereitschaft bestehen, sicherheitskonformes Verhalten auch ausführen zu wollen. Denn wie die von Barnes (2006) entwickelte Privacy Paradox-Theorie verdeutlicht, kann den Nutzenden der Schutz der Privatsphäre zwar wichtig sein, dieses Motiv wird jedoch nicht immer auf das Handeln übertragen.[33]

Die Durchführung präventiver Maßnahmen im Kontext von Cybercrime kann dabei helfen, diese Risiken transparent zu machen, bevor eine Betroffenheit entstanden ist. Bedeutsam hierbei ist jedoch, dass das Thema Cybercrime nicht bereits zu einer Resignation geführt hat. Darüber hinaus gilt es zu bedenken, dass „die unzureichende Medienkompetenz, das technische Unwissen und individuelle Fehler auf Seiten der Mediennutzerinnen und Mediennutzer als eigene Komponente einer Unterstützung und Ermöglichung des Kontrollverlusts gesehen werden“ (Hagendorff 2019, S. 98) können. Und dass „viele Menschen (…) zurück in eine bessere Vergangenheit, Mauern bauen, sich wieder sicher fühlen“ (Blom 2017, S. 19) wollen. Insofern macht es Sinn, nun eine weitere Theorie von Ajzen und Fishbein, die des geplanten Verhaltens, zu betrachten.

2.3.8 Die Theorie des geplanten Verhaltens (TPB)

Die Theorie des geplanten Verhaltens (Theory of Planned Behavior, TPB) ist eine Erweiterung der Theorie des überlegten Handelns, da sie in die vorherige Theorie die willentlich kontrollierbare Komponente („perceived behavioral control“) zur Ausführung des intendierten Verhaltens implementiert. Ajzen postuliert, dass Intentionen als alleinige Prädiktoren für Verhalten exakt dann unzureichend sind, wenn die persönliche Kontrolle über das Verhalten eingeschränkt ist: „[…] refers to the perceived ease or difficulty of performing the behavior and it is assumed to reflect past experience as well as anticipated impediments and obstacles“ (Ajzen 2005, S. 111). Dargestellt wird dies in der Abbildung 22.

[33] Barnes (2006) macht dies mit der Nutzung von Google-Suchanfragen trotz bekanntem Tracking deutlich.

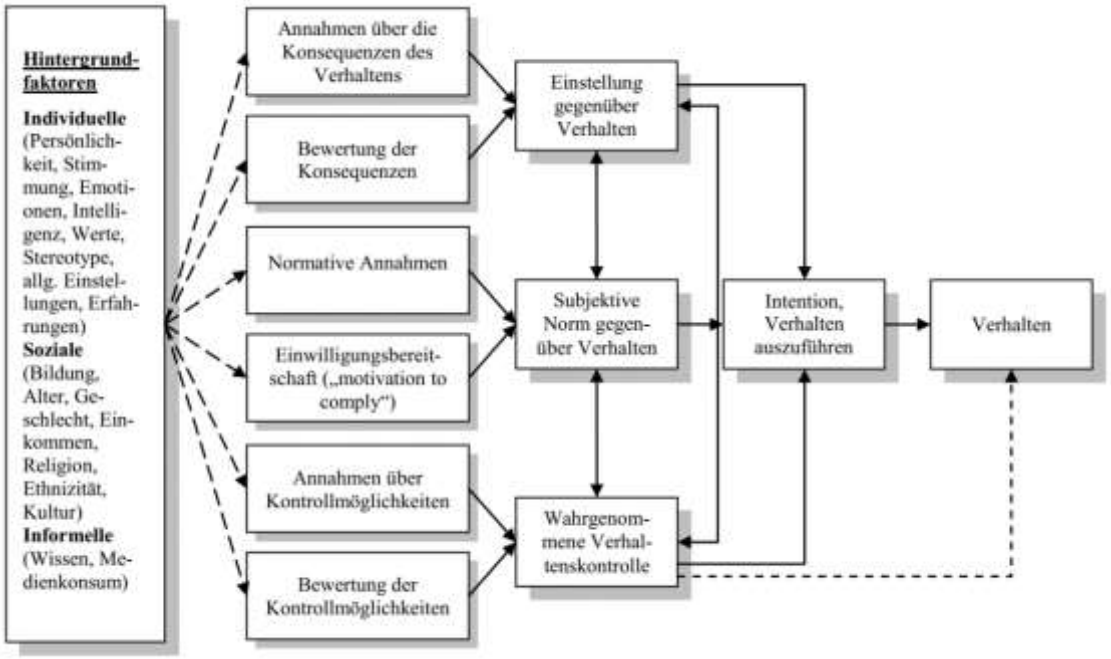


Abb. 22: Theorie des geplanten Verhaltens (Winter 2013, S. 182; in Anlehnung an Ajzen & Fishbein 1980)

Damit rückt die wahrgenommene Verhaltenskontrolle, die sich aus Kontrollüberzeugung und Selbstwirksamkeit zusammensetzt (Moser 2017) und bereits in den Kapiteln 2.3.4 und 2.3.5 behandelt wurde, in den Fokus der Betrachtung und bildet eine weitere Determinante der Verhaltensintention im Modell des geplanten Verhaltens. Die subjektiven Überzeugungen, Verhalten auch umsetzen zu können, die durch Fähigkeiten, allokierbare Ressourcen und Sinn-Bewertungen bedingt sind, entscheiden (mit), ob ein Verhalten umsetzbar ist oder nicht. Verhalten, das vertraut und konditioniert ist, bietet synchron die Möglichkeit der subjektiven Verhaltenskontrolle. Außergewöhnliche Abläufe wie unerwartete Cyberangriffe bedürfen daher neuer oder adaptierter Copingstrategien, um keine Resignation entstehen zu lassen.

Präventive Maßnahmen im Kontext von Cybercrime besitzen das Potenzial, die wahrgenommene Verhaltenskontrolle in neue Situationen zu übertragen, in denen die vorhandenen bzw. aufzubauenden Bewältigungsstrategien reflektiert werden können. Praktisch ist es jedoch nicht nur wichtig, eine Fokussierung auf die Prädiktoren der Verhaltensbeeinflussung vorzunehmen, sondern auch, die Persistenz des Verhaltens, die durch Interventionen erreicht werden kann, zu fokussieren. Die Betrachtung der operationalisierbaren Verhaltenspersistenz ist evident, da nur so Wirkungen durch erfolgreiche Sequenzierungen erhalten bleiben. Diesbezüglich wird nun ein weiteres Modell zu Persistenz und Verhalten vorgestellt.

2.3.9 Das transtheoretische Modell

Sicherheitskonformes Verhalten bedarf der Persistenz, um tatsächlich Sicherheit zu gewährleisten und bspw. digitale Infrastrukturen langfristig zu schützen.

Prochaska und Diclemente (1983) stellen in ihrem transtheoretischen Ansatz ein Stufenmodell der Verhaltensänderung vor, das auf sechs Stufen („stages of change“) basiert und von Prochaska und Prochaska (2016) übernommen wurde.

Tab. 9: Stufen der Verhaltensänderung (Keller 1998, S. 1)

Stufen der Veränderung im Rahmen des TTMs	
Sorglosigkeit *(„precontemplation“)*	Es gibt keine Intention, das problematische Verhalten in den nächsten sechs Monaten zu verändern.
Bewusstwerden *(„contemplation“)*	Es wird erwogen, das problematische Verhalten in den nächsten sechs Monaten zu verändern.
Vorbereitung *(„preparation“)*	Erste Schritte zur Veränderung wurden eingeleitet, das Zielverhalten wird in den nächsten 30 Tagen angestrebt.
Handlung *(„action“)*	Das Zielverhalten wird seit weniger als sechs Monaten gezeigt.
Aufrechterhaltung *(„maintenance“)*	Das Zielverhalten wird seit mehr als sechs Monaten beibehalten.
Stabilisierung *(“termination“)*	Das Zielverhalten wird dauerhaft aufrechterhalten. Es ist keine situative Versuchung bzw. Rückfallgefahr mehr vorhanden.

Die erste Stufe bildet die Sorglosigkeit („precontemplation“). Das eigene Verhalten wird hier nicht als problematisch angesehen, da Verhaltensweisen noch nicht auf bewusste Kontexte übertragen wurden. Eine Intention zur Veränderung des Verhaltens ist nicht vorhanden, da kein Zugang zum Thema vorhanden ist. Prochaska und Prochaska (2016, S. 1) schreiben hierzu: „‚Precontemplation‘ is the stage in which individuals do not intend to take action in the near future usually defined as the next six months, which is about as far ahead as most people plan when it comes to making changes“. Im Kontext der Informationssicherheit können das unzureichende Risikobetrachtungen sein, die in einem Ignorieren oder Transfer des Risikos deutlich werden.

In der zweiten Phase wird das eigene Verhalten zum Kontext in Relation gesetzt und eine Bewusstwerdung („contemplation“) durch Nachdenken vollzogen. In dieser Phase findet eine kognitive Auseinandersetzung mit dem derzeitigen Verhalten und dessen möglichen Konsequenzen statt. In präventiven Maßnahmen zu Cybercrime kann dies durch Darstellungen und Vorführungen aktueller Sicherheitsvorfälle erreicht werden, die eine mögliche Selbstbetroffenheit bei den Teilnehmenden adressieren. Prochaska und Prochaska (ebd., S. 15) weisen zusätzlich darauf hin, dass TeilnehmerInnen in dieser Phase der contemplation innerhalb von sechs Monaten Maßnahmen zur Veränderung ergreifen: „People who are at the stage of ‚contemplation‘ in their change process generally intend to take action within the next six months“.

In der dritten Stufe („preparation“) wird versucht, innerhalb von 30 Tagen das angedachte Verhalten umzusetzen („take action in the next thirty days“).

Die vierte Stufe („action“) stellt die tatsächliche Umsetzung der Verhaltensänderung für eine Dauer von sechs Monaten („change but for less than six months“) dar.

Die fünfte Stufe („maintenance“) bezeichnet die Beibehaltung des Verhaltens für einen längeren Zeitraum als sechs Monate („behavior for more than six months“).

Auf der sechsten Stufe („termination“) ist das „neue“ Verhalten selbstverständlich geworden, ein Rückfall ist ausgeschlossen („not tempted to relapse“). Im Idealfall bedeutet dies im Kontext von sicherheitskonformen Verhalten Persistenz.

2.3.10 Die empirische Unterfütterung der dargelegten Erklärungsmodelle im Kontext von Cybercrime

Nun werden die oben vorgestellten Theorien mit aktuellen Forschungsergebnissen zum Thema Informationssicherheit untersetzt.

Bezüglich der Bedeutung der Theorie des geplanten Handelns (TPB) im Kontext der IT-Sicherheit zeigen Bulgurcu, Cavusoglu und Benbasat (2010) in ihrer kanadischen Studie (n = 464, p < 0,01), dass sich die erklärte Varianz für das Konstrukt, Sicherheitsrichtlinien einzuhalten, durch 35 % TBP-Konstrukte aufklären lässt (siehe Abbildung 23).

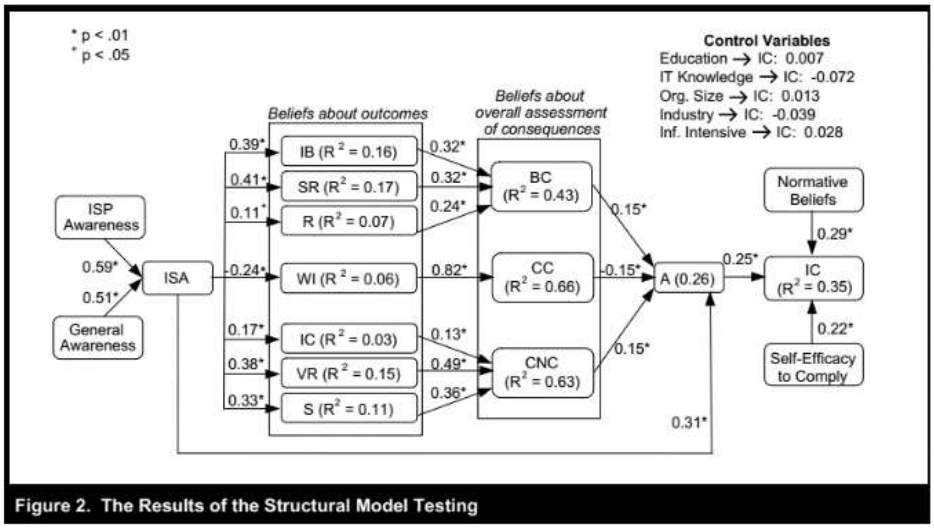


Abb. 23: Ergebnisse der Strukturmodellprüfung (Bulgurcu et al. 2010, S. 540)

Damit kann davon ausgegangen werden, dass das TPB-Konstrukt durchaus auch im Kontext von IT-Sicherheit von Bedeutung ist, wenn das Verhalten in den Fokus gesetzt werden soll. Analysen von Ifinedo (2013) zeigen ebenfalls, dass die Einstellung[34] zu Richtlinien das Verhalten im Kontext der Informationssicherheit signifikant beeinflussen kann (siehe Abbildung 24).

[34] ISSP steht für: Information systems security policy compliance.

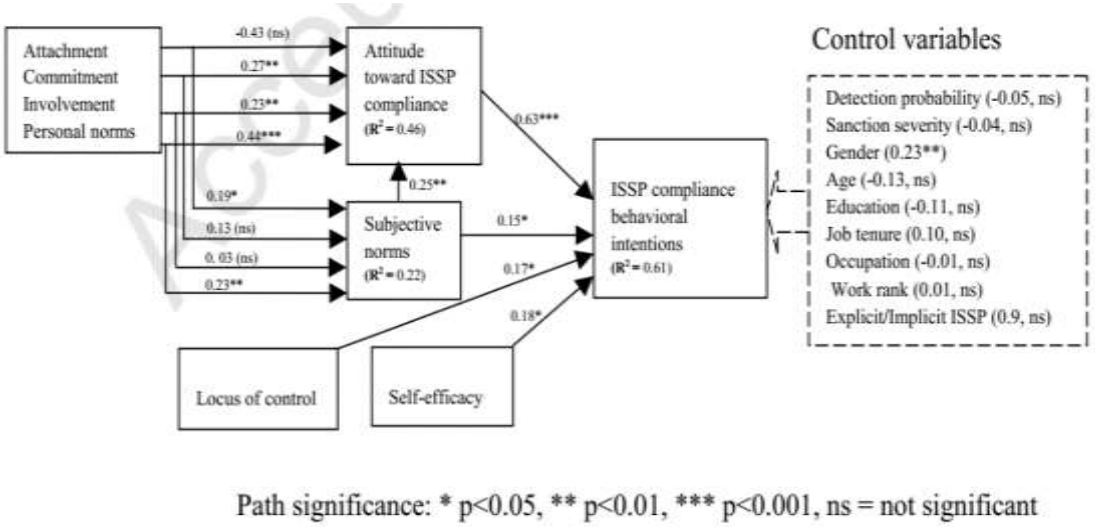


Abb. 24: Die SmartPLS 2.0-Ergebnisse für die getestete Beziehung (Ifinedo 2013, S. 74)

Die Studie „Effects of Organization Insiders' Self-Control and Relevant Knowledge on Participation in Information Systems Security Deviant Behavior" von Ifinedo zum Sicherheitsverhalten untersuchte die folgenden Verhaltensanomalien:[35]

- „Not immediately notifying your organization of the loss of IT ressources (e.g, USB) containing confidential data.
- Connecting computers to the Internet through an insecure wireless network.
- Reusing the same password and username on different websites.
- Using generic and unencrypted USB on organization's network.
- Using personal mobile devices to connect to organization's network without permission.
- Not disposing and destroying all unneeded sensitive documents and information on computer on time.
- Carrying unnecessary sensitive information on a laptop when travelling.
- Opening emails from unverified senders.
- Using social media sites for personal reasons at work.
- Using simple passwords for convenience" (Ifinedo 2012a, S. 3).

[35] Diese wurden zum Teil in die präventive Maßnahme integriert, da sie aktuell relevant sind.

Die Ergebnisse der Studie zeigen, wie in der Abbildung 25 ersichtlich wird, dass eine niedrige Selbstkontrolle und die Bildung einen signifikanten Effekt auf abweichendes Sicherheitsverhalten (ISSDB = Information systems security deviant behavior) haben (Ifinedo 2012a).

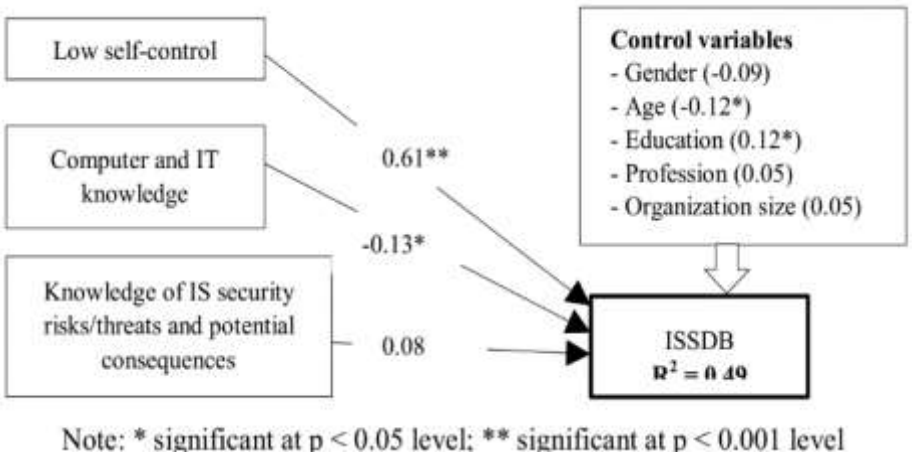


Abb. 25: Ergebnisse der PLS-Analyse (Ilfinedo 2012a, S. 6)

Neben den Modellen von Ajzen und Fishbein wird in der Forschungsliteratur häufig auch auf Modelle Bezug genommen, die Sanktionen als Mittel der Verhaltenskorrektur in den Fokus ziehen. D'Arcy, Hovav und Galletta (2009) berichten hierzu aus den USA (n = 269) über eine fehlende Varianz von R= -.065 und somit R²= .00 für die Schwere der Sanktionen sowie ein R= -.176 und somit R²= .03 für die wahrgenommene Sicherheit von Sanktionen (siehe Abbildung 26).

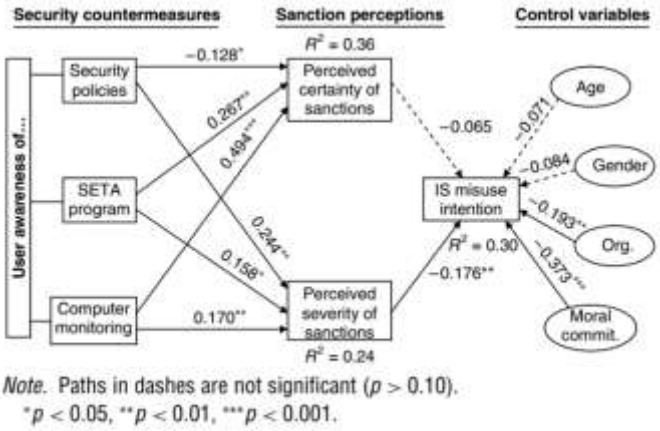


Abb. 26: Resultat der Analyse des NAME-Models (D'Arcy, Hovav & Galletta 2009, S. 89)

Daher lässt sich festhalten: „Der Zwang oder das bloße Vertrauen, dass die erarbeiteten Vorkehrungen von den Organisationsmitgliedern befolgt werden, führt dementsprechend nicht zum Ziel der Informationssicherheit" (Fussan 2010, S. 299). Die finnische Studie von Pahnila, Siponen und Mahmood (2007) weist ebenfalls keinen signifikanten Effekt von Sanktionen aus: „The effect of sanctions on intention to comply was not significant" (ebd., S. 7).

Eine aktuellere brasilianische Studie aus dem Jahr 2016 (n = 117) zu sicherem Verhalten im Kontext von Informationssicherheit und Richtlinien legen Klein und Luciano vor, die u.a. folgende Hypothesen aufstellen und untersuchen:

> „H1: The perceived susceptibility of the threat to Information Security positively influences safe behavior regarding Information Security.
>
> H2: The perceived severity of the threat to Information Security positively influences safe behavior regarding Information Security.
>
> H3: The perception of the certainty of detection of not following the guidelines on Information Security positively influences safe behavior regarding Information Security.
>
> H4: The perception of the Punishment Severity for not following the guidelines regarding Information Security positively influences safe behavior in terms of Information Security.
>
> H5: The perception of effort to safeguard when following the Information Security guidelines negatively influences safe behavior related to Information Security.
>
> H6: Satisfaction with colleagues, superiors or organization positively influences Safe Behavior regarding Information Security“ (Klein & Luciano 2016, S. 483).

Die beiden kommen in Anbetracht der erhobenen Daten gleichfalls zu dem Ergebnis, dass das wahrgenommene Strafmaß für sanktioniertes Fehlverhalten für das sicherheitskonforme Verhalten unbedeutend ist: „They also show that the main effects of the perceived Punishment Severity are not significant“ (ebd., S. 489). Bedeutsamer, so die Autoren, sind die Zufriedenheit mit dem Arbeitsplatz und die empfundene eigene Anfälligkeit für eine Bedrohung. So zeigen die in der Abbildung 27 visualisierten Ergebnisse, dass die aufgeklärte Varianz mit 0.413 = 41 % überwiegend auf die Zufriedenheit zurückzuführen ist.

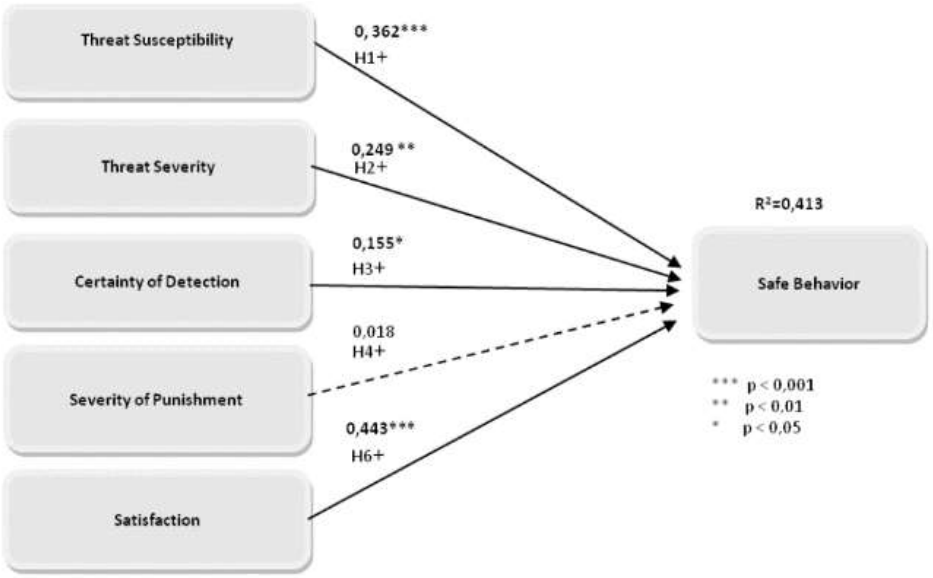


Abb. 27: Das theoretisches Modell von Klein & Luciano und seine Hypothesen (Klein & Luciano 2016, S. 483)

Resümierend ist an dieser Stelle festzuhalten, dass die abgehandelten Theorien, Konstrukte und Studien aufzeigen, welche Prädiktoren Verhalten beeinflussen können. Dies

ist insofern gemäß dem Forschungsinteresse dieser Arbeit relevant, als sich relational aus den Prädiktoren Interventionsmöglichkeiten ableiten lassen und Rückschlüsse darauf gezogen werden können, was genau wie in Maßnahmen positiv beeinflusst werden kann. Insofern wird im Folgenden auf die Intervention durch präventive Veranstaltungen eingegangen.

2.4 Präventive Veranstaltungen

Präventive Veranstaltungen im Kontext von Cybercrime haben die Anwenderinnen und Anwender im Blick, die – neben vielen anderen Angeboten – das Angebot erhalten, kostenlose Veranstaltungen zu besuchen, um in Zukunft fachkundige Entscheidungen im Bereich der Informationssicherheit treffen zu können. Ziel solcher Maßnahmen sollte es sein, den Nutzenden von technischen Infrastrukturen deutlich zu machen, dass gezielte (partikulare) oder nicht gezielte (generalisierte) Cyberangriffe auf unterschiedlichem Niveau stattfinden können und dass diesbezüglich dezidierte Schutzmaßnahmen erforderlich sind. Denn Erwachsene und insbesondere Eltern und pädagogisches Personal müssen (wieder!) in der Lage sein, Risiken von Cyberangriffen sowie eigene Potentiale zu erkennen, um Wissensdefizite auszugleichen und somit letztendlich neue Gegenmaßnahmen implementieren zu können. Denn Jugendliche haben bereits seit vielen Jahren die Möglichkeit, selbstständig einfache Angriffe zu starten, und laufen damit Gefahr, den rechtskonformen Raum zu verlassen, ohne dass ihre Eltern rechtzeitig intervenieren können. Eltern dürfen sich auch angesichts der Komplexität und der damit verbundenen Kompliziertheit nicht von der „Bildfläche“ verabschieden oder sich einem Kontrollverlust hingeben, da dies für die Schutzbefohlenen negative Konsequenzen haben kann. Hilfreich können für diese Zielgruppe präventive Maßnahmen sein, wie sie im Folgenden beleuchtet werden.

2.4.1 Prävention im Kontext von Cybercrime

Präventive Maßnahmen im Kontext von Cybercrime erheben in dieser Arbeit den Anspruch, Verhaltensformen und -weisen, die selbstschädigend sind, nicht in Erscheinung treten zu lassen. Die primäre Fokussierung liegt darin, abweichendes Verhalten frühzeitig aufzufangen, bevor kriminelle Handlungen durch Cyberkriminelle möglich werden oder die AdressatInnen selbst (ggf. unwissentlich) kriminell agieren.

Redmiles, Malone und Mazurek (2016) zeigen in ihrer amerikanischen Studie (n = 24), dass selbsterlebte oder gehörte Sicherheitsvorfälle zu Verhaltensänderungen geführt haben, und unterstreichen damit die Theorie der Selbstwirksamkeit von Bandura. Diese Verhaltensänderungen bleiben nach Redmiles, Malone und Mazurek jedoch aus, wenn aus Sicht der Betroffenen alles getan wurde, um eigene Systeme abzusichern,

und wenn im Kontext IT-Sicherheit vermittelt wird. Viele Erwachsene unterliegen jedoch einer technischen Wissensillusion, die ihnen selbst nicht bewusst ist: Die Illusion, bereits zu wissen, dass in einer Gemeinschaft Sachkunde existiert, lässt Menschen glauben, selbst fachkundig zu sein (Park 1999; Holtz & Miller 1985). In der Praxis anzutreffende Meinungen aufgrund der Uneinsichtigkeit, es letztendlich durch negative Erfahrungen zu lernen (Hofielen 2018), indem durch einen Zusammenstoß die Wirklichkeit erschlossen wird (Günther 1966), sind wenig hilfreich, um Verhalten zu ändern. Denn hierdurch kann zwar die Selbstwirksamkeit möglicherweise erhöht (Kuhl 2001), die Kontrollmöglichkeit jedoch negativ beeinflusst werden, sodass damit die wahrgenommene Verhaltenskontrolle als Prädiktor des Verhaltens negativ beeinflusst wird, wie es im Kapitel 2.3.8 bereits detailliert dargestellt wurde. Gleichfalls sei darauf verwiesen, dass Cyberangriffe irreparable Schäden verursachen können (Morgan 2019), indem Daten unwiederbringlich zerstört werden.

Die Lösung kann somit nicht darin gesehen werden, reale Cyberangriffe stattfinden zu lassen, um Erfahrungen zu sammeln, und damit das Risiko einzugehen, Kontrollverluste hinnehmen zu müssen, sondern es gilt, präventiv zu agieren, indem die Zuhörenden von mündlichen Berichten profitieren (Pierce & Cheney 2013) oder/und an bereitgestellten Infrastrukturen Erfahrungen sammeln. Da sich die Zielgruppen jedoch in ihrem Interaktionsbereich, der Medienkompetenz und den damit verbundenen Risiken unterscheiden, bedürfen präventive Maßnahmen ebenfalls einer Unterscheidung, wie nachfolgend skizziert wird.

Verschiedene Formen der Prävention

In den nachfolgenden Abschnitten werden unterschiedliche Formen der Prävention aufgenommen und behandelt.

Universelle, selektive und indizierte Prävention

Eine Unterteilung der Prävention in universelle, selektive und indizierte Prävention adressiert entweder unterschiedliche Personengruppen (universell, selektiv) oder gefährdete Personen partikular (indiziert).

Zu einer *universellen Prävention* gehören insbesondere Maßnahmen, die sich an die allgemeine Bevölkerung richten. Das können klassische Informationsmaterialien, präventive Veranstaltungen oder Kampagnen sein. Universelle Prävention bedeutet demnach, aktuelle Cyberbedrohungen auszuwählen und die vorhandene Kompliziertheit didaktisch zu reduzieren, um eine universelle Zielgruppe in die Lage zu versetzen, dargebotene Daten als Informationen zu erkennen und mit diesen das vorhandene Wissen zu ergänzen. So sollte bspw. Folgendes vermittelt werden: „One important concept that

any home user should understand is that any computer connected to the internet, can be susceptible to cyber-attacks“ (Teymourlouei 2015, S. 678).

Die *selektive Prävention* richtet sich an Gruppen, die besonders bedroht sind, also an sogenannte Risikogruppen. Im Kontext von Cybercrime können das Personen sein, die mit hoch schützenswerten Informationen umgehen müssen. Spezielle Themen, die spezielle Sicherheitsvorkehrungen erforderlich machen, können zielgruppenbezogen präventiv begleitet werden.

Die *indizierte Prävention* richtet sich hingegen an Personen, die bereits ein manifestes Risikoverhalten etabliert haben. Hier ist es erforderlich, etablierte Verhaltensweisen transparent zu machen und eine Verhaltensänderung herbeizuführen.

Forschungsbezogene Betrachtungen im Kontext Cybercrime zeigen, dass präventive Maßnahmen allgemein durch Sensibilisierung (Awareness) signifikante Wirkungen mit einer hohen Effektstärke erzielen können (siehe Tabelle 10).

Tab. 10: Regressionsanalyse zur Verhinderung von Cyberkriminalität (Ali 2016, S. 21)

Independent Variables	Prevent Cyber Crime					
	Standart Coefficients Beta	R^2	Adjusted R^2	Sig. F Change	F Change	Durbin-Watson
Law Enforcement	0.966	0.934	0.933	0.000	2084.957	0.414
Awareness	0.953	0.907	0.907	0.000	1449.293	0.537
Ethics	0.909	0.827	0.826	0.000	708.231	0.172
IT Technology	0.878	0.770	0.769	0.000	496.598	0.189

Situative und soziale Prävention

Andere Differenzierungen speziell im Kontext Crime erlauben eine Unterscheidung nach situativer und sozialer Verbrechensverhütung. Beides wird nachfolgend beschrieben, auch wenn diese Formen nicht direkt im Kontext von Cybercrime stehen.

Die situative Prävention: Situational Crime Prevention

Der Situational-Crime-Prevention-Ansatz ist nach Tonry und Farrington (1995) eine von vier postulierten Hauptstrategien, um Verbrechen zu verhindern. Dazu zählen zudem Strafverfolgung, Entwicklungsverhinderung sowie Gemeinschaftsverhinderung. In seiner wegweisenden Konzeption der Situational Crime Prevention unterscheidet Clarke (1995) jedoch zwischen drei Kategorien der situativen Kriminalprävention:

1. Erhöhung des Tataufwandes für die Täterin bzw. den Täter (Schutzmechanismen),
2. Erhöhung des Risikos für die Täterin bzw. den Täter (Transparenz),
3. Reduzierung des Nutzens für die Täterin bzw. den Täter (Wirtschaftlichkeit).

Ausführlicher ist die Zusammenstellung von Cornish und Clarke (2003), die in Risiken, Aufwand, Anreiz und Kosten kategorisieren. Diese Autoren zeigen, dass kriminelle Handlungen nach dem Minimal- und Maximalprinzip „betriebswirtschaftlichen" Abwägungen unterworfen sind. Denn ausgewählt wird das, was am meisten Gewinn bei den geringsten Kosten verspricht (Brand 2004).

Essenziell für eine hierauf Bezug nehmende präventive Maßnahme ist es damit, Schutzmechanismen für Cyberangriffe, wie sie im Kapitel 2.2. beschrieben wurden, vorzustellen.

Die soziale Prävention: Social Crime Prevention

Die soziale Prävention von Kriminalität („Social Crime Prevention") konzentriert sich auf die sozialen und wirtschaftlichen Bedingungen, die zu gewalttätigem und kriminellem Verhalten beitragen. McLaughlin und Muncie (2006) beschreiben verschiedene Maßnahmen (vor allem Abschreckungsstrategien), die Straftaten, bei welchen soziale Ursachen die Kriminalität bedingen, verhindern können. Grant (2015, S. 3) definiert Social Crime Prevention als Strategien zur Verhütung sozialer Kriminalität: „Social crime prevention strategies are those that seek to reduce the social risk factors in society (family, community, peer), rather than a strict focus on the individual offender". Damit adressiert die soziale Kriminalität eher die sozialen Risikofaktoren in der Gesellschaft (Familie, Gemeinschaft, Gleichaltrige).

Zusammenfassung

Diesbezüglich ist es essenziell für die Konzipierung präventiver Maßnahmen, vorab zu entscheiden, welche Zielgruppe in den Fokus genommen werden soll und welches Präventionsmodell eine zielgruppenadäquate Passung aufweist. Diese Arbeit fokussiert eine universelle Prävention, die sich auf das Situational-Crime-Prevention-Modell stützt, da es einer heterogenen Gruppe (18- bis 67-Jährige), die berufsfähig ist, zugeordnet werden kann und in der Lage ist, IT-Sicherheitsrisiken zu minimieren und Schutzmaßnahmen transparent zu machen.

Die Absicherung der präventiven Intervention auf der Grundlage des normativen Modells rationalen Handelns nach Obrecht

Weiterhin ist es essentiell, nicht nur die Zielgruppe einzugrenzen, sondern auch zu prüfen, ob eine Intervention abgesichert durchgeführt werden kann. Ein hierzu verwendbares Modell ist das normative Modell rationalen Handelns nach Obrecht (1996).

Bevor präventive Maßnahmen als Mittel der Intervention in einen größeren Kontext gesetzt werden, sollte entschieden werden, ob eine Durchführung als Intervention anzuraten ist oder nicht. Denn erfolgt diese Prüfung nicht, besteht die Gefahr, mit präventiven

Maßnahmen im Kontext des Cybercrime keine oder fehlgelagerte Wirkungen zu erzielen, die die Situation noch verschlimmern.

Für die Planung von derartigen Präventionsangeboten sind verschiedene Planungsmodelle in unterschiedlichen Kontexten entwickelt worden. Einen aussichtsreichen Vorschlag zur Bearbeitung von sozialen Problemen legt Obrecht (ebd.) vor, welcher hierzu die schrittweise Erarbeitung eines universalen, handlungstheoretisch fundierten Problemlösungsmodells vorschlägt und den Handlungsprozess in einzelne Phasen differenziert. Obrecht unterteilt hierzu sein Modell des rationalen Handelns in fünf unterschiedliche Problemlösungsprozesse, die sukzessiv aufeinander aufbauend wirksam werden (siehe Tabelle 11). Diese Phasen können individuell zugeschnitten und durch kontextspezifische Inhalte untersetzt werden.

Tab. 11: Das Modell rationalen Handelns von Obrecht (1996)

Phase 1: Situationsanalyse
Phase 2: Bewertung und Problemdefinition
Phase 3: Zielsetzung und Planung
Phase 4: Entscheidung und Implementierung des Planes
Phase 5: Evaluation

In der *ersten Phase* erfolgt eine Analyse der Ist-Situation. Wie im Kapitel 2.1.2 beschrieben wurde, sind Interventionen, die ein sicherheitskonformes Verhalten möglich machen, erforderlich, um schädigenden Zuständen langfristig entgegenzuwirken. Denn wie die Abbildung 1 zeigte, gibt es auch aktuell eine Vielzahl von Cyberangriffen, und Nutzende einer digitalen Infrastruktur stehen unterschiedlichen TäterInnen(profilen) mit unterschiedlichen Angriffsformen gegenüber (vgl. dazu Kapitel 2.1.5 und 2.2.1-2.2.3).

In der *zweiten Phase* werden Auswirkungen fokussiert, welche entstehen können, wenn keine Präventivmaßnahmen erfolgen. Denn nicht selten finden betriebswirtschaftliche Abwägungen statt, die präventive Interventionen als „vermeidbare“ Kostenfaktoren ohne eine offenkundige Rentabilität betrachten. Diese vermitteln den Eindruck einer fehlenden Korrelation bzw. Kausalität solcher Maßnahmen zur Kosteneinsparung. Betrachtungen von Hermann und Bubenitschek (dargestellt in der nachfolgenden Tabelle 12) zeigen jedoch (auch betriebswirtschaftlich!), dass Kriminalprävention, wenn auch hier auf andere Deliktformen und Orte bezogen, durchaus überdurchschnittlich rentabel sein kann.

Tab. 12: Rentabilität präventiver Maßnahmen im Jahr 2015 (nach Hermann & Bubenitschek 2015, S. 37)

Ort	Kosten kommunaler Kriminalprävention	Durchschnittlicher Nutzen durch Reduzierung der Gewalt- und Straßenkriminalität	Rentabilität in %
Heidelberg	582782 €	1157421 €	50,35
Hockenheim	80871 €	538806 €	15,01
Leimen	68183 €	500320 €	13,63
Schwetzingen	69586 €	696852 €	9,99
Wiesloch	49565 €	150800 €	32,87
Gesamt	850987 €	3044199 €	27,95

Andere Auswirkungen von präventiven Maßnahmen adressieren Fragestellungen der Legitimation von Kriminalprävention durch Ethik. So formuliert Hermann (2016) die Prämisse, dass Kriminalprävention genau dann legitim ist,

- „wenn sie ohne Freiheitsverletzung auskommt oder die Betroffenen zuvor eine freiheitsverletzende Maßnahme ausgeführt haben“ (ebd., S. 10). Präventive Maßnahmen zum Thema Cybercrime sind also legitim, wenn die Teilnahme freiwillig erfolgt oder wenn sie eine Reaktion auf eine aktuelle Normverletzung darstellen.
- „wenn die Maßnahme wirkungsvoll ist und folglich die Glücksbilanz für die Gesellschaft verbessert“ (ebd., S. 12).
- wenn die Wirkung intersubjektiv bzw. objektiv nachgewiesen wird (womit sich der empirische Teil dieser Arbeit befasst).
- „wenn die Maßnahme aus der Sicht der Verantwortlichen dem Wohl der Teilnehmer oder der Gesellschaft dienen soll“ (ebd., S. 14).
- „wenn die erwarteten Folgen von Maßnahmen verantwortet werden können“ (ebd., S. 14), d.h., wenn mögliche Folgen auf ihre Schädlichkeit geprüft wurden und die positiven Effekte überwiegen.

Die Vermittlung von Informationen über Angriffsmethoden birgt jedoch die Gefahr, dass dieses Wissen später unautorisiert eingesetzt werden kann. Um dies einzuschränken, soll die im Rahmen dieser Arbeit evaluierte präventive Maßnahme, wie im Kapitel 2.3.4 bereits erörtert wurde, nur bei Erwachsenen eingesetzt werden.

In der *dritten Phase* der Planung erfolgt die Festschreibung der Zielsetzungen: „Die Entwicklung von Zielen verfolgt dabei den Anspruch, als problematisch erkannte Zustände in positiv bewertete Alternativen überführen zu können“ (Metzger 2011, S. 15). Wirksame Cyberangriffe sind solche problematischen Zustände, die Infrastrukturen negativ beeinflussen können. Diese Zustände sind bekannt und werden beobachtet (siehe Abbildung 3). Präventive Maßnahmen zum Thema Cybercrime besitzen also das Potential, die Wirksamkeit von Cyberangriffen zu reduzieren.

In der *vierten Phase* erfolgen die Konzipierung und Implementierung eines Plans, der die herausgestellten Ziele mit Handlungen unterfüttert. Wobei laut Stimmer (2000) bei der Entwicklung der Handlungsablaufpläne Rahmenbedingungen, handlungsleitende Konzepte, Arbeitsprinzipien und -formen, Medien sowie die Methodenwahl zu berücksichtigen sind. Der Erfolg präventiver Maßnahmen im Kontext von Cybercrime hängt also maßgeblich von gesetzten Zielen ab, die unter anderem durch Rahmenbedingungen, Didaktik und Methodik beeinflusst werden. Deshalb ist eine sorgsame Konzipierung präventiver Maßnahmen unabdingbar, um Ziele wie ein sicherheitskonformes Verhalten erreichen zu können.

In der *fünften Phase* erfolgt die Evaluation, denn das Erreichen der beabsichtigten Wirkungen wird in dieser Phase überprüft. Gerade in präventiven Veranstaltungen sind Evaluationen wichtig, damit unerwünschte Wirkungen (Furcht, Resignation) vermieden werden können. Denn präventive Maßnahmen im Kontext von Cybercrime besitzen das Potential, nicht nur Variablen zum sicherheitskonformen Verhalten zu verbessern, sondern diese auch zu verschlechtern. Ohne eine abschließende Überprüfung der Ziele und Wirkungen sind derartige Maßnahmen also ggf. kontraproduktiv und verschlechtern die Ausgangssituation noch.

2.4.2 Wirksamkeitsbezogene Vorüberlegungen

Das normative Modell rationalen Handelns nach Obrecht (1996) macht deutlich, dass wirksamkeitsbezogene Vorüberlegungen essentiell sind und Beachtung finden sollten, um eine beabsichtigte Wirkung zu erreichen und unerwünschte Wirkungen zu vermeiden. Denn: „Investing in technology is a crucial step in any security strategy, but education and appropriate processes are equally important“ (Bunker 2020, S. 19), oder wie Paul es bereits im Jahr 1967 beschrieb: „What treatment, by whom, is most effective for this individual with that specific problem, and under which set of circumstances“ (Paul 1967, S. 111)? Wirksamkeitsbezogene Vorüberlegungen sind somit auch für präventive Maßnahmen im Kontext von Cybercrime wichtig, um auch hier ein sicherheitskonformes Verhalten zu erreichen und unerwünschte Nebeneffekte zu vermeiden. Jedoch ist es schwierig, wie Schäfer (2017) hierzu hervorhebt, verlässliche Daten über die Wirkungen sowie die monetären und sonstigen Erträge von Weiterbildungsmaßnahmen zu gewinnen, da es hierzu so gut wie keine Erkenntnisse gibt. Adressiert man hierzu die Erwartungen an Weiterbildungen, so stehen an der Spitze die persönliche Zufriedenheit mit 84 % sowie die Erwartung, mehr leisten zu können (78 %) und neue berufliche Aufgaben zu übernehmen (65 %) (Autorengruppe Bildungsberichterstattung, 2016). Noch deutlicher werden die Anmerkungen von Spitzer (2015), der auf unerwünschte Nebeneffekte

in der präventiven Arbeit aufmerksam macht, wenn Lerninhalte und das Alter unberücksichtigt bleiben. Damit wird deutlich, dass präventive Interventionen einer intensiven Vorbereitung bedürfen, um die beabsichtigte Wirkung (Motiv-Handlung-Konsequenz) auch erzielen und Erwartungen erfüllen zu können.

Didaktik in der Erwachsenenbildung

Überall, wo intentionell gelernt wird, ist auch ein Bezug zur Didaktik zu finden. Beispiele hierfür sind in allen Lebenslagen vorhanden, weshalb Didaktik für jede/n Einzelne/n lebensbegleitend und prägend zugleich ist. Wird der Versuch unternommen, den Begriff Didaktik etymologisch herzuleiten, findet sich in diversen Abhandlungen primär der Verweis auf das altgriechische Word didáskein, womit dem Wort Didaktik die Bedeutung Lehren oder Lehrkunst zugewiesen wird (Riedl 2004). Andere AutorInnen wie Kron verweisen auf weitere altgriechische Begriffe wie:

„Didactos: lehrbar, gelehrt, unterrichtet,
Didaskalia: Lehre, Belehrung, Unterricht, belehrend,
Didasko: Lehrer sein, lehren, belehren, unterrichten,
Didachae: das Lehren, die Lehre, die Belehrung, Unterricht“ (Kron 1993, S. 40).

Um den Begriff Didaktik intersubjektiv zu rahmen, wurde bisher eine große Anzahl von Definitionsversuchen unternommen. Humbert (2005) weist in diesem Kontext darauf hin, dass im Laufe der Zeit mithilfe von unterschiedlichen Definitionen der Didaktik zwar verschiedene Schwerpunkte gesetzt wurden, diese jedoch jeweils dem Ziel verpflichtet sind, eine theoriegeleitete, konstruktive Leistung zu erbringen, die dem Lehren und Lernen dienlich ist. Denn die Zielsetzung der Didaktik ist es, eine Antwort auf die Frage, was gelehrt werden soll, zu geben (Habedank 2011), sodass gilt: „Die Frage nach den Zielen kann nur durch ein intensives Studium der Bezüge in den Dimensionen Ziele, Bildung, Themen und Inhalte beantwortet werden“ (Humbert 2006, S. 4). Ableitend hieraus finden sich unterschiedliche Definitionen tradierter AutorInnen, die die Didaktik als Wissenschaft (und Lehre) vom Lehren und Lernen definieren (Dolch 1965) oder die Lehrzielformulierung, die Auswahl der Unterrichtsinhalte und die dazu passenden Lehrmethoden im Fokus der Didaktik sehen (Arnold, Eysenck & Meili 1971). Dolch (1965) weist zusätzlich darauf hin, dass auch Beratungen und Vorträge aus einer didaktischen Perspektive zu betrachten sind, da diese dazu dienen, Wissen entstehen zu lassen. Denn Wissen ist dabei alles, was Zustimmung beanspruchen kann (Hönigswald 1918). Didaktisches Handeln erhebt insofern den Anspruch, Voraussetzung zu sein, um wirksames Lernen stattfinden zu lassen. Deshalb werden im Folgenden unterschiedliche Strömungen der Didaktik und verschiedene Lerntheorien erörtert, die eine Relevanz für die Konzeption und Durchführung von präventiven Maßnahmen haben können.

Die konstruktivistische Didaktik

Eine der hier vorgestellten Theorien der Didaktik ist die konstruktivistische Didaktik, welche die Grundidee des Konstruktivismus aufnimmt und im Kontext des Lernens weiterentwickelt. Wissen, so die konstruktivistische Didaktik, ist eine subjektive Konstruktionsleistung der Lernenden, die individuell, fallbezogen und unter Berücksichtigung der Wahrnehmungen erfolgt. Vorhandene Einflüsse wie Umwelt, Bildung und Medien bilden Beeinflussungsfaktoren, die im Konstruktionsprozess wirken, den Lehrenden jedoch, wenn sie nicht operationalisiert werden, verborgen bleiben. Lernziele, die den Anspruch erheben, in einer homogenen Gruppe identische Resultate zu erzielen, werden somit zu einer Illusion (Arnold 2007). AutorInnen der konstruktivistischen Didaktik wie Siebert (2012) und Reich (2005b) postulieren jedoch nicht nur das Lernen als konstruktiven und situativen Prozess, sondern beschreiben auch, welche Unterstützungen erforderlich werden, damit Lernen erfolgreich umgesetzt werden kann. Denn das Ziel der konstruktivistischen Didaktik ist es, dass die Lernenden die vorhandene subjektive Konstruktion der Wirklichkeit selbst erweitern. Lorenz (1992) und Winter (2001) verweisen beispielsweise darauf, dass es wesentlich ist, eigene körperliche Erfahrungen für das Verständnis von Größen zu machen, und untersetzen damit den von Bandura (1976) postulierten wirksamsten Selbstwirksamkeitsprädiktor: die eigenen Erfahrungen. Wie bereits beschrieben, können solche Erfahrungen jedoch auch die Kontrollüberzeugung, die Rotter (1975) belegt und beschreibt, beeinflussen und eine Selbstwirksamkeitsüberzeugung verhindern. Reich (2005b) weist weiter darauf hin, dass das übliche Instruieren von eigenen konstruierten Welten (der Lehrenden) von den Lernenden nicht übernommen werden kann, da individuelle Konstrukte der Wirklichkeit bereits vorhanden sind und auch Lehrende nicht über Wahrheiten, sondern nur über eigene Konstrukte verfügen. Subjektive Wirklichkeiten, so Reich, müssen daher selbst (neu) konstruiert werden und erfordern somit eine subjektive Auseinandersetzung mit dem Thema. Mediale Darstellungen, die die Wichtigkeit von Cybersicherheit präsentieren, können somit nur ein erster Schritt in die beabsichtigte Richtung sein. Reich postuliert hierzu die drei Kategorien Rekonstruktion, Konstruktion und Dekonstruktion. Für das Thema der Rekonstruktion übernimmt er Ansätze aus der Reformpädagogik und beschreibt unter Berücksichtigung der Erkundung der reformpädagogischen Praxis die zum Lerninhalt gewonnenen Informationen. Klassische Methoden der Informationsgewinnung und -reduktion wie Kontextualisierung und Dekontextualisierung werden hierzu angewendet. Reich bezeichnet dies als konstruktiven Moment, in dem auch für die Lehrenden exklusiv transparent wird, welche Einstellungen und Emotionen bei den Lernenden überhaupt vorhanden sind.

Für das Forschungsanliegen dieser Arbeit bedeutet dies eine Auseinandersetzung mit Fragen wie bspw. derjenigen nach der Wirksamkeit von Schutzmechanismen, die für

die Lernenden die Möglichkeit bereithält, vorhandene Erfahrungen zu erweitern oder neue Erfahrungen zu sammeln. Gelingt die Auseinandersetzung mit dem Thema, kann zukünftig Gelerntes kontextbezogen dekonstruiert werden. Die Lernenden sind befähigt, aus neu empfangenen Nachrichten Informationen zu generieren, um diese in das subjektive Wissenskonstrukt stimmig zu integrieren und damit Wissen zu erweitern oder zu aktualisieren. Somit besitzt die konstruktivistische Didaktik durchaus das Potenzial, durch reale Beispiele Kompetenzen entstehen zu lassen, die im Umgang mit neuen Fragestellungen zur Cybersicherheit hilfreich sein können. Dies ist besonders wichtig, da neue Bedrohungsszenarien Schutzmaßnahmen erforderlich machen, die erst entwickelt werden müssen (Alsbih & Mentel 2019).

Die identitätstheoretische Didaktik

Auch die identitätsorientierte Didaktik tangiert die konstruktivistische Blickrichtung und sieht Bildungsarbeit nicht länger im Kontext von Gestaltung und Machen, sondern sieht im Vordergrund das Wachsenlassen und Hegen. Im Zentrum der Betrachtung steht die Identität, die nicht verliehen wird, sondern ein konstruktivistisches Produkt darstellt, das durch subjektives Reflektieren erworben werden muss (Siebert 1996). Den Interaktionsrahmen bilden hierzu unterschiedliche Reflexionskontexte, in denen die „Anderen“ als Richtmaß für Verhalten, Werte und Normen fungieren. Damit nimmt die identitätsorientierte Didaktik den Bezug der Normierung nicht nur gemäß dem symbolischen Interaktionismus auf, sondern auch die bereits von Fishbein und Ajzen postulierten Prädiktoren der Verhaltensintention, z.B. die soziale Norm (siehe Abbildung 21). Lernen bedeutet aus dem Blickwinkel der identitätsorientierten Didaktik, die eigene Konstruktion der Wirklichkeit ständig und in jeweils neuen Kontexten auf ihre Brauchbarkeit zu prüfen, um langfristig psychisch und sozial stabil zu bleiben. Kritische Lebensabschnitte, die durch eine soziale Unterstützung nicht ausreichend aufgefangen werden können, bedeuten eine unumgängliche Auseinandersetzung mit neuen Situationen, deren empfundener Schwierigkeitsgrad von erlebten Reflexionskontexten und deren Bewältigungsfähigkeit maßgeblich beeinflusst wird. Ereignisse werden so zu einem Konstrukt in der menschlichen Existenz, fokussiert durch eine begrenzte Sichtweise, die im Ringen mit den widrigen Umständen hergestellt wird und als wesentlich und entscheidend empfunden wird, obgleich sich dies dann im zeitlichen und kulturellen Wandlungsprozess verändern kann (Reich 1998). Aus der Perspektive der Lernenden ist es somit wichtig, einen Rahmen für eine biografieorientierte Selbstreflexion und Anbindung des Lernens an das eigene Leben und die eigenen Lebenserfahrungen zu haben (Bubolz-Lutz 2017). Denn gelingt dieses Reflektieren dauerhaft nicht, sind Zuschreibungen wie internale Attributionen, ausgedrückt durch niedrigen Selbstwert, Resignation oder gar Aggression (Baeriswyl 2013), eine mögliche Folge, die gesundheitliche Beeinträchtigungen nach sich ziehen

kann. Damit nimmt die gewählte Didaktik, insbesondere die identitätstheoretische Didaktik, eine sonderpädagogische Blickrichtung ein, die sich im Kontext der Aufgabenstellungen widerspiegeln kann. Tietgens (1992) macht hierzu deutlich, dass erwachsenenpädagogisches Handeln eine hohe Verantwortung trägt, da dies in Lebensläufe interveniert. Im Kontext dieser Arbeit bedeutet dies, dass Digitalisierung und künstliche Intelligenz schnell ihre eindeutige Bewertung als vorteilhaft verlieren, wenn Sicherheitsaspekte unberücksichtigt bleiben und sich dies durch Sicherheitsvorfälle „unerwartet in Erinnerung“ bringt. Erforderliches Verständnis wird so, im schlimmsten Fall, zur erlernten Hilflosigkeit, wenn die Komplexität dem erhofften Nutzen von digitalen Produkten mit IT-Sicherheitsmängeln langfristig widerspricht und keine Lösung gefunden wird (Seligman 1979). „Dementsprechend soll der Mensch über ein Handlungsrepertoire verfügen, das ihn befähigt, die zunehmende Komplexität und Unbestimmtheit seiner gesellschaftlichen Umwelt zu begreifen und durch kompetentes und verantwortliches Handeln zu gestalten“ (Pätzold 2006, S. 176).

Die bildungstheoretische Didaktik

Die bildungstheoretische Didaktik, die von Wolfgang Klafki begründet wurde, rückt den Begriff Bildung ins Zentrum der Betrachtungen und verweist darauf, dass bildungswirksame Inhalte einer überlegten Auswahl bedürfen. Klafki (1964) postuliert hierzu fünf Grundfragen und stellt damit (s)eine didaktische Analyse mit der Integration der Fragen wie folgt vor:

1. Die exemplarische Bedeutung des Inhalts

Die exemplarische Bedeutung nimmt, wie der Terminus „exemplarisch“ bereits vermuten lässt, das Beispiel in den Fokus der Betrachtungen. Exemplarisch nennt man Unterricht, der darauf angelegt ist, Inhalte statt in stofflicher Vollständigkeit „in sinnfälligen Beispielen zu vermitteln“ (Rohlfes 1997, S. 280). Den Lernenden werden demnach ausgewählte Beispiele angeboten, die eine Auseinandersetzung mit der Thematik möglich werden lassen, sodass Kenntnisse eigenständig erworben und idealerweise Fähigkeiten entwickelt werden können, die Comenius (1891, S. 204) wie folgt beschreibt: „Bei den Werkzeugen zeige man den Gebrauch vielmehr in der Wirklichkeit als durch Worte d.h. vielmehr durch Beispiele als durch Vorschriften“. Strategisch zielt die exemplarische Inhaltshervorhebung darauf ab, die Prinzipien bekannter Beispiele verallgemeinern zu können, um diese auf neue Problemlagen adaptiv übertragen zu können. Bekemeier (2011, S. 138) verweist hierzu auf Impulsfragen wie: „Welche Gemeinsamkeiten und Unterschiede kann ich zwischen dem neu erworbenen Wissen und dem bisher Gedachten ausmachen?“

Bezogen auf Maßnahmen zur Prävention von Cybercrime kann die Arbeit mit Beispielen insbesondere bedeuten, den Lernenden konkrete Cyberangriffe vorzustellen. Dabei ist es sinnvoll, die Beispiele möglichst zielgruppenorientiert mit essentieller Bedeutung auszuwählen, sodass die Lernenden sie als lebensnah bewerten.

2. Die Gegenwartsbedeutung des Inhalts

Lernende erwarten, dargebotene Lerneinheiten aktuell praktisch einsetzen zu können, egal ob im Beruf oder in der Freizeit. Klafki spricht mit dieser Forderung die Aktualität der angebotenen Lerninhalte an, deren Praxistauglichkeit abzusichern ist. Das Ineinander von Gegenwärtigem und Zukünftigem, die Bedeutung der Augenblicksorientierung sowie die Kontinuität und Zukunftsverantwortung adressieren Lernzielbetrachtungen (Schicke, Felden & Schäffter 2014).

Für die hier konzipierte präventive Maßnahme bedeutet dies, keine Sicherheitslücken, Sicherheitsempfehlungen oder Gesetze zu präsentieren, die nicht mehr aktuell oder gültig sind. Denn diese würden nicht nur die Gegenwartsbedeutung des Inhalts infrage stellen, sondern auch die Vorbereitungsleistung der oder des Lehrenden. Ebenfalls sei darauf verwiesen, dass die Gegenwartsbedeutung des Inhalts die Arbeitsfähigkeit der Lernenden beeinflusst (Karl 2009) und somit einen Grund zur Teilnahme an präventiven Maßnahmen darstellen kann. Diesbezüglich sind Inhalte ständig auf Aktualität sowie lebensweltlichen Bezug der Lernenden zu prüfen und ggf. auszutauschen.

3. Die Zukunftsbedeutung des Inhalts

Die Auswahl von Lerninhalten, wie zum Beispiel Cyberangriffe und die Schutzmöglichkeiten davor, bedürfen einer Fokussierung des Inhalts über die Gegenwartsbedeutung hinaus. Problematisch für die Zukunftsbedeutung ist jedoch, dass Sicherheitslücken mitunter schnell geschlossen und Cyberangriffe in der spezifischen Art, wie sie in einem Lernmodul vielleicht vorgestellt werden, daher nicht mehr umgesetzt werden können, da nun Sicherheitstechnologien greifen oder Voraussetzungen fehlen (z.B. das alte Betriebssystem). Gerade hier zeigt sich jedoch das Potenzial der Anwendung exemplarischer Lerninhalte, die nicht nur das Beispiel als partikulares Objekt adressieren, sondern primär die Adaptivität zukünftiger Cyberangriffe in den Fokus der Betrachtungen stellen. Deutlich wird dies etwa bei einer partikularen Perspektive auf ein singuläres Schutzziel, wie zum Beispiel Vertraulichkeit, ohne auf andere Schutzziele wie Verfügbarkeit und Integrität zu achten. Denn ein WLAN kann sicher verschlüsselt sein (Vertraulichkeit), jedoch auch gestört werden (Verfügbarkeit). Diesbezüglich ist es hilfreich, nicht nur auf spezielle Cyberangriffe, wie sie im Kapitel 2.2 dargestellt wurden, zu verweisen, sondern vielmehr aufzuzeigen, warum derartige Angriffstaxonomien aus den

Perspektiven der Herstellenden, der Regierung, der Technik und Moral erfolgreich werden können (vgl. Kapitel 2.2.3). Gleichfalls bedeutsam für die Lernenden ist die Anwendbarkeit des Wissens in der Zukunft. Ausgewählte Beispiele müssen daher für die Teilnehmenden erfassbar und adaptierbar sein, um ebenfalls einen Einfluss auf die Erhaltung der Arbeitsfähigkeit zu haben, da nur so neue Entwicklungen nutzbar und damit zugänglich werden (Howaldt 2004).

4. Zugänglichkeit

Ausgewählte Beispiele müssen für die Teilnehmenden verständlich und anschaulich dargestellt sein. Hierzu sind Beispiele auszuwählen, die sowohl eine berufliche als auch eine private Betroffenheit veranschaulichen können und nicht frei erfunden sind. Bei der Auswahl von Beispielen ist weiter darauf zu achten, dass sich die Kompliziertheit didaktisch im Verhältnis zur verfügbaren Vermittlungszeit reduzieren lässt. Komplexe Cyberangriffe wie Buffer-Overflows (Speicherüberlauf) oder die Anwendung von Exploits (Nutzung von Schwachstellen) sind daher ungeeignet und Themen für SpezialistInnen.

5. Sachstruktur des Inhalts

Die Sachstruktur des Inhalts behandelt die Art und Weise, wie die Themen konzeptionell aufeinander aufgebaut werden. Dazu ist es erforderlich, das Vorwissen der Teilnehmenden abzufragen oder abzuschätzen. Deklaratorisches Wissen ist ebenfalls unabdingbar für den Diskurs und die Vermittlung von Informationen, denn es ist wichtig, dass die Teilnehmenden unter den Begrifflichkeiten dasselbe verstehen. Haben die Teilnehmenden verstanden, dass Informationen schützenswert sind, können Angriffe gezeigt werden, deren Ziel es ist, Informationen unautorisiert abzugreifen, um weitere Angriffe starten zu können (vgl. Kapitel 2.2).

Die lerntheoretische Didaktik

Wie soll der zu erlernende Inhalt vermittelt werden? Auf diese Frage versuchen die lerntheoretische Didaktik, die auch als Berliner Didaktik bezeichnet wird, und die später entwickelte sogenannte Hamburger Didaktik eine Antwort zu geben. Heimann, Otto und Schulz (1965) konzipierten hierzu ein Modell, das sich von der bildungstheoretischen Didaktik abgrenzen soll (Jank & Meyer 2002). Bildung wird hierbei als ideologisch negativ besetzt und somit ungeeignet begriffen (Peterßen 1982). Denn Lernen soll wertfrei sein und praktiziert werden und keine Interdependenzen zu Ideologien besitzen. Heimanns Anspruch besteht vielmehr darin, den Lehrenden eine verbindliche Handlungsordnung an die Hand zu geben, die sich auch auf wissenschaftliche Untersuchungen stützen kann (Peterßen 2001).

Hinsichtlich der Gestaltung von Lehr- und Lernprozessen unterscheidet das Berliner Modell zwischen zwei Reflexionsphasen, nämlich der Struktur- und der Faktorenanalyse. In der Strukturanalyse sehen die AutorInnen die vorgegebenen Entscheidungs- und Bedingungsfelder, die alle interdependent zueinander in Beziehung stehen (Gassmann 2013). Dazu gehören Entscheidungsfelder wie Intentionalität, Thematik, Methodik und Medienwahl und die Bedingungsfelder (Euler & Hahn 2014). Aus diesem Grund werden nun Bedingungsfelder und Entscheidungsfelder näher betrachtet.

Bedingungsfelder

Um Bedingungsfelder transparent zu machen, bedarf es unterschiedlichster Analysen, die bei Flechsig (1996) zu finden sind und deren Ergebnisse zu Bedingungsfeldern werden. Folgende Analysen sind laut Flechsig (ebd., S. 24) möglich:

1. Kulturanalysen,
2. Zielgruppenanalysen,
3. Ressourcenanalysen,
4. Vorgabenanalysen und
5. Anforderungsanalysen.

Die *Kulturanalyse* ist eine Beschreibung der Kultur der Lernenden und Lehrenden, die prägende Auswirkung auf das Lernen hat. Die kulturellen Unterschiede bedürfen einer differenzierten Analyse und Beachtung. Für die konzipierte präventive Maßnahme bedeutet dies, den Kulturkreis festzulegen. Dabei ist die evaluierte Maßnahme im Wesentlichen auf die Mitglieder des abendländischen Kulturkreises ausgerichtet.

Die *Zielgruppenanalyse* beschreibt die Personengruppe, die die Maßnahme nutzen soll. Hierzu bedarf es idealerweise einer Analyse der Zielgruppe, die sich nach Lerntypen kategorisieren lässt. In der evaluierten Maßnahme handelt es sich um eine Zielgruppe, die sich aus Erwachsenen im Alter von 18 bis 67 Jahren zusammensetzt, welche individuell über unterschiedliche Bildungsniveaus verfügen und probabilistisch untersetzt sind durch auditive, visuelle, haptische oder intellektuelle (auch verbal-abstrakt genannte) Lerntypen.

Die *Organisationsanalyse* analysiert Rahmenbedingungen der Lehrveranstaltung, an die die Lehrenden gebunden sind. Dies können finanzielle Prämissen oder auch räumliche Gegebenheiten sein. Präventive Veranstaltungen finden zielgruppenbezogen teilweise ortsunabhängig statt und werden auch von unterschiedlichen VeranstalterInnen gebucht. Deshalb ist es erforderlich, Technik einzusetzen, die ortsunabhängig funktional und zuverlässig ist. Um Cyberangriffe demonstrieren zu können, bedarf es einer entsprechenden Hard- und Softwareausstattung, die für die hier konzipierte Maßnahme angeschafft wurde.

Die *Ressourcenanalyse* beschreibt die für die Veranstaltung benötigten Unterrichtsmittel. Das Ergebnis der Ressourcenanalyse steckt somit die Grenzen des Möglichen ab und ist damit letztendlich vom finanziellen Rahmen abhängig. Die präventive Maßnahme „Der zweite Blick“ ist eine Maßnahme, die vom Landesrat für Kriminalitätsvorbeugung im Jahr 2018 mit 4.000 Euro gefördert wurde.

Die *Vorgabenanalyse* analysiert die Vorgaben der Institution, bei der die Bildungsmaßnahme angesiedelt ist bzw. von der sie getragen wird. Das können Beschränkungen des Zugangs zur Lernumgebung und/oder zum Inhalt oder persönlich aufzubringende Kosten sein. Der Landesrat für Kriminalitätsvorbeugung setzte im Fördermittelbescheid entsprechende Prämissen für präventive Projekte, die das Thema fokussierten und die Nachweispflicht festlegten (LfK 2019).

Die *Anforderungsanalyse* versucht zu ergründen, was warum gelernt werden soll. Potenziale für die Persönlichkeitsentwicklung und Anforderungen eines künftigen Arbeitsplatzes sind ebenso zu berücksichtigen wie aktuelle gesellschaftliche Situationen (siehe Kapitel 2.1.3 und 2.1.4).

Entscheidungsfelder

Aufsetzend auf diese Bedingungsfelder, werden nun die Entscheidungsfelder der lerntheoretischen Didaktik vorgestellt:

1. Intentionalität,
2. Thematik,
3. Medienwahl und
4. Methodik.

Das Entscheidungsfeld *Intentionalität* gibt Auskunft darüber, welche Absichten die Lehrenden mit ihren Interventionen in den Fokus genommen haben, und bildet die Voraussetzung für die Auswahl einer passenden Thematik. Das Gesamtziel dieser präventiven Maßnahme ist es, den Teilnehmerinnen und Teilnehmern sicherheitskonformes Verhalten vorzustellen, dieses zu reflektieren und, falls erforderlich, Risiken im Umgang mit digitalen Medien zu mindern.

Das Entscheidungsfeld *Thematik* wird maßgeblich von den Absichten beeinflusst und soll ein oder mehrere eindeutige/-s Lernziel/e formulieren.

Beim Entscheidungsfeld *Medienwahl* wird danach gefragt, welche Medien zum Einsatz kommen müssen und welche Medien zum Einsatz kommen können. Da präventive Maßnahmen kurzzeitige Maßnahmen sind und unterschiedlichsten Lerntypen entsprechen sollen, ist es sinnvoll, durch die Beachtung der Binnendifferenzierung der Medien ein breites Medienangebot zu gestalten, um idealerweise alle Teilnehmenden gemäß ihrer individuellen Lernzugänge zu erreichen. Eine Differenzierung in der Erwachsenenbildung kann nach Druckmedien, Projektionsmedien, Tonmedien und Fernsehmedien

vorgenommen werden (Ruprecht 1977). In der evaluierten präventiven Intervention kamen dementsprechend folgende Medien zum Einsatz: Auf den Einsatz von Druckmedien wurde verzichtet, da HackerInnenshows ebenfalls keine Lernmaterialen in dieser Form anbieten und in dieser Konstellation als Kontrollgruppe dienten. Der Einsatz von Projektionsmedien erfolgte durch die Darstellungen der Bildschirminhalte von Opfern und simulierten CyberangreiferInnen. Denn auf diese Weise konnten realitätsnahe Cyberangriffe und deren Auswirkung miterlebt werden, wie es Billett wie folgt beschreibt „The majority of what we learn arises through its direct experiencing, albeit sometimes mediated by others“ (Billett 2018, S. 197). Der Einsatz von Tonmedien erfolgte durch einen aktuellen Nachrichtenpodcast, der als Opener diente, um einen Diskurs über Nachrichten und Informationen stattfinden zu lassen. Denn auf diese Weise konnten die Teilnehmenden anhand eines Beispiels aus der Praxis Informationen von Nachrichten trennen und auf den Kontext Cybersicherheit adaptieren. Der Einsatz von Fernsehmedien lässt sich von Präsentationsmedien kaum noch unterscheiden, da Inhalte per Computer angezeigt (Herzig et al. 2010) und großflächig präsentiert werden können.

Bezüglich des Entscheidungsfelds *Methodik* ist das Folgende festzuhalten: Gelingendes Lernen basiert nicht nur auf der Fokussierung der vorhandenen Voraussetzungen aller Beteiligten, sondern auch auf dem Arrangieren zielbezogener Lerninhalte. Die Methodik, abgeleitet von dem altgriechischen Wort méthodos mit der Bedeutung „Weg nach“, zielt auf die didaktische Wissensorganisation. Sie verfolgt das Ziel, zusammen mit den verwendeten Medien eine stimmige Anordnung der Lerninhalte zu erreichen. Damit Lernsettings erfolgreich durchgeführt werden können, sind umfassende didaktische Vorbereitungen und das Schaffen didaktischer Rahmenbedingungen unabdingbar (Siebert 1996). Praktisch bedeutet dies unter anderem, die bestmögliche Reihenfolge in der Behandlung der Lerninhalte zu wählen, damit der Aneignungsprozess so gut wie möglich verlaufen kann (Meder 2006).

Diachrone Betrachtungen zur Didaktik machen deutlich, dass der Unterricht als Methodik besonders hervorzuheben ist. Didaktische Methodik bedarf dementsprechend erforderlicher Lehrkompetenzen, die nachfolgend erörtert werden.

2.4.3 Kompetenzen Lehrender in präventiven Maßnahmen

Die Person der bzw. des Lehrenden spielt in allen Lehrveranstaltungen und so auch in präventiven Maßnahmen eine zentrale Rolle und ist mitverantwortlich für den Erfolg der Maßnahme. Diesbezüglich bedarf es Kompetenzen, die nicht nur das Fachliche betreffen, sondern insbesondere die Erwachsenenbildung selbst. Hierzu wurden bereits Richtlinien von Weiterbildungsinstitutionen und anderen Organisationen erlassen, beispielsweise der Kompetenzpass für WeiterbildnerInnen der Technischen Universität Dresden

(Technische Universität Dresden 2009) sowie die Kompetenzvoraussetzungen für Lehrende in der Erwachsenbildung anhand der Studie des luxemburgischen Wissenschaftsministeriums (David 2014). Diese sind:

1. bildungstheoretische Kompetenzen,
2. didaktische Kompetenzen,
3. Sozialkompetenzen,
4. Fachkompetenzen,
5. wissenschaftsorientierte Kompetenzen,
6. Organisationskompetenzen,
7. pädagogische Qualifikationen,
8. unternehmerische Kompetenzen,
9. Kompetenzen im Bibliothekswesen und Informationsmanagement,
10. Reflexionskompetenzen,
11. Kompetenzen zu Einwirkungsmöglichkeiten zur Entwicklung von Selbstkompetenz und
12. Professionskompetenzen.

Bei den *bildungstheoretischen Kompetenzen* geht es unter anderem um die Verortung von Weiterbildung im weiteren Sinne, die Kenntnisse des jeweiligen nationalen Bildungssystems sowie aktuelle Entwicklungen zu Themen wie unter anderem Gender, Diversität und Medienkompetenz.

Die *didaktischen Kompetenzen* lassen sich u.a. unterteilen in die

- konzeptionelle Kompetenz (Scarbath & Beyer-Stiepani 2012),
- methodische Kompetenz (Frei 2003),
- Lernbegleitungskompetenz (Röbe 2019),
- Evaluationskompetenz (Hallet 2006),
- Prozesskompetenz (Rabenstein 2003),
- Didaktikreflexionskompetenz (Abels 2011) sowie die
- Moderationskompetenz (Krampen & Zayer 2006).

Damit wird deutlich, wie umfangreich die erforderlichen didaktischen Kompetenzen sind, was unterschiedliches prozedurales Wissen an die Lehrenden adressiert.

Der Begriff *Sozialkompetenz* umschreibt die Fähigkeit, individual- und zielgruppenspezifisch zu kommunizieren, heterogene Lerngruppen zu leiten, die Gruppendynamik zu berücksichtigen und bei Konflikten mediativ eingreifen zu können. Hallet (2006) weist praxisbezogen darauf hin, dass auch jede inhaltsbezogene Äußerung nicht nur Fachwissen transportiert, sondern auch die Beziehung zwischen Lernenden und Lehrenden reflektiert.

Die *Fachkompetenz* umfasst Kenntnisse über das jeweilige Thema (Becket et al. 2008). Helmke (2010) hebt hierzu hervor, dass selbst das bestoptimierte Lehr-/Lernszenario keine Lernwirksamkeit erzielt, wenn es an Fachkompetenz fehlt. Reinmann-Rothmeier und Mandl (2001) verweisen andererseits aber darauf, dass bloßes wissenschaftlich abgesichertes Fachwissen unzureichend ist und es einer zusätzlichen praktischen Erfahrung bedarf. Pretty et al. (1981) machen hierzu weiter deutlich, dass gemäß dem Elaboration-Likelihood-Modell die erfolgreiche Kommunikation von starken Argumenten oder der Expertise der KommunikationspartnerInnen (z.B. TrainerInnen) abhängig ist (wie es bereits im Kapitel 2.4.1 beschrieben wurde).

Die *wissenschaftsorientierten Kompetenzen* adressieren den Umgang mit wissenschaftlichen Quellen, ihre Rezeption und Interpretation (Prexl 2016).

Die *Organisationskompetenzen* betreffen die Allokation erforderlicher Ressourcen sowie das Abstimmen und Treffen von Vereinbarungen.

Die *pädagogische Qualifikation* beinhaltet Fachwissen sowie Handlungskompetenzen aus den Bereichen der (pädagogischen) Psychologie, Sozialforschung und Neurowissenschaft (z.B. Lernforschung).

Die *unternehmerischen Kompetenzen* beziehen sich auf die Fähigkeit, die Maßnahme finanziell abzusichern.

Die *Kompetenzen im Bereich des Bibliothekswesens und Informationsmanagements* umfassen die Fähigkeit, in den unterschiedlichsten Bibliotheken (online) Informationen zu finden, zu dekontextualisieren, zu systematisieren, zu reduzieren und lerngerecht aufzubereiten, um sie im Lehr-/Lernsetting kontextualisieren zu können.

Die *Reflexionskompetenz* ermöglicht Lehrenden, die Perspektiven der Teilnehmenden und Lernenden einzunehmen, um die sich bei ihnen ereignenden (Lern-)Prozesse nachzuvollziehen zu können. Die Reflexionskompetenz erfordert somit neben der Selbstreflexionsfähigkeit die Bereitschaft und Fähigkeit zum Perspektivwechsel und Empathie für andere Personen (Zeuner 2011, S. 4).

Im Hinblick auf die *Selbstkompetenzen* ist der Begriff des Lernens am Modell (Bandura 1976) zentral. Demzufolge erfolgen kognitive Lernprozesse, die entstehen, wenn Individuen sich durch die Beobachtung des Verhaltens anderer Individuen neue Verhaltensweisen aneignen oder bereits angeeignete Verhaltensweisen abändern. Das beobachtete Individuum, und somit auch die oder der Lehrende, wird für Bandura primär zur Erfahrungsquelle. Voraussetzungen für diese Form des sozialen Lernens sind die Fähigkeit, das Modell adäquat wahrnehmen und beobachten zu können (Linden & Hautzinger 1981), und die Kompetenz, das Beobachtete in eigene Verhaltensweisen und Entscheidungen einfließen zu lassen. Damit nehmen Lehrende eine Vorbildwirkung ein, die durch ihre Stiltypisierung, Seriosität, Zuverlässigkeit und Loyalität sichtbar wird.

Was die *Professionskompetenzen* anbelangt, so ist festzuhalten: „Professionalität materialisiert sich gewissermaßen in einer spezifischen Qualität erwachsenenpädagogischer Handlungspraxis, die eine Erhöhung von Handlungsoptionen, Chancenvervielfältigung und die Steigerung von Partizipations- und Zugangsmöglichkeiten zur Folge hat“ (Dewe 2004, S. 324).

Ein zur Profession gehörendes artikuliertes Bewusstsein der gemeinsamen Aufgaben und Verantwortungen wird so zu einer Grundvoraussetzung für eine gelingende Professionalisierung (Hartig 2009). Lehrende müssen daher ständig an der eigenen Professionalität arbeiten.

2.5 AdressatInnenorientierte Medienkompetenz

Der Diskurs, dass Medienkompetenz von besonderer Bedeutung ist, ging im Jahr 2019 in die nächste Phase und rückte erfreulicherweise von der partikularen technischen Allokation weiter ab. Die Bundeszentrale für politische Bildung unterstützt(e) die Medienkompetenz in den Schulen und fügte den Kompetenzen Lesen, Schreiben und Rechnen im Jahr 2015 die Medienkompetenz hinzu (Bundeszentrale für politische Bildung 2015). Diese Position ist jedoch, zumal für jüngere Kinder, nicht unumstritten, wie beispielsweise Spitzer (2012) bemerkt, der auf präventive Maßnahmen verweist, die negative Seiteneffekte implizieren: „Wer in jungen Jahren schon mit den digitalen Medien in Kontakt kommt, lernt auch mit großer Wahrscheinlichkeit schon sehr früh, wie und wo man an all die verbotenen oder zumindest von den Eltern unerwünschten Inhalte kommt“ (ebd., S. 309). Die Medienforschung zeigt, dass hierüber kontrovers diskutiert wird. Jüngst und Dörr (1998) postulieren hierzu, dass sich Mediennutzung in einem diachronen Zyklus entwickelt: Erst sei sie von Begeisterung, anschließend von Ernüchterung geprägt. Die Autoren betonen diesbezüglich den aufkommenden Hype von CBTs und deren Randstellung (Implementierung in Blended-Learning-Konzepte), die im Zeitalter der Pandemien wieder aufgelöst wird. Medienkompetenz wird im Kontext unterschiedlicher Notfallkonzepte zu einer Kernkompetenz, wenn der Schulbetrieb eingestellt werden muss, weil Ansteckungsgefahren die Präsenz unmöglich machen.

Erfolgt ein Blick auf die Definitionen von Medienkompetenz, finden sich in der Literatur verschiedene Ansichten, die hier kurz angeführt werden. Baacke (1996) sieht und beschreibt die Medienkompetenz in vier Dimensionen: Medienkritik, Medienkunde, Mediennutzung und Mediengestaltung. Schorb (2009, S. 52) hingegen definiert Medienkompetenz als „die Fähigkeit, sich Medien anzueignen“. Und Tulodziecki (2010) beschreibt die Fähigkeiten in Kompetenzbereichen und Kompetenzaspekten, die auch andere AutorInnen selektiv betrachten:

- Strukturierung nach Feldern bzw. Bereichen von Medienkompetenz (Baacke 1996),
- Strukturierung nach Dimensionen (Aufenanger 2001),
- Strukturierung nach Medienarten (Spanhel 1999).

Weiter verweist Schorb (2020) auf die Verbindung zwischen Wissen, Bewerten und Handeln (siehe Abbildung 28).

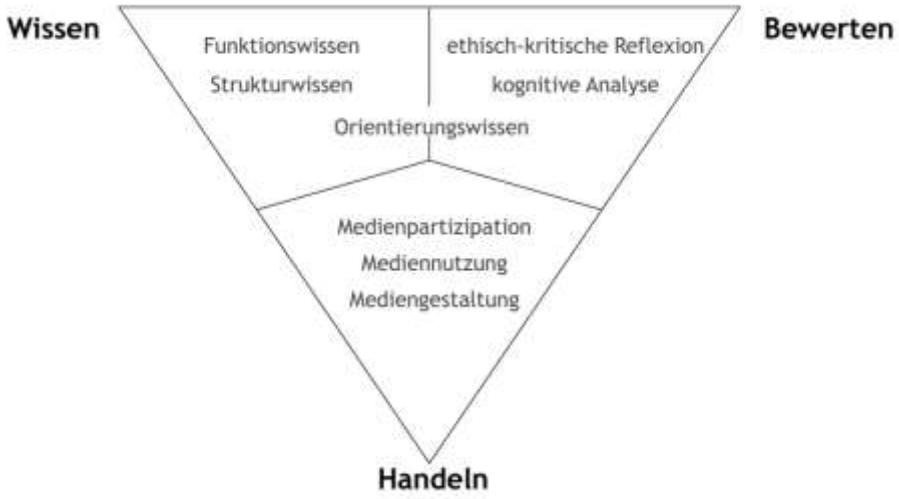


Abb. 28: Drei Aspekte von Medienkompetenz (Schorb 2020, S. 4)

Der Medienkompass Mecklenburg-Vorpommern (2016) „Medienbildung im mittleren und höheren Alter“ untermauert die theoretischen Dimensionen durch ausführliche Fakten. Alterstypische Herausforderungen im Feld von Medienkompetenz sind demnach: Wertschätzung des bestehenden Wissens, gesellschaftliche Partizipation mit und über Medien sowie die Berücksichtigung veränderter ästhetischer Kompetenz aufgrund der abnehmenden Leistungsfähigkeit der Sinnesorgane (Rosenstock 2016). Für den Bildungsgegenstand Medienkompetenz bedeutet dies einerseits milieusensible und lebensweltbezogene Offerten, andererseits aber auch dauerhaft zugängliche Angebote durch eine verlässliche Förderung entsprechender Netzwerke und durch InsiderInnen, die entsprechende Projekte entwickeln, organisieren und zugänglich machen (ebd.).

Das gewachsene Interesse Erwachsener an den neuen digitalen Medien und an Medienbildungsangeboten bietet einen weiteren Hintergrund für die Diskussion um eine Förderung von Medienkompetenz (Burmeister, Rackow & Sparschuh 2013). Aufgrund der Beendigung der beruflichen Laufbahn im Rentenalter gewinnt bei den über 64-Jährigen erwartungsgemäß die allgemeine Weiterbildung an Bedeutung (Pietraß 2009). Dabei splitten sich die Interessen der ab 50-Jährigen im Bereich der beruflichen Bildung in naturwissenschaftliche Themen, EDV-/Computerkurse und allgemeine Bildung (ebd.).

Angesichts der fortschreitenden Kommunikationsmöglichkeiten gewinnt die Nutzung des Internets im Alter zunehmend an Bedeutung. Denn zu den wesentlichen Mehrwerten der Nutzung des Internets gehören der stärkere Kontakt zu der Familie und zu FreundInnen, ein längerer Erhalt der Selbstständigkeit, Möglichkeiten des Zeitvertreibs und des Wissenserwerbs sowie das Einsparen von Zeit (Bothmer 2017). Weiterhin bedeutend sind informelle Lernprozesse und das Interesse an Informationen (Doh 2011), die jedoch einer von Baacke (1996) postulierten Medienkritik bedürfen, damit die Nutzenden die Informations-„Angebote“ werten und verwenden können.

Gänzlich zu kurz – wenn sie überhaupt betrachtet wird – kommt somit die Fokussierung auf den sicherheitskonformen Umgang Erwachsener mit digitalen Medien. Diese Fokussierung ist jedoch erforderlich, da gerade Erwachsene an digitalen Interaktionsprozessen teilnehmen wollen und auch müssen und sie dabei keiner Gefahr ausgesetzt sein sollten.

2.5.1 Der digitale Raum als dynamische Informationsquelle

Die Nutzung des digitalen Raums als Daten-, Nachrichten- und Informationsquelle ist jederzeit und zu jedem Thema möglich, besitzt jedoch eine Ambivalenz. Ein Beispiel hierfür sind Erwachsene, die im Jahr 2017 zu 80 % (n = 990) an der Erhaltung ihrer Gesundheit interessiert waren (Statista 2017) und diesbezüglich auch spezielle Internetangebote nutzten. Um die gewünschten Informationen zu erhalten, nutzten 72 % der Befragten im Alter von 18 bis 80 Jahren Internetportale wie Wikipedia und andere Onlinelexika. 52 % derjenigen, die sich im Internet zu Gesundheitsthemen informierten, waren mit den Ergebnissen meistens oder immer zufrieden, und zusätzliche 44 % waren zumindest teils, teils zufrieden. 65 % bestätigten jedoch auch, dass vertrauenswürdige Informationen schwer zu erkennen seien. Die Hälfte der Befragten war zudem der Ansicht, dass die Informationsfülle und das wachsende Angebot an Gesundheitsinformationen PatientInnen verunsichere, beunruhige und verwirre (Haschke, Westrick & Schwenk 2018).

Damit zeigt sich, dass Erwachsene den digitalen Raum als Wissensspeicher adressieren und bereits Erfahrungen gesammelt haben, um Wissenslücken selbstständig internetbasiert zu kompensieren. Es kann somit davon ausgegangen werden, dass grundlegende Funktionalitäten des Internets als digitaler Raum aufgefasst werden und dass deren Bedienung bekannt und somit prozedurales Wissen vorhanden ist. Sackmann und Winkler (2013) konstatieren ebenfalls, dass verschiedene Generationen die Medien nutzen, die insofern lebensbegleitend sind, und untersetzen diese Annahme mit einer Kategorisierung von unterschiedlichen (Technik-)Generationen (siehe Tabelle 13).

Tab. 13: Definition von Technologiegenerationen (Sackmann & Winkler 2013, S. 497)

Technikgeneration	Geburtskohorte
Frühtechnische Generation	geboren vor 1938
Generation der Haushaltsrevolution	geboren 1939-1948
Generation der zunehmenden Haushaltstechnik	geboren 1949-1963
Computergeneration	geboren 1964-1980
Internetgeneration	geboren ab 1980

Kolland, Wanka und Gallistl (2019) leiten daraus ab, dass Lernende auch in der Lebensphase Alter nicht „aufhören", Technik zu nutzen, sondern dass in jedem Lebensalter diejenigen Technologien genutzt werden, mit denen die Lernenden vertraut sind. Entsprechende Milieuforschungen weisen allerdings eine enge Kopplung zwischen dem sozialen Milieu und motivationspsychologischen Merkmalen aus (Bartz & Tippelt 2004). Hopf (2010) bestätigt dies und verweist zusätzlich darauf, dass neben dem Elternhaus das schulische Umfeld eine Weiterbildungsbeteiligung begünstige. Haben sich Lernende für eine höhere Bildung entschieden bzw. wurde die Entscheidung durch das Elternhaus prädeterminiert (Rech 2006), tragen Bildungserfahrungen zu einer weiteren (Weiter-)Bildungsbeteiligung (Eckert 2009) und damit verbundenen Potenzierung von deren Wirksamkeit bei (Merton 1968).

Auch spielt die Kategorie Geschlecht im geschlechterdifferenten Feld der Technik eine Rolle. Die traditionellen Geschlechterrollen, die vor allem in der Sozialisation der älteren Kohorten eine große Wirksamkeit besaßen, deklarieren Technikaffinität als typisch männliche Eigenschaft und schreiben Technikdistanz meist Frauen zu (FFG 2016). Und ein geschlechtersensibler Blick auf die Internetnutzenden weist in den Jahren 2001 bis 2018 zwar eine steigende Nutzung des Internets insgesamt aus, jedoch auch eine Differenz zwischen den Geschlechtern. So nutzten im Jahr 2018 88 % der Männer und 80 % der Frauen das Internet (Rabe 2019). Eine Untersuchung der Bedeutung des Geschlechts bei der Nutzung von Weiterbildungsangeboten (Anding 2002) macht ebenfalls deutlich, dass die Planung und Umsetzung von Aktivitäten geschlechtersensibel erfolgen sollte (Köster 2009).

2.5.2 Weiterbildung als Instrument der Arbeitsmarktförderung

Betrachtet man den Arbeitsmarkt allein als eine Art Marktplatz, so zeigt sich, dass die Zuordnung von Angebot und Nachfrage hier sowohl quantitative Disproportionalitäten als auch qualitative Dysfunktionalitäten entstehen lässt (Hobbensiefken 1980). Diesen Fehlfunktionen versuchen Arbeitsorganisationen durch eigene Fort- und Weiterbildungsmaßnahmen oder Veränderungen im Zuschnitt von Arbeitsplätzen zu begegnen

(Schuleret et al. 1995). Die Wissensaneignung spielt also eine wichtige Rolle auch für den Arbeitsmarkt und zieht damit zwangsläufig die Weiterbildung in den Fokus der Betrachtungen. Daraus ergibt sich gleichfalls die Aufforderung, unterschiedliche Formen der Weiterbildung auf „ihre eigene Praxis und deren institutionelle und organisatorische Voraussetzungen auf ihre inkludierenden und exkludierenden Wirkungen hin zu prüfen“ (Kronauer 2010). Denn nur durch zielgruppenspezifische Angebote können beispielsweise auch Menschen mit Behinderungen von präventiven Maßnahmen im Kontext von Informationssicherheit profitieren. Hier spielen Faktoren wie die Bildauflösung oder die Lautstärke bei Präsentationsmedien oder behindertengerechte Zugangsmöglichkeiten des Veranstaltungsortes eine essenzielle Rolle, was oft vergessen wird, wenn keine eigene Betroffenheit und keine sozialen Perspektiven vorhanden sind.

Marktwirtschaftlich fokussiert, wird die Kosten verursachende Weiterbildung gern auf Lebenslanges Lernen transferiert, um Kostenvorteile zu nutzen. Weiterbildung wird in diesem Sinne mit dem Lebenslangen Lernen gleichgesetzt.

> „Lifelong learning. The concept of learning as a process that continues throughout life to address an individual’s learning needs. The term is used widely in adult education to refer to learning processes in many forms and at many levels“ (UNESCO 2005, S. 418).

Wolter (2009) weist in diesem Zusammenhang allerdings darauf hin, dass Lebenslanges Lernen als ein internationales bildungspolitisches Konzept gegenüber dem Weiterbildungsbegriff eine eigenständige Begriffsgeschichte und Traditionslinie besitzt, die die Gesamtheit allen formalen, nichtformalen und informellen Lernens über den gesamten Lebenszyklus eines Menschen hinweg einschließt. Dieser Kategorisierung entspricht auch das „Memorandum für Lebenslanges Lernen“ der Europäischen Union aus dem Jahr 2000 (Memorandum über Lebenslanges Lernen 2000).

Feld et al. (2013) weisen darauf hin, dass die Politik und öffentliche Hand vor der Aufgabe stehen, neben den vorschulischen, schulischen, beruflichen und hochschulischen Bildungseinrichtungen eine Infrastruktur zu entwickeln und bereitzustellen, um den Gesellschaftsmitgliedern zur Förderung des Lebenslangen Lernens Informations- und Medienkompetenz zugänglich zu machen. Diese Positionierung ist essenziell, da beschleunigte Innovationszyklen, demografischer Wandel und rascher Wissensverfall in allen gesellschaftlichen Bereichen relevant sind (Quilling & Nicolini 2007). Voraussetzung für Lebenslanges Lernen ist die Verknüpfung individueller und sozial-gesellschaftlicher Interessen im Konzept des Lebenslangen Lernens, das über Lernen Verbindungen zwischen der Sozialzeit und der Eigenzeit, zwischen privatem und öffentlichem Interesse, zwischen ökonomischen Zeitinteressen und pädagogischen Zeitverständnissen herstellt, die kritisch bis hoch konfliktträchtig sind (Schmidt-Lauff 2018). Lebenslanges Lernen darf somit nicht in ein unverbundenes Nebeneinander oder gar Gegeneinander

von zahllosen Einzelaktivitäten auseinanderfallen, vielmehr müssen pädagogische Entscheidungen und Hilfen begründbar und verantwortbar sein und bleiben (Braun, Stübig & Stübig 2018). Hierbei ist zu beachten, dass Angebote so zu konzipieren sind, dass sie auch für Menschen mit Behinderungen zugänglich werden. Entsprechende gesetzliche Regelungen, unter anderem verankert in der UN-Behindertenrechtskonvention (UN-BRK), beinhalten bereits in Art. 24 Abs. 4 die Bildung von Menschen mit Behinderungen als ihr staatlicherseits zu erfüllendes Recht.

Diese Ausführungen machen deutlich, dass Lebenslanges Lernen als ein Bestandteil von Weiterbildung gesehen werden muss, damit auch ArbeitgeberInnen die (Mit-)Verantwortlichkeit für die Qualifizierung ihrer Mitarbeitenden nicht verlieren. Wobei die digitalen Medien hierzu diverse Möglichkeiten bieten: Besteht im Zeitalter der digitalen Medien ein „akutes“ Interesse an der Wissenserweiterung, müssen nur bedingt Präsenzveranstaltungen besucht werden, denn internetbasierte Lernformen machen Online-Lehre möglich. 2,8 Millionen KursteilnehmerInnen aus 119 Ländern auf der Lernplattform Udacity.com (Dpa 2014), eine Million SchülerInnen und 23.000 LehrerInnen mit 90 Millionen angemeldeten Lernminuten (GMT 2018) auf de.khanacademy.org und eine bunte Ansammlung von verschiedenen Lernangeboten auf YouTube machen deutlich, dass das Lernangebot im Internet bereits unüberschaubar angewachsen ist und eine breite NutzerInnenschaft findet (Wind & Breiter 2011). Heutigen Nutzenden steht damit ein Kosmos von Informationen zur Verfügung (Ortner 2016), denn das Internet ist ein schier unbegrenzter Raum, in dem Wissen – in Wissensnetzen kollektiv zusammengetragen (Mohr 2008) und ständig aktualisiert (Hannig 2002) – den Interessierten schnell zur Verfügung gestellt wird. Digital gestütztes Lernen erfolgt heute vermehrt online. Kleinkinder, die sich auf dem Smartphone lustige YouTube-Videos anschauen (Krauthausen 2012), Studierende, die Online-Universitäten nutzen (Beise & Schäfer 2016), oder Erwachsene, die eine Wissenslücke füllen möchten (Kersten-Frisch 2015) – sie alle bedienen sich des Internets als Wissensquelle und haben somit die Möglichkeit, aktuelle Informationen zu finden und jederzeit abzurufen. Spitzer (2012) weist in diesem Kontext jedoch darauf hin, dass eine erfolgreiche Suche vorwissengeleitet ist, denn ohne entsprechendes Vorwissen sei eine Suchanfrage kaum erfolgversprechend. Insofern untermauert Spitzer die Forderung von Gaigl an die Lehrenden, „Methoden und Materialien flexibel auf das Vorwissen, die Erwartungen und Ressourcen der Teilnehmenden abzustimmen“ (Gaigl 2014, S. 43).

3 Entwicklung einer präventiven Maßnahme

> „There are multiple questions a home user could commonly ask about the subject of cyber-attack. What is a cyber-attack? What can be done to protect myself from such an attack? How will I know if I have been a victim?“ (Teymourlouei 2015, S. 678)

Präventive Interaktionen besitzen das Potenzial, das Thema zu adressieren, damit Wissen sukzessiv weiter aufgebaut werden kann, um letztlich Fragen wie die oben genannte beantworten zu können. Im Folgenden werden die Konzeption und Umsetzung einer solchen präventiven Maßnahme dargelegt, die nach ihrem Abschluss auf ihre Wirksamkeit überprüft wurde. Der Anspruch dieser präventiven Maßnahme im Kontext IT-Sicherheit sollte es sein, die Lernenden nicht nur mit wichtigen Informationen in Kontakt zu bringen, sondern sie ein Interesse entwickeln zu lassen, das dazu dienlich ist, Informationen in eigenes Wissen zu verwandeln, um letztendlich die eigenen Kompetenzen zu erweitern (Krebs 1998; siehe auch North 2016). Grotlüschen (2010) beschreibt dies als Herausschälen der übrig gebliebenen Interessen aus einer Reihe von Schalen, da die Interessengenese möglicherweise auch eine Negativkomponente enthalte, und spricht damit diachrone Veränderungen der Bedeutung des Lebenslangen Lernens an (Dellori 2016). Die Weichen hierfür werden nach Pfadenhauer und Kurtz (2010) schon in der Kindheit gestellt.

Aus diesen Einsichten folgt, dass Teilnehmende von präventiven Maßnahmen an das Konzept des selbstgesteuerten Lernens (Bandura 1977) heranzuführen und für die Verantwortung des eigenen Lernprozesses zu sensibilisieren sind (Gaigl 2014). Hilfreich hierzu sind nicht nur Veranstaltungen mit dezidierter Lernfokussierung, sondern auch Interessenorganisationen wie Vereine, die das Lernen ihrer freiwillig engagierten Mitglieder möglich werden lassen, indem sie typischerweise mehr Raum für Interaktionen und Aushandlungsprozesse als andere Organisationsformen eröffnen (Hansen 2008). Welche theoretischen Fundierungen dazu notwendig sind, beschreibt das nächste Kapitel.

3.1 Theoretische Fundierung

Die Entwicklung einer präventiven Maßnahme zur Sensibilisierung von Internetnutzenden für die Gefahren von Cybercrime bedarf einer theoretischen Fundierung, um reale Veränderungen herbeirufen zu können. Hierzu ist es essenziell, die Ergebnisse der theoretischen und empirischen Forschung zu berücksichtigen. In den vorangegangenen Kapiteln wurde sicherheitskonformes Verhalten im Kontext von Cybercrime anhand unterschiedlicher Theorien erklärt, die für die Entwicklung einer präventiven Maßnahme erforderlich sind, in der sicherheitskonforme Verhaltensweisen fokussiert werden. So

machen Petty und Cacioppo (1986) im ELM-Modell deutlich, dass Einstellungsänderungen, die auf einer umfassenden Ausarbeitung von problemrelevanten Argumenten beruhen, beständiger, widerstandsfähiger und verhaltensprädiktiver sind als Einstellungsänderungen, die auf einfachen Hinweisen beruhen.

Im vorliegenden Kontext ist die Vorstellung von Cyberangriffen (ein Spektrum hiervon wurde im Kapitel 2.2 dargestellt) hilfreich, um den Lernenden eine problemrelevante Auseinandersetzung möglich zu machen. Finden Cyberangriffe statt oder haben diese stattgefunden, bedarf es Bewältigungsstrategien (Lazarus & Folkman 1984). Solche Strategien können in präventiven Maßnahmen geübt werden. Erkennt die oder der Lernende durch eigene Erfahrungen, dass er oder sie sich wirksam gegen Cyberangriffe schützen oder – im akuten Fall – sich dagegen wehren kann, so wird gemäß Bandura (1997) die Selbstwirksamkeit in der höchst möglichen Effektivität verbessert (vgl. Banduras Selbstwirksamkeitstheorie im Kapitel 2.3.4). Bevor präventive Maßnahmen angeboten werden, ist jedoch unbedingt zu prüfen, inwieweit nichtbeabsichtigte Nebeneffekte möglich sind und welche Zielgruppe adressiert werden soll. Denn bspw. hat die Drogenprävention in Schulen den Drogenkonsum teilweise noch verstärkt (Spitzer 2015).

Studien zu Schwierigkeiten und erfolgsfördernden Faktoren von Sensibilisierungsmaßnahmen im Kontext von Cybersicherheit sind bisher kaum vorhanden. Abhandlungen, die das Thema in den Fokus ziehen, sind bei Helisch und Pokoyski (2009) zu finden, die jedoch das Thema Lernen nur sehr kurz behandeln und vermehrt E-Learning in den Fokus ziehen. Scholl (2017a) griff diese Positionierung jedoch im Jahr 2017 weiter auf und untersetzt die E-Learning-Strategie durch neue Lernprodukte zu den Themen Sensibilisierung für Social Engineering und Phishing, wobei er darauf hinweist, dass deren Wirksamkeit abgesichert sei. Gleichzeitig verweist Scholl darauf, dass die reine Vermittlung von Informationen bzw. Kenntnissen ohne die Einbeziehung interaktiver Elemente nicht imstande sei, ein anhaltendes Bewusstsein im Kontext IT-Sicherheit zu schaffen, und verweist hierzu auf Studien von SanNicolas-Rocca, Schooley und Spears (2014) sowie der DSV-Gruppe (2006).

Ausführlicher behandeln Khan et al. (2011) unterschiedliche Lernmethoden und auch Medien, die im Sensibilisierungsprozess auf ihre Wirksamkeit geprüft wurden. Hier zeigt sich wiederum, dass Lehrmethoden wie Präsentationen und Diskurse eine Verhaltensänderung bewirken können (siehe Tabelle 14).

Tab. 14: Effektivität der Methoden zur Sensibilisierung für Informationssicherheit (Khan et al. 2011, S. 10863)

S/No.	Tool and technique	Component of know-ledge	Component of attitude change	Component of subjec-tive norms	Component of Intention	Change in behavior	Effectiven-ess Overall
1	Education presentation	✓	✓	✗	✓	✓	4
2	Email messaging	✓	✓	✗	✓	✗	3
3	Group discussion	✓	✓	✓	✓	✓	5
4	Newsletters	✓	✓	✗	✗	✗	2
5	Video games	✗	✓	✗	✓	✗	2
6	CBT	✓	✓	✗	✗	✗	2
7	Posters	✓	✓	✗	✗	✗	2

Dombach und Schmitz (2016) verneinen dies jedoch und verweisen darauf, dass präsentative Sensibilisierungen unzureichend seien und zusätzlich eines Trainings bedürften, wie es in Schulungen zu Softwareprodukten der Fall sei. Diese Position teilt auch Scholl (2017b) und verweist auf Sensibilisierungen und wissensvermittelnde Maßnahmen, die erlebnisorientiert gestaltet sind. Scholl, Fuhrmann und Pokoyski (2016) zeigen gleichfalls auf, dass neben dem theoretischen Ansatz zum Wissenstransfer ein systematisch emotionaler Ansatz zur Kommunikation in teambasierten Anwendungen erforderlich wird. Um in präventiven Maßnahmen zum Kontext Cybersicherheit eine Differenzierung zwischen Sensibilisierung, Training und Bildung vornehmen zu können, sind die Ausführungen von Whitman und Mattord (2008) hilfreich, die bereits im Jahr 2008 Sensibilisierung, Training und Bildung differenzierten und diese theoretische Elemente im Jahr 2017 zu dem Framework „security education training and awareness (SETA)“ zusammenfügten (ebd. 2017, S. 212; siehe Tabelle 15).

Tab. 15: Framework des SETA (Whitman & Mattord 2017, S. 212)

	Education	Training	Awareness
Attribute	Why	How	What
Level	Insight	Knowledge	Information
Objective	Understanding	Skill	Exposure
Teaching method	Theoretical instruction • Discussion seminar • Background reading • Hands-on practice	Practical instruction • Lecture • Case study workshop • Posters	Media • Videos • Newsletters
Test measure	Essay (interpret learning)	Problem solving (apply learning)	• True or false • Multiple choice (identify learning)
Impact timeframe	Long term	Intermediate	Short term

Auch Wilson und Hash (2003) postulieren dieser Kategorisierung und erweitern diese für unterschiedliche Zielgruppen (siehe Abbildung 29).

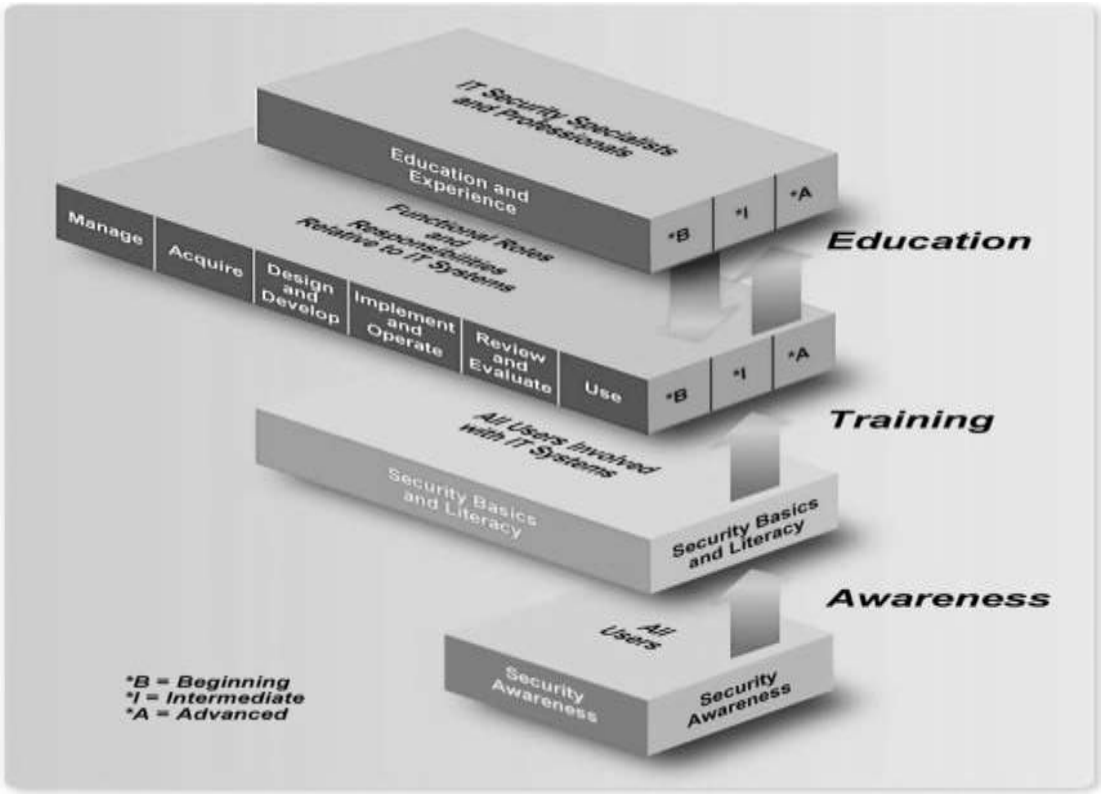


Abb. 29: Das IT-Sicherheits-Lernkontinuum (Wilson & Hash 2003, S. 8)

Gleichfalls machen sie deutlich, dass Awareness das Schaffen von Bewusstsein bedeutet und vom Training zu differenzieren ist: „Awareness is not training. The purpose of awareness presentations is simply to focus attention on security“ (ebd., S. 8). Diese Differenzierung führt weiter als zum Beispiel das von Helisch und Pokoyski (2009) bezeichnete Awareness, das als ein Zusammenspiel zwischen Können, Wissen und Wollen die oben genannten Kategorien noch vermischt (siehe Abbildung 30).

Abb. 30: Security Awareness (Helisch 2009, S. 11)

Jedoch trägt nicht nur die Differenzierung zwischen Sensibilisierung, Training und Bildung zur Wirkung von Maßnahmen bei, sondern auch die Lerninhalte müssen sorgfältig ausgewählt werden. Als mögliche Quelle für Lerninhalte zum Thema Cybersicherheit sind unter anderem die Empfehlungen des US-Cert United States Computer Emergency Readiness Teams zu nennen (McDowell 2018). Diese geben eine mögliche Richtung für den inhaltlichen Aufbau einer Maßnahme vor, wie es in der Tabelle 16 dargestellt ist.

Tab. 16: Tipps für Sensibilisierungsmaßnahmen des US-Cert (McDowell 2018, S. 1)

General Information	**General Security**
- Definitionen	- Verständnis zu Firewalls
- Verständnis zu Service-Providern	- Risiken (Kinder!)
- Öffentlichkeit des Internets	- Gute Sicherheitsgewohnheiten
Attacks and Threats	**Email and Communication**
- Angriffsmethoden und Schutzmaßnahmen	- Funktionalität eines E-Mail-Client
- Recovering nach Cyberattacken	- Social-Media und Cybersecurity
- Risiken im Online-Handel	- Warum können E-Mail-Anhänge gefährlich sein?
Mobile Devices	**Privacy**
- Physischer Schutz von mobiler Technik	- Anonymität
- Risiken mit dem Umgang von USB-Sticks	- Sicheres Löschen von Dateien
- Funktion eines WLAN	- Passwortsicherheit
Safe Browsing	**Software and Applications**
- Zertifikate	- Verständnis zu Voice over Internet Protocol
- Verständnis zu Bluetooth- Technologien	- Risiken zu File File-Sharing Technologien
- Verständnis zu Active Content und Cookies	- Verständnis zu Updates

Hilfreicher ist es jedoch, aktuelle Angriffsmethoden in den Fokus der Betrachtung zu ziehen, wie es in der Abbildung 1 dargestellt und in den vorgelagerten Kapiteln behandelt wurde.

3.2 Entwicklung der präventiven Maßnahme „Der zweite Blick“

In diesem Kapitel wird die Entwicklung der präventiven Maßnahme „Der zweite Blick“ beschrieben und reflektiert. Detailliert wird neben der didaktischen Grundlegung und dem Ablaufplan der Maßnahme der methodische Ansatz des Lernangebotes erläutert.

Das zentrale Ziel dieser Maßnahme ist bei Moallem (2019) zu finden, der dies wie folgt benennt: „A Security Education, Training and Awareness (SETA) programme is designed to reduce the number of security breaches that occur through a lack of employee security awareness“ (ebd., S. 61). Aufbauend auf dem SETA-Framework (Whitman & Mattord 2017) und dem IT Security Learning Continuum (Wilson & Hash 2003) mit dessen Bestandteilen Bildung, Training und Bewusstsein wurde die präventive Maßnahme für eine Experimentalgruppe und eine Kontrollgruppe konzipiert. Denn um die präventive Maßnahme auf ihre Wirkung analysieren zu können, war es notwendig, eine Trennung zwischen Kontoll- und Experimentalgruppe vorzunehmen. Die Kontrollgruppe (KG) nahm lediglich an einer Awareness-Maßnahme teil, in der Cyberangriffe vorgeführt wurden, während die Experimentalgruppe (EG) auch ein Training bekam (siehe Abbildung 31).

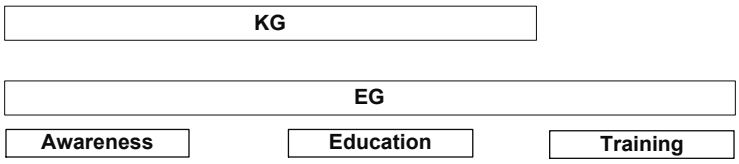


Abb. 31: Gegenüberstellung der Kontroll- und Experimentalgruppe der präventiven Maßnahme

3.2.1 Entwicklungsprozess der präventiven Maßnahme

Der Entwicklungsprozess der präventiven Maßnahme erfolgte auf der Grundlage des Modells des normativen rationalen Handelns (Obrecht 1996). Ausgehend von der aktuellen Situation erfolgreicher Cyberangriffe sollten mögliche TäterInnen und deren Angriffsvektoren dargestellt werden. Dabei sollten solche IT-Sicherheitsrisiken dargestellt werden, aus denen sich Verantwortungen auch im Kontext der Haftung des pädagogischen Personals ableiten lassen.

Phase 1: Situationsanalyse
Aktuelle Lage, Angriffsvektoren
Phase 2: Bewertung und Problemdefinition
IT-Sicherheitsrisiken ohne Intervention: Verantwortung, Haftung, Rentabilität
Phase 3: Zielsetzung und Planung
Lernziele, Interventionsmöglichkeiten, Zielgruppe – Methoden
Phase 4: Entscheidung und Implementierung des Planes
Wissen über Entscheidungen
Phase 5: Evaluation
Wissen über die Wirksamkeit von konkreten Interventionen, Wissen über die Erwünschtheit von konkreten Interventionen

Abb. 32: Prozessmodell der präventiven Maßnahme (nach Obrecht 1996)

Im Folgenden werden die ersten drei Phasen skizziert.

Phase 1 – Situationsanalyse

In der ersten Phase wird die aktuelle Situation im Bereich Cybercrime analysiert und dargestellt, wie sie in den vorliegenden Kapiteln beschrieben wurde (siehe vor allem Kapitel 2.1.2). Die für die Sensibilisierungsmaßnahme zentrale Information lautet: Cyberangriffe sind jederzeit möglich und stellen eine Gefahr für BürgerInnen und Gesellschaft dar. Die Abhandlungen in den vorgelagerten Kapiteln zeigen auf, dass diverse Studien transparent machen, wie leicht Cyberangriffe möglich werden, wenn Risiken nicht bekannt sind und sicherheitskonformes Verhalten defizitär ist. Der Umgang mit Medien bedarf nicht nur einer Perspektive, wie sie von Tulodziecki oder Aufenanger postuliert wird, sondern darüber hinaus eine weitere Fokussierung auf das Thema Informationssicherheit im Kontext von Medienkompetenz.

Phase 2 – Bewertung und Problemdefinition

Die zweite Phase legt den Fokus auf die Frage der Notwendigkeit oder Verzichtbarkeit von präventiven Maßnahmen. Die für die Sensibilisierungsmaßnahme zentrale Einsicht lautet: Ein Verzicht auf solche Maßnahmen würde bedeuten, dass Wissensvorteile weiter bei den Cyberkriminellen verbleiben und sicherheitskonformes Verhalten weiter uneinschätzbar bleibt (siehe Kapitel 2.1.4). Aufgrund der teilweise hohen Komplexität von Cyberangriffen kann davon ausgegangen werden, dass derartige Themen nicht von jeder Person erschlossen werden können und gerade älteren Menschen verschlossen bleiben. Damit besteht ein unbekanntes und somit unkalkulierbares Risiko, dem nur durch Auflösung der Kompliziertheit begegnet werden kann.

Phase 3 – Zielsetzung, Planung und Studie

Die dritte Phase umfasst die Definition der fokussierten Ziele, Zielgruppen und angedachten Methoden der Stoffvermittlung und der Planung. Der Zusammenhang zwischen Zielen, Inhalten, Methoden und den Bedingungen, denen der Vermittlungsprozess unterliegt, ist entscheidend für eine erfolgreiche Stoffvermittlung (Zeuner 2011). Diesbezüglich bedarf es eines fundierten Erstellungsprozesses, der den Ablauf deutlich macht.

3.2.2 Erstellungsprozess einer präventiven Maßnahme

Erstellungsprozesse können sequenziell und nach anschließender Evaluation iterativ erfolgen. Folgende Sequenzen sind möglich, wobei die Theorien der Verhaltensbeeinflussung die Grundlage für die Erstellung bilden (siehe Kapitel 2.3).

- Die Recherche und Aufbereitung der verfügbaren Informationsquellen bilden die erste Sequenz in dieser Phase, für die des Weiteren eine Sichtung bereits

existierender Maßnahmen und deren theoretischer Fundierung notwendig ist (Vierbuchen 2015).

- Die Entwicklung von Zielen sowie die Planung der präventiven Maßnahme bilden die zweite Sequenz.
- Die Durchführung der Maßnahme und der Studie erfolgt in der dritten Sequenz.
- Die Überarbeitung der Maßnahme aufgrund der in der Evaluation gewonnenen Erkenntnisse findet in der vierten Sequenz statt.

Nachfolgend werden die aufgeführten Sequenzen kontextbezogen beleuchtet.

3.3 Theorien der Verhaltensbeeinflussung als Grundlage

Die im Kapitel 2.3 dargelegten Theorien ziehen die Möglichkeit in Betracht, Verhalten ändern und persistent halten zu können. So weist das Elaboration-Likelihood-Modell (ELM) von Petty und Cacioppo (1986) darauf hin, dass Einstellungsänderungen, die auf einer umfassenden Ausarbeitung von problemrelevanten Argumenten beruhen, beständiger, widerstandsfähiger und verhaltensprädiktiver sind als Einstellungsänderungen, die auf einfachen Hinweisen beruhen. Diesbezüglich werden Möglichkeiten implementiert, die es erlauben, sich umfassend mit dem Thema auseinanderzusetzen, bspw. in Form von implementierten Reflektionsphasen für die Lernenden durch Diskurse. Durch den erhöhten kognitiven Aufwand für die Lernenden ist eine Verhaltensänderung nach dem Heuristic Systematic Model (HSM) von Eagly und Chaiken (1993) beständiger. Unterstützend sollen den Lernenden gemäß der Protection Motivation Theory (PMT) Copingstrategien vermittelt werden, die sicherheitskonform (adaptiv) und nicht sicherheitskonform (maladaptiv) im Verhalten sind, da beide in jeglichem Problemlösungsprozess involviert und nie voneinander getrennt sind (Lazarus & Lazarus 2006). Ajzen und Fishbein (1980) weisen in ihrer Theorie auf unterschiedliche Bedingungen hin, die Verhalten beeinflussen können. Verhaltensänderungen sind unter anderem fundiert durch die Einstellung und die wahrgenommene Verhaltenskontrolle, die sich nach Niemand (2014) aus dem Sammelkonstrukt der Selbstwirksamkeit Banduras (1994) und dem Kontrollüberzeugungs-Konstrukt nach Rotter (1975) zusammensetzen lässt. Für die Konzeption der Maßnahme bedeutet dies, ausgewählte Cyberangriffe so auszuwählen und vorzuführen, dass keine Kontrollverluste entstehen und die Selbstwirksamkeit durch präsentierte und eigene Erfahrungen gestärkt werden kann. Wird eine Verhaltensänderung erreicht, ist es von Interesse, in wie weit die Verhaltensänderung durch die Maßnahme persistent gehalten werden kann. Die entsprechende Theorie des transtheoretischen Modells von Prochaska und DiClemente wurde im Kapitel 2.3.9 behandelt und soll in der

Stufe “preparation“ nach 30 Tagen überprüft werden, wie es in der Tabelle 9 veranschaulicht ist. Das Zusammenspiel der verschiedenen Theorien als Basis der präventiven Maßnahme ist in der folgenden Abbildung 33 dargestellt.

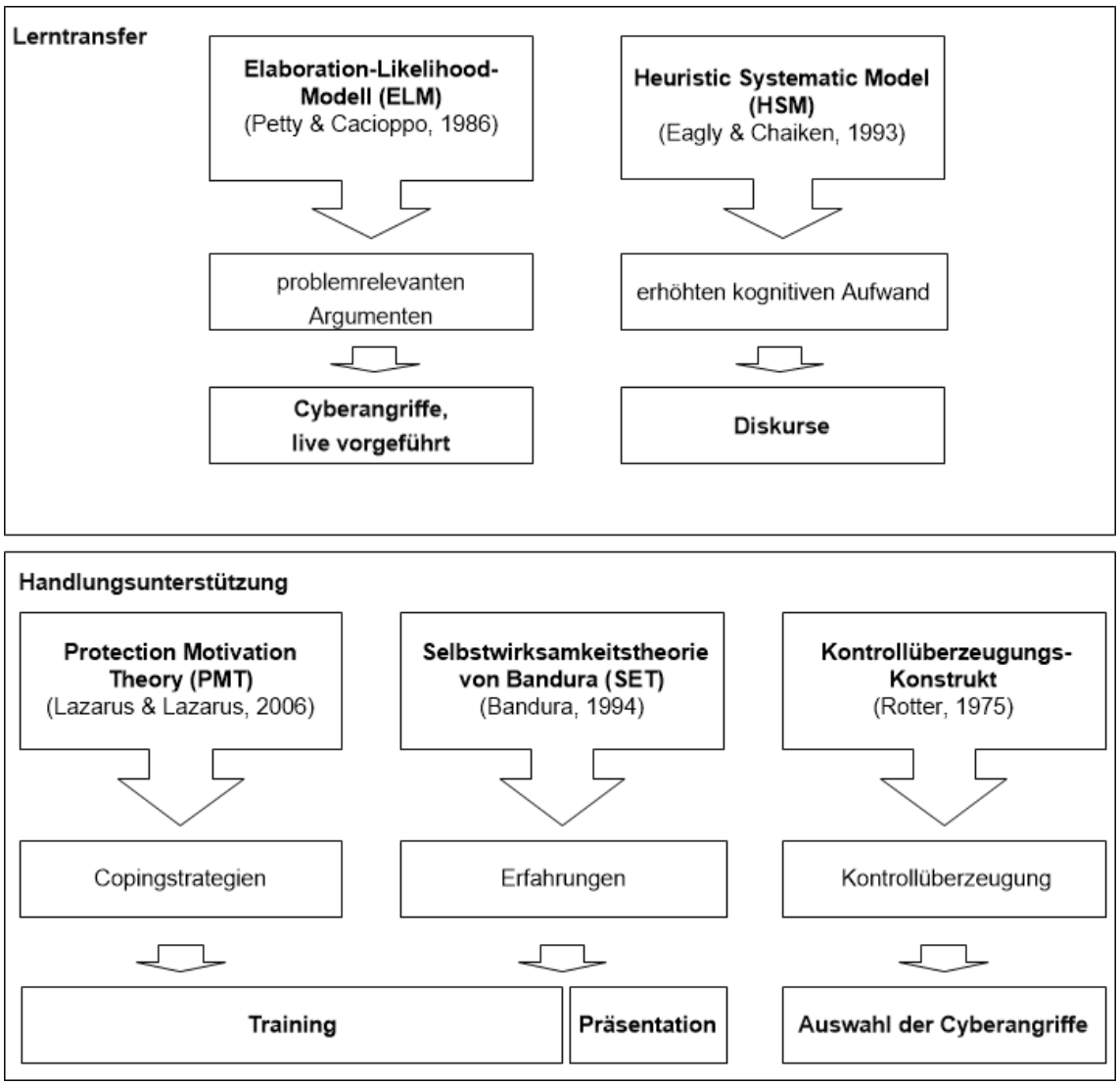


Abb. 33: Theorien der Verhaltensbeeinflussung als Grundlage der präventiven Maßnahme

3.4 Recherche und Aufbereitung

Für die hier vorgestellte präventive Maßnahme wurden Inhalte gewählt, die aktuell sind, einen zeitlichen Bezug haben und Cyberangriffe realitätsnah darstellen. Das Thema Cyberangriff wurde hierzu möglichst formal betrachtet (von den konkreten Kontexten realer Angriffe dekontextualisiert), modellhaft dargestellt und forschungsbezogen untersetzt (mit weiterem Wissen kontextualisiert). Für die Recherche wurden internationale Internetquellen, die durch unterschiedliche Protokolle (http, https, ftp) erreichbar sind, genutzt. Das Material wurde hierzu geprüft, aufgrund der Kompliziertheit einer didaktischen Reduktion unterzogen, in didaktische Methoden eingearbeitet und in den Ablauf der präventiven Maßnahme integriert.

3.5 Lernziel und Methoden

Das Ziel der präventiven Maßnahme war es, bei den Teilnehmenden ein sicherheitskonformes geplantes Verhalten zu bewirken, das langfristig persistent ist und auf einem Erkennen der aktuellen Situation und einer möglichen Betroffenheit beruht. Hierzu bedurfte es einer Auflösung der Kompliziertheit von Cyberangriffen, die durch eine didaktische Reduktion möglich wurde. Die folgende Abbildung zeigt in Anlehnung an Riedl (2000), wie die didaktische Reduktion im Kontext von Schutzmaßnahmen zu Cybercrime umgesetzt wurde.

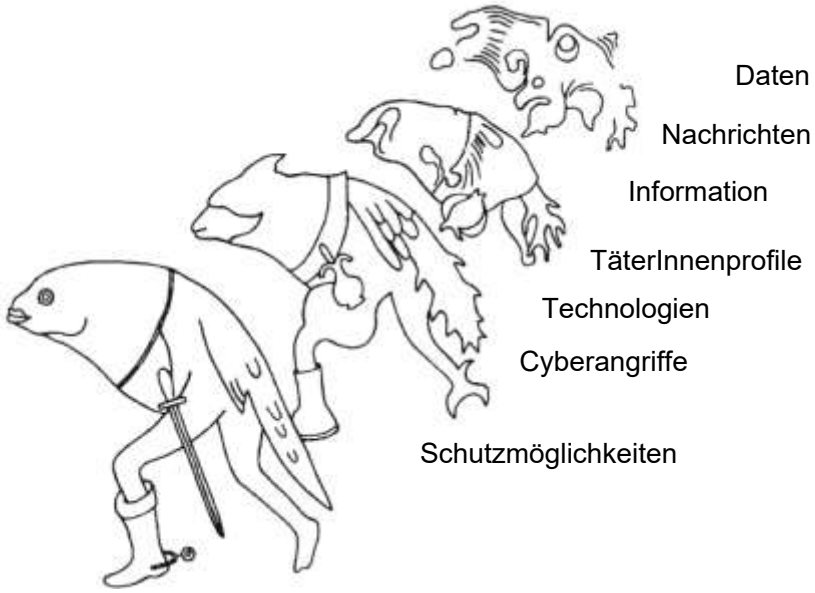


Abb. 34: Didaktische Reduktion (in Anlehnung an Riedl 2000, S. 73)

Hierbei galt es folgendes zu berücksichtigen: „However, a growing element of the knowledge that needs to be learnt for contemporary digitised work cannot be experienced directly. It is opaque, hidden or abstracted in some way and, therefore, individuals cannot be directly experience it“ (Billett 2018, S. 198). Denn Medien besitzen das Potential, Kompliziertheit aufzulösen, wenn sie, wie in der präventiven Maßnahme, exemplarisch gegenwarts- und zukunftsbedeutend eingesetzt werden (siehe Abbildung 35).

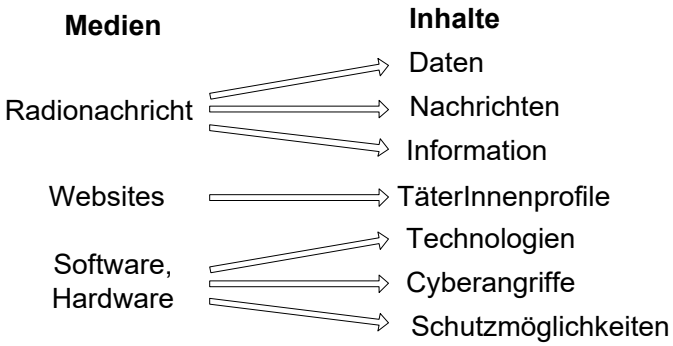


Abb. 35: Die Beziehung zwischen Medien und Inhalten in der präventiven Maßnahme

Der Einsatz von Medien kann in unterschiedliche Methoden integriert werden. Allerdings bedeutet die wirksame Gestaltung des Lernens nicht nur die Reduktion der Kompliziertheit, sondern auch die Granularität der Lernziele, die sukzessiv konzipiert werden müssen. Hilfreich hierzu ist es, die Lernziele, wie von Edelmann und Möller (1977) vorgeschlagen, in Richt-, Grob- und Feinziele zu unterteilen.

Richtziel: Kompetenzentwicklung nach Abschluss der Maßnahme

Das Richtziel der Maßnahme war die Entwicklung einer adressorientierten Medienkompetenz im Kontext von Cybercrime, die eine Wirkung auf das geplante eigene Verhalten hat. Die Maßnahme wäre also dann erfolgreich in Bezug auf ihr Richtziel, wenn folgende Äußerung von Abawajy zutreffen würde: „After completing the training almost all of the participants had the correct idea about phishing and the dangers it poses both to the individual and to an organisation“ (Abawajy 2012, S. 247).

Grobziel: Kompetenzentwicklung nach Abschluss eines Moduls

Die Maßnahme bestand aus sechs Modulen: Theoretisches Wissen, Social Engineering, Cyberangriffe auf Infrastrukturen und Übungen zu Schutzmöglichkeiten (EG). Für jedes Modul wurden vorab Lernziele festgeschrieben:

1. Das Lernziel des ersten Moduls bestand darin, dass die Teilnehmenden die Begriffe Daten, Nachricht und Information definieren und selbst korrekt nutzen können. Dieses Lernziel war essenziell, da die folgenden Module auf dieses Vorwissen aufbauten und einer intersubjektiven Übereinstimmung bedurften, um die genannten (und weitere) Begriffe in den richtigen Kontext setzen zu können. In den vorgelagerten Kapiteln wurden die Generierung von Informationen als auch die Information selbst als besonders schützenswert hervorgehoben.
2. Das Lernziel des zweiten Moduls war es, dass die Teilnehmenden Social-Engineering-Angriffe zu identifizieren und abzuwehren vermögen. Hierzu wurde das Victim Communication Stack aufgenommen und in den Kontext von Social Engineering gesetzt (siehe Abbildung 9). Das Thema Social Engineering wurde

hierzu mithilfe der identitätstheoretischen Didaktik in mögliche Betroffenheitskontexte gesetzt, um eine maximale Zielgruppe zu erreichen.

3. Das Ziel der Module 3-6 lautete, die Teilnehmenden zu befähigen, technische Cyberangriffe zu erkennen und abzuwehren. Mögliche Cyberangriffe wurden im Kapitel 2.2 ausführlich behandelt. Die Auswahl der Beispiele bot die Möglichkeit, exemplarische, gegenwartsbezogene und zukunftsbedeutende Inhalte gemäß der bildungstheoretischen Didaktik (Klafki 1964) erlebbar zu machen, indem sie vorgeführt werden.
4. Gleichfalls wurde HackerInnenequipment vorgestellt, um auch kinästhetische Lerntypen zu erreichen.
5. Das letzte Modul gab den Teilnehmenden der EG die Möglichkeit, selbst präventive Schutzmaßnahmen auszuwählen und zu diskutieren.

Feinziel: Kompetenzentwicklung nach Realisierung der jeweiligen Kompetenzstufe

Um zu beschreiben, dass Teilnehmende Kompetenzen in den Bereichen Wissen, Verständnis, Anwendung, Analyse, Synthese und Beurteilung erworben haben, lassen sich unterschiedliche Formulierungen nutzen wie:

- kann erläutern,
- kann einordnen,
- kann anwenden,
- kann analysieren,
- kann lösen,
- kann beurteilen (Bloom 1976).

Die Formulierungen beschreiben die unterschiedlichen Taxonomie- und Kompetenzstufen, die sukzessiv aufeinander aufbauen. Gleichzeitig macht die Art der aktiven verbalen Beschreibung den Übergang vom deklaratorischen zum prozeduralen Wissen sichtbar. Sie verdeutlicht ebenso die Unabdingbarkeit der intersubjektiven Übereinstimmung über die Begrifflichkeiten als Voraussetzung für einen aufkommenden Diskurs.

Die Lernenden sollten zu einem Wechselspiel zwischen Vortrag, Live-Vorführungen, Diskursen und Spaß eingeladen werden (EG), denn: „Information security awareness level can be increased and sustained through multiple delivery methods“ (Abawajy 2012, S. 247). Die Arbeitsgemeinschaft ‚Betriebliche Weiterbildungsforschung‘ entwickelte eine Handlungsanleitung für Referentinnen und Referenten zur Ausgestaltung von Modulen, die das Feinziel, die Methode und die Sozialform des Lernens adressiert (Aulerich et al. 2004).

Die Maßnahme für die EG unterteilte sich in sechs Module von je 30 Minuten. Zwischen den Modulen waren 10-minütige Pausen implementiert, um einen informellen Diskurs stattfinden zulassen (siehe Abbildung 36).

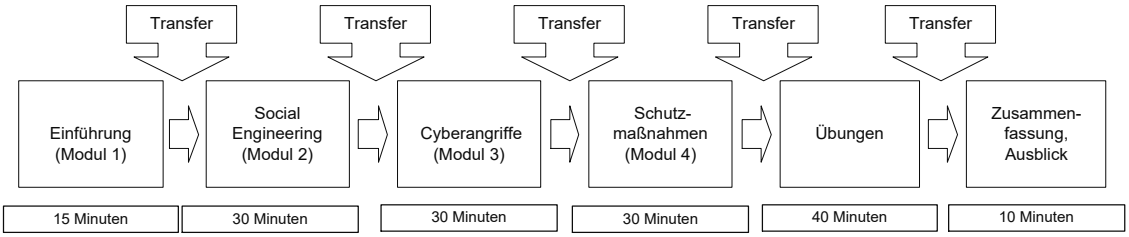


Abb. 36: Ablauf der präventiven Maßnahme für die EG

Die Maßnahme für die KG präsentierte die gleichen Cyberangriffe, jedoch ohne detaillierten Transfer (siehe Tabellen 17-20) und ohne dass Sicherheitsmaßnahmen am Ende geübt wurden (siehe hierzu Abbildung 37).

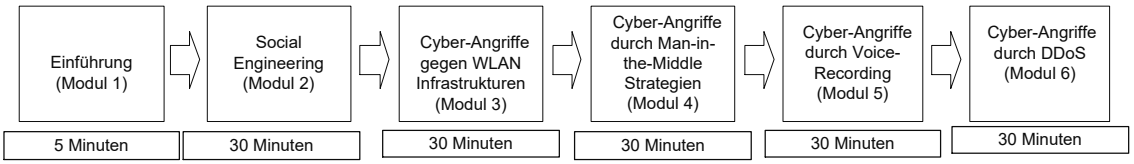


Abb. 37: Ablauf der präventiven Maßnahme für die KG

Das Konzept wird dargestellt in den folgenden Tabellen 17 bis 20.

Tab. 17: Feinziel und Methoden des Moduls 1 für die EG (in Anlehnung an Aulerich et al. 2004, S. 86)

Lernzieltaxonomie		Beispiele für Feinzielformulierungen	Methoden, Medien; Sozialformen des Lernens	Beispiele für die Formulierung
1	**Kompetenz zum Wissenserwerb** Fachbegriffe definieren können	… verfügt über … kennt … weiß	Vortrag, Präsentation einer Radionachricht, Diskussion	… informieren … anhören … ansehen
2	**Transfer** Abgrenzung von anderen Begriffen: Information, Nachrichten, Daten	… kann erläutern … kann einordnen … kann systematisieren … kann demonstrieren … kann darlegen … kann wiederholen … kann zusammenfassen … kann begründen … kann erklären	Team-/Gruppenarbeit, Diskussion in Kleingruppen, selbstorganisiertes Lernen mittels Internet	… bearbeiten … verarbeiten … erarbeiten
3	**Handlungskompetenz** Nachrichten, Information, Daten erstellen können	… kann anwenden … beherrscht … kann entwerfen … kann entwickeln … kann erstellen … kann konzipieren … kann durchführen	Diskurse über Information, Daten, Nachrichten führen	… bearbeiten … verarbeiten … erarbeiten … trainieren/ üben … präsentieren

Im zweiten Modul erfolgte die Darstellung von Social Engineering, dessen Feinziele in der Tabelle 18 dargestellt sind.

Tab. 18: Feinziel und Methoden des Moduls 2 für die EG (in Anlehnung an Aulerich et al. 2004, S. 86)

Lernzieltaxonomie		Beispiele für Feinzielformulierungen	Methoden, Medien; Sozialformen des Lernens	Beispiele für die Formulierung
1	**Kompetenz zum Wissenserwerb** Social Engineering - Angriffe erkennen können	… verfügt über … kennt … weiß	Vortrag, Präsentation von Angriff-Szenarien und Forschungsergebnissen (z.B. Tischer et al., 2013), Diskussion	… informieren … anhören … ansehen
2	**Transfer** Manipulationsversuche verstehen können	… kann erläutern … kann einordnen … kann systematisieren … kann demonstrieren … kann darlegen … kann wiederholen … kann zusammenfassen … kann begründen … kann erklären	Diskussion in Kleingruppen, selbstorganisiertes Lernen mittels Internet	… bearbeiten … verarbeiten … erarbeiten
Lernzieltaxonomie		**Beispiele für Feinziel-formulierungen**	**Methoden, Medien; Sozialformen des Lernens**	**Beispiele für die Formulierung**
3	**Handlungs-kompetenz** Social Engineering-Angriffe abwehren können	… kann anwenden … beherrscht … kann entwerfen … kann entwickeln … kann erstellen … kann konzipieren … kann durchführen	selbstorganisiertes Lernen mittels Internet, Präsentation der erarbeiteten Schutzmaßnahmen	… bearbeiten … verarbeiten … erarbeiten … trainieren/üben … präsentieren

Die Module 3-6 beschäftigten sich mit technischen Cyberangriffen (siehe Tabelle 19).

Tab. 19: Feinziel und Methoden der Module 3-6 für die EG (in Anlehnung an Aulerich et al. 2004, S. 86)

Lernzieltaxonomie		Beispiele für Feinzielformulierungen	Methoden, Medien; Sozialformen des Lernens	Beispiele für die Formulierung
1	**Kompetenz zum Wissenserwerb** Cyberangriffe erkennen	… verfügt über … kennt … weiß	Livevorführung von Cyberangriffen	… informieren … anhören … ansehen
2	**Transfer** Cyberangriffe verstehen von: WLAN-Angriff, WLAN-Tracking, Media Dropping, Dumpster Diving, Waterholing, Phishing	… kann erläutern … kann einordnen … kann systematisieren … kann darlegen … kann wiederholen … kann zusammenfassen … kann begründen … kann erklären	Team-/Gruppenarbeit, Diskussion in Kleingruppen, selbstorganisiertes Lernen mittels Internet	… bearbeiten … verarbeiten … erarbeiten
3	**Handlungs-kompetenz** Cyberangriffe abwehren können	… kann anwenden … beherrscht … kann entwerfen … kann entwickeln … kann erstellen … kann konzipieren … kann durchführen	selbstorganisiertes Lernen mittels Internet, Präsentation der Abwehrmaßnahmen	… bearbeiten … verarbeiten … erarbeiten … trainieren/üben … präsentieren

Im letzten Modul (siehe Tabelle 20) erfolgte die Auseinandersetzung mit den unterschiedlichsten Schutzmaßnahmen, indem diese den Angriffstopologien aus der Tabelle 19 zugeordnet wurden.

Tab. 20: Feinziel und Methoden des Moduls 4 für die EG (in Anlehnung an Aulerich et al. 2004, S. 86)

Lernzieltaxonomie		Beispiele für Feinzielformulierungen	Methoden, Medien; Sozialformen des Lernens	Beispiele für die Formulierung
1	**Kompetenz zum Wissenserwerb** Schutzmaßnahmen zuordnen	… verfügt über … kennt … weiß	Vortrag, Präsentation von Schutzmaßnahmen, Diskussion	… informieren … anhören … ansehen
2	**Transfer** Schutzmaßnahmen anwenden	… kann erläutern … kann einordnen … kann systematisieren … kann demonstrieren … kann darlegen … kann wiederholen … kann zusammenfassen … kann begründen … kann erklären	Team-/Gruppenarbeit, Diskussion in Kleingruppen, selbstorganisiertes Lernen mittels Internet	… bearbeiten … verarbeiten … erarbeiten
3	**Handlungskompetenz** Schutzmaßnahmen entwickeln können	… kann anwenden … beherrscht … kann entwerfen … kann entwickeln … kann erstellen … kann konzipieren … kann durchführen	selbstorganisiertes Lernen mittels Diskurs, Präsentation der präventiven Schutzmaßnahmen	… bearbeiten … verarbeiten … erarbeiten … trainieren/üben … präsentieren

3.6 Ablauforganisation

Für den Ablauf der präventiven Maßnahme wurde das OIDÜR-Modell von Mutzeck (2007) herangezogen, da es sich als Mikrostruktur von Trainingsphasen und damit als Bestandteil von Trainings (z.B. LehrerInnentrainingsprogramm Kooperative Beratung) bewährt hat und in der Erwachsenbildung gut einsetzbar ist. Vierbuchen (2015) weist zwar darauf hin, dass das Modell bisher noch keiner wissenschaftlichen Fundierung durch Evaluation unterzogen wurde, doch auch sie unterstreicht, dass vorhandene Vorteile wie die Vereinigung der unterschiedlichen Lerntheorien und die damit erzielte größtmögliche Effektivität für die Arbeit mit diesem Modell sprechen. Das OIDÜR-Modell gliedert sich in folgende Phasen für die Experimentalgruppe (EG):

Orientierung -> **I**nformation -> **D**emonstration -> **Ü**bung -> **R**ückmeldung – Reflexion.

Die Orientierungsphase (15 Minuten) diente in der präventiven Veranstaltung der Annäherung an die vorhandene Zielgruppe und der Reflektion der bei den Teilnehmenden vorhandenen Erfahrungen. Selbst erlebte Cyberangriffe konnten kurz besprochen und als Opener genutzt werden.

Die Teilnehmenden wurden anschließend informiert, welche Inhalte Bestandteil der Themenfokussierung sind und welche Inhalte zusätzlich implementiert werden können. Die Phase der Information (30 Minuten) diente dem Transparentmachen der Quellen und Unterlagen. In den Demonstrationsphasen (je 30 Minuten) erfolgte eine Vorstellung von Beispielen durch Livevorführungen von Cyberangriffen. Die Übungsphase in der EG (30 Minuten) diente dem Reflektieren der verstandenen Lerninhalte, denn: „Erwachsene

behalten wenig im Gedächtnis, was sie nur hören; mehr was sie hören und sehen (zum Beispiel schriftlich oder im Film); am meisten, was sie selbst erarbeiten. Aktivität erhöht den Lernerfolg“ (Siebert 1977, S. 132). In der letzten Phase des Reflektierens ging es um das „Erleben und Erkennen von Beziehungs- und Wirkungszusammenhängen durch die Rekonstruktion und Reflektion“ (Mutzeck 2007, S. 414).

Inwieweit statistisch signifikante Unterschiede zwischen der EG und KG vorhanden waren, wird in den nächsten Kapiteln beleuchtet.

4 Hypothesen

Das Ziel dieser Forschungsarbeit liegt in der Überprüfung der Wirksamkeit einer präventiven Maßnahme. Die übergreifende Fragestellung der Untersuchung lautet: Wirkt sich die Teilnahme an der präventiven Maßnahme „Der zweite Blick“ mit anschließendem Training positiver auf die Faktoren Einstellung, Urteilsfähigkeit, Kontrollüberzeugung und Selbstwirksamkeit im Kontext von IT-Sicherheit und diesbezüglich auf ein geplantes Verhalten aus, als die reine Präsentation von Cyberangriffen? Eine positive Beantwortung dieser Frage würde bedeuten, dass methodisch untersetzte präventive Maßnahmen wirksamere Effekte erzielen und somit als Bestandteil präventiver Arbeit in der Schadensverhütung von Cyberangriffen anderen Maßnahmen vorzuziehen sind. Die Vorgehensweise in dieser Arbeit ist hypothesenüberprüfend, sodass nachfolgend auf der Grundlage der im folgenden Kapitel operationalisierten Zielkriterien gerichtete Hypothesen formuliert werden.

4.1 Erster Hypothesenkomplex: Messinstrumente

Die ersten Hypothesen beziehen sich auf die selbst entwickelten Skalen, die Bestandteil des in dieser Studie eingesetzten Fragebogens sind. Da die ersten Hypothesen die Erhebungsinstrumente validieren, erfolgt die Einteilung in a und b.

4.1.1 Hypothese 1: Faktorenstruktur der selbst entwickelten Skalen

Im Fragebogen zum geplanten Verhalten gehören 26 der vorhandenen Items zu verschiedenen Skalen des geplanten Verhaltens und erheben somit die Aspekte Einstellung, Urteilsfähigkeit, Kontrollüberzeugung und Selbstwirksamkeit im Kontext von IT-Sicherheit. Die Items wurden hierzu aus dem Fragebogen von Hiemisch (2017; vgl. Anhang 1) entnommen, um diese nach erfolgter Dimensionsreduzierung und Dimensionsabgrenzung den oben genannten Skalen (explorative Faktorenanalyse) zuordnen zu können. Die diesbezügliche Hypothese ist nachfolgend als H1 formuliert und wird in der Abbildung 38 visualisiert. Ziel ist es, die Angemessenheit und Zulässigkeit dieser Operationalisierung durch die Konstruktvalidität zu untermauern.

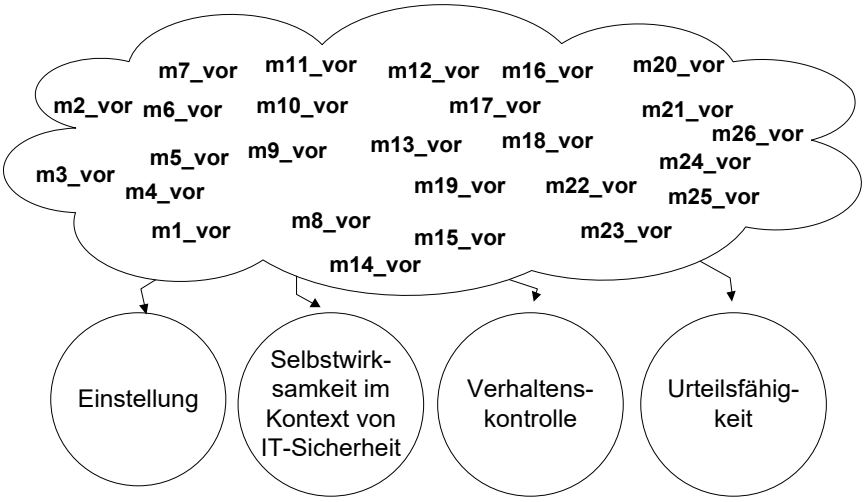


Abb. 38: Faktorenanalyse des geplanten Verhaltens

Um das Vorgehen zu reflektieren, ist es notwendig, auf mögliche Fehlerquellen zu achten (Fahrenberg 2002). Typische Operationalisierungsfehler sind nach Fahrenberg (ebd., S. 352):

1) „Fehler der unzureichenden Referenz (ein Konstrukt hat mehr Bedeutungskomponenten als durch die verwendete(n) Variable(n) erfasst sind)“,
2) „falsche Spezifikationen (die verwendete Variable gehört nicht zu dem Zielkonstrukt)“,
3) „Überschussbedeutung (die verwendete Variable trägt auch Bedeutungskomponenten anderer Konstrukte, die dann fälschlicherweise dem Zielkonstrukt zugeschrieben werden)“.

Es wird vermutet, dass sich die entwickelten Fragen zu übergeordneten Skalen zusammenfassen lassen. Die inhaltliche Hypothese lautet demnach:

H1: Die aus den Theorien SET, FAT, TRA und TPB abgeleiteten Variablen, die das geplante Verhalten im IT-Kontext erfassen sollen, lassen sich in übergeordnete Faktoren zusammenfassen.

Die aus H1 abgeleiteten statistischen Hypothesen lauten:

H0: V = 1

H1: V > 1

V = Faktoren

4.1.2 Hypothese 2: Faktorenstruktur der selbst entwickelten Skalen

Ziel ist es auch hier, die Angemessenheit und Zulässigkeit dieser Operationalisierung durch die Konstruktvalidität zu untermauern. Die zweite Hypothese (H2) bezieht sich auf den ebenfalls neu entwickelten Fragebogen zum Teilnahmegrund der ProbandInnen. Dabei wird zwischen einer themenbezogenen und einer nicht themenbezogenen Teilnahmemotivation unterschieden. Denn neben dem Bedürfnis nach themenbezogener

Weiterentwicklung kann die Teilnahme auch aus anderen Gründen erfolgen, beispielsweise um sich ein soziales Netzwerk aufzubauen oder zu erhalten (Kaufmann & Windany 2013) oder um unterhalten zu werden. Es wird vermutet, dass diese Items sich den
jeweiligen übergeordneten Skalen zuordnen lassen (siehe Abbildung 39).

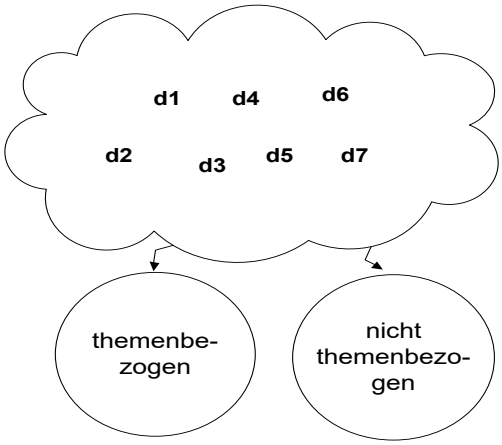


Abb. 39: Faktorenanalyse der Beweggründe der Teilnahme

Die inhaltliche Hypothese lautet demnach*:*

H2: Die auf theoretischer Grundlage abgeleiteten Items, die die Teilnahmegründe erfassen sollen, lassen sich in Skalen zu den Faktoren themenbezogen vs. nicht themenbezogen abstrahieren.

Die aus H2 abgeleiteten statistischen Hypothesen lauten:

H0: $T_{\not{I}\not{N}} = 0$

H1: $T_{\not{I}\not{N}} \neq 0$

$T_{\not{I}}$ *= Faktoren der themenbezogenen Teilnahme*

$T_{\not{N}}$ *= Faktoren der nicht themenbezogenen Teilnahme*

4.2 Zweiter Hypothesenkomplex: gesamte Stichprobe

Die übergreifende Annahme des zweiten Hypothesenkomplexes ist, dass eine stärkere Beeinflussung des geplanten Handelns durch die Schulung der Experimentalgruppe stattfindet, als es bei der Kontrollgruppe der Fall ist.

4.2.1 Hypothese 3: Einstellungsänderung

Gelerntes auf neue Gegenstandsbereiche zu übertragen, bedarf eines Transfers des Gelernten, der durch spezielle Lernsettings unterstützt werden kann (Hansen 2008).

Hillenbrand, Melzer und Hagen (2013) weisen darauf hin, dass Einstellungsänderungen mit Wissen und Handlungskompetenzen verknüpft sein müssen, und verweisen damit auf die Studie von Dreyer (2018). Die Studie von Forlin und Chambers (2011) zeigt, dass die reine Zunahme von Fachwissen noch keine Einstellungsänderung

bewirkt. Im Kapitel 2.3.1 wurde hierzu herausgearbeitet, dass Einstellungsänderungen, die auf einer umfassenden Ausarbeitung von problemrelevanten Argumenten beruhen, als beständiger gelten als Einstellungsänderungen, die auf einfachen Hinweisen beruhen (Petty & Cacioppo 1986). Es wird diesbezüglich vermutet, dass eine Einstellungsänderung eher stattfindet, wenn, wie für die EG konzipiert, eine subjektive Auseinandersetzung mit dem Thema stattfindet. Die inhaltliche Hypothese lautet dementsprechend:

H3ab: Die Lernenden der EG, die die präventive Maßnahme absolvieren, verändern sowohl kurzfristig als auch längerfristig ihre Einstellung stärker als die Lernenden der KG, die nur Cyberangriffe präsentiert bekommen.

Die statistischen Hypothesen lauten:

Hypothese 3a: im Prä-Post-Vergleich

H0: $\mu^{E}2EG = \mu^{E}2KG$

H1: $\mu^{E}2EG > \mu^{E}2KG$

Hypothese 3b: im Prä-Post-Follow-up-Vergleich

H0: $\mu^{E}3EG = \mu^{E}3KG$

H1: $\mu^{E}3EG > \mu^{E}3KG$

E = Einstellung im Kontext von IT-Sicherheit

4.2.2 Hypothese 4: Urteilsfähigkeit

Die Urteilsfähigkeit im Kontext von IT-Sicherheit entscheidet, wie sich InterakteurInnen sicher in der digitalen Welt bewegen, digitale Produkte bewerten oder digitale Infrastrukturen nutzen (siehe Kapitel 2.3.2). Für die Erforschung der Urteilsfähigkeit von RezipientInnen eignen sich kognitive Informationsverarbeitungsmodelle, wie sie aus der Wirkungsforschung bekannt sind, etwa das Elaboration-Likelihood-Modell (ELM) oder das heuristisch-systematische Modell (HSM) (Geuß 2018). Die Urteilsfähigkeit macht deutlich, inwieweit sich die Rezipientin oder der Rezipient gemäß dem ELM und HSM (siehe Kapitel 2.3.1 und 2.3.2) mit der Thematik auseinandergesetzt hat oder auseinandersetzen wird. Denn „auf der Grundlage von Regeln, die sie durch Beobachtung gewonnen haben, lernen Menschen unter anderem Urteilsfähigkeit, Sprachstile, Begriffssysteme, Strategien zur Informationsverarbeitung, kognitive Operationen und Verhaltensstandards“ (Bandura 1979, S. 50). Dabei reicht es für die Einzelnen jedoch nicht aus, lediglich betroffen zu sein.

> „Vielmehr ist es notwendig, die wissenschaftlichen Hintergründe und Zusammenhänge zu verstehen, um sie für sich verfügbar zu machen und mit anderen in einer zielführenden Diskussion vertiefen zu können. Nur so entsteht Urteilsfähigkeit, und Urteilsfähigkeit ist die Voraussetzung für verantwortungsvolles Handeln“ (Meyer 2009, S. 11).

Sauter, Sauter und Wolfig (2018) ergänzen hierzu, dass das Beurteilungsvermögen durch Erfahrungen und über laufende Reflexionen der eigenen Urteilsfähigkeit bestimmt

wird und untermauern damit die Theorie der Selbstwirksamkeit von Bandura (siehe Kapitel 2.3.4). Vor diesem Hintergrund wird für die hier unternommene Untersuchung vermutet, dass die Inszenierung aktiver Auseinandersetzungsprozesse, wie sie in der EG angeregt werden, förderlicher auf die Urteilsfähigkeit wirkt als die reinen Präsentationen in der KG. Die inhaltliche Hypothese lautet:

H4ab: Die Lernenden der EG profitieren stärker in ihrer Urteilsfähigkeit als Lernende der KG.

Die aus H4ab abgeleiteten statistischen Hypothesen lauten:

Hypothese 4a: im Prä-Post-Vergleich

H0: $\mu^{U}2EG = \mu^{U}2KG$

H1: $\mu^{U}2EG > \mu^{U}2KG$

Hypothese 4b: im Prä-Post-Follow-up-Vergleich

H0: $\mu^{U}3EG = \mu^{U}3KG$

H1: $\mu^{U}3EG > \mu^{U}3KG$

U= Urteilsfähigkeit im Kontext von IT-Sicherheit

4.2.3 Hypothese 5: Kontrollüberzeugung

Die Theorie des geplanten Verhaltens (siehe Kapitel 2.3.8) postuliert als dritte Determinante der Verhaltensintention die wahrgenommene Verhaltenskontrolle, die sich aus der Kontrollüberzeugung und der Selbstwirksamkeit zusammensetzt. Die Kontrollüberzeugung adressiert die Ansicht, Ziele selbst verwirklichen und erreichen zu können, und betrifft damit die subjektive Gestaltungsfähigkeit von Lebensereignissen (Kreß 2016). Forschungsergebnisse von Ifinedo (2012) zeigen auf, dass bei nichtkonformem Verhalten im Kontext von Informationssicherheit präventive Maßnahmen genau dann besonders wirksam sind, wenn eine geringe Selbstkontrolle vorhanden ist. Damit spricht Ifinedo die von Kaschek und Schumacher (2015) vorgetragene positive Erfahrung an, die die Kontrollüberzeugung nicht nur entstehen sondern auch anwachsen lässt und die Resilienz erhöht (Rothgangel 2010). Einfache Präsentationen von Cyberangriffen wie diejenigen in der KG lassen somit vermutlich die Kontrollüberzeugung abnehmen, während die Kontrollüberzeugung durch die Methoden der Selbstreflexion in der EG erhöht werden kann. Die inhaltliche Hypothese lautet:

H5ab: Die Kontrollüberzeugung der Lernenden der EG nimmt stärker zu als die Kontrollüberzeugung der Lernenden der KG.

Die aus H5ab abgeleiteten statistischen Hypothesen lauten:

Hypothese 5a: im Prä-Post-Vergleich

H0: $\mu^{wV}2EG = \mu^{wV}2KG$

H1: $\mu^{wV}2EG > \mu^{wV}2KG$

Hypothese 5b: im Prä-Post-Follow-up-Vergleich

H0: $^{\mu wV}3EG = {}^{\mu wV}3KG$

H1: $^{\mu wV}3EG > {}^{\mu wV}3KG$

wV = Kontrollüberzeugung im Kontext von IT-Sicherheit

4.2.4 Hypothese 6: Selbstwirksamkeit im Kontext von IT-Sicherheit

Eine weitere Determinante zur wahrgenommene Kontrollmöglichkeit ist die Selbstwirksamkeit (Moser 2017). Bandura (1997) verweist in seiner Theorie (siehe Kapitel 2.3.4) auf die Einflussgrößen der Selbstwirksamkeit und beschreibt in diesem Kontext die durch die Dozentin bzw. den Dozenten vorgetragenen Erfahrungen als zweitstärkstes Mittel, um die Selbstwirksamkeit zu erhöhen. Wirkungsvoller seien nur eigene Erfahrungen. Koldner (2014) verweist in diesem Zusammenhang darauf, dass Personen, die in der Lage sind, IT-Sicherheitsrisiken zu erkennen, geeignete Maßnahmen zum Schutz sensibler Daten ergreifen und fundierte Entscheidungen über den sicheren Umgang mit Informationen und Technologien treffen können. Dabei wirken sich ihre Erfahrungen auf die Selbstwirksamkeit aus und lassen damit eine Verbesserung der Selbstwirksamkeit im Kontext von IT-Sicherheit möglich werden. Diese Fähigkeiten sollen nach Steffen (2019) durch didaktische Maßnahmen erkannt, entdeckt und weiter verbessert werden. Nerdinger, Blickle und Schaper (2011) weisen darüber hinaus darauf hin, dass das Üben von Verhaltensweisen eine wichtige Transfertechnik ist, da es Sicherheit vermittelt, die eine realitätsnahe Bewertung von eigenen Handlungsspielräumen transparent werden lässt. Es wird somit vermutet, dass sich durch die Implementierung von Aufgabenstellungen, wie sie in der EG erfolgt, die Selbstwirksamkeit im Kontext von IT-Sicherheit stärker entwickelt als in der KG, in der keine Aufgabenstellung angeboten wird, um ein Reflektieren des prozeduralen Wissens möglich werden zu lassen. Die inhaltliche Hypothese lautet:

H6ab: Die Lernenden der EG, die die präventive Maßnahme absolvieren, verändern sowohl kurzfristig als auch langfristig stärker ihre Selbstwirksamkeit im Kontext von IT-Sicherheit in Bezug auf sicherheitskonformes Verhalten als die Lernenden der KG.

Die aus H6ab abgeleiteten statistischen Hypothesen lauten:

Hypothese 6a: im Prä-Post-Vergleich

H0: $^{\mu SwIT}2EG = {}^{\mu SwIT}2KG$

H1: $^{\mu SwIT}2EG > {}^{\mu SwIT}2KG$

Hypothese 6b: im Prä-Post-Follow-up-Vergleich

H0: $^{\mu SwIT}3EG = {}^{\mu SwIT}3KG$

H1: $^{\mu SwIT}3EG > {}^{\mu SwIT}3KG$

SwIT = Selbstwirksamkeit im Kontext von IT-Sicherheit

4.3 Dritter Hypothesenkomplex: Moderatoren

Der dritte Hypothesenkomplex untersucht, welche soziodemografischen Faktoren die Wirksamkeit der Präventionsmaßnahme beeinflussen. Als Aspekte der Wirksamkeit werden die Einstellung, die Selbstwirksamkeit und die Kontrollüberzeugung im Kontext von IT-Sicherheit der ProbandInnen betrachtet. Als mögliche Moderatoren werden die Zugehörigkeit zur Technikgeneration (siehe Tabelle 13), der Bildungsstand und das Geschlecht der Teilnehmenden untersucht, da gezeigt wurde, dass InterakteurInnen in der digitalen Welt abhängig von diesen Merkmalen Medien unterschiedlich nutzen und diesbezüglich differente Weiterbildungsangebote wahrnehmen (siehe Kapitel 2.5.1).

4.3.1 Hypothese 7: Generationenzugehörigkeit

Das Alter beeinflusst den Umgang mit Technologien, wobei es eine zentrale Rolle spielt, mit welchen Technologien die/der Lernende aufgewachsen ist. Denn gemäß dem Mere-Exposure-Effekt (Zajonc & Moreland 1982) werden bekannte Technologien positiver bewertet als unbekannte Technologien. Differenzierte Interaktionssequenzen mit Technologien führen zwar zu entsprechenden differenzierten Bewertungen (Vogel 2016), jedoch sind auch diese von den (Vor-)Erfahrungen abhängig (siehe auch Kapitel 2.5.1). Gemäß der Tabelle 13 lassen sich folgende Gruppen ableiten:

Tab. 21: Technikgenerationen im Kontext der präventiven Maßnahme

Nr.	Trainingsdatum	Geburtsdatum	Alter	Technikgeneration
1	2018	1980	18-38	Internetgeneration
2	2018	1964	39-54	Computergeneration
3	2018	1949	55-69	Generation der zunehmenden Haushaltstechnik

Es wird somit vermutet, dass die Wirksamkeit der in der vorliegenden Studie untersuchten Präventionsmaßnahme von der Zugehörigkeit zu einer Technologiegeneration (Alter) abhängig ist. Die inhaltliche Hypothese lautet:

H7: Das Alter schwächt die Wirksamkeit der Maßnahme (Prä-Post- Follow-up) in der Gesamtstichprobe (KG, EG).

Die aus H7 abgeleiteten statistischen Hypothesen lauten:

Hypothese 7: H0: $b_{A,G} = 0$

H1: $b_{A,G} \neq 0$

b_{A} = Regressionskoeffizient Alter

b_{G} = Regressionskoeffizient Wirkungskoeffizient

4.3.2 Hypothese 8: Bildungsstand

Diverse Statistiken weisen seit Jahren das Bildungsniveau als wirksamsten Prädiktor für den Erfolg einer Weiterbildung aus (Reich-Claassen 2010). Lernende mit einer höheren Ausbildung profitieren stärker von Bildungsmaßnahmen (Lumsden & Sherron 1978) als Lernende mit einer geringeren Ausbildung, was den mehrfach untersuchten und bestätigten sogenannten Matthäus-Effekt[36] (Merton 1968) untermauert, den Wilkens und Leber (2003) auf der Datengrundlage des sozioökonomischen Panels auch für die (berufliche) Weiterbildung bestätigen. Es wird somit vermutet, dass der Bildungsstand der Teilnehmenden die Wirksamkeit der präventiven Maßnahme beeinflusst. Die inhaltliche Hypothese lautet:

H8: Der Bildungsstand der Lernenden moderiert die positive Wirksamkeit der Maßnahme (Prä-Post) in der EG und der KG.

Die aus H8 abgeleiteten statistischen Hypothesen lauten:

Hypothese 8: H0: $a_{BL} = 0$

H1: $a_{BL} \neq 0$

a_{BL} = Regressionskoeffizient Bildung

4.3.3 Hypothese 9: Geschlecht

Untersuchungen zur Nutzung des Internets zeigen, dass diese nach Geschlecht unterschiedlich ist. Zwar schwinden diese Unterschiede in der Nutzung digitaler Medien zusehends, sind jedoch weiter vorhanden (siehe Kapitel 2.5.1). Studien von Mennicken, Sack und Ziefle (2011) zeigen, dass signifikante Korrelationen zwischen dem Grad der technikbezogenen Selbstwirksamkeit und dem Geschlecht vorhanden sind und dass diese Selbstwirksamkeit tendenziell bei Frauen geringer ausgeprägt ist als bei Männern. Erklärungen hierfür sieht Hammel (2005) in den geringeren Ausprägungen technikbezogener Selbstwirksamkeit bei Mädchen bereits am Ende der Grundschulzeit, die weiter bestehen bleiben. Es wird daher vermutet, dass auch das Geschlecht einen Einfluss auf die Wirksamkeit der präventiven Maßnahme besitzt. Die inhaltliche Hypothese lautet:

H9: Das Geschlecht der Lernenden moderiert die Wirksamkeit der präventiven Maßnahme (Prä-Post) in der EG und der KG.

Die aus H9 abgeleiteten statistischen Hypothesen lauten:

Hypothese 9: H0: $a_{GS} = 0$

H1: $a_{GS} \neq 0$

a_{GS} = Regressionskoeffizient Geschlecht

[36] Dieser Effekt beschreibt die „Zunahme der Weiterbildung mit Bildungsgrad und beruflicher Position“ (Hooß 2014, S. 5).

4.3.4 Hypothese 10: VersuchsleiterInnenartefakt

Die ungewollte Beeinflussung von Forschungsergebnissen durch die Versuchsleitung wird mit dem sogenannten Rosenthal-Effekt beschrieben und erklärt. Rosenthal (1976) macht jedoch zugleich deutlich, dass derartige Beeinflussungen kaum verhindert werden können. Der VersuchsleiterInneneffekt ist damit stets eine zu reflektierende Komponente, um die Objektivität der Effekte einer Lehrveranstaltung abzusichern. Diese Absicherung ist somit Bestandteil der Gütekriterien für Lehrveranstaltungen sowie für darauf bezogene Forschungen (Bortz & Doering 2009). In der Studie gab es zwei verschiedene Lehrende (den Autor dieser Arbeit und eine weitere Dozentin), die die präventive Maßnahme sowohl in der KG als auch in der EG durchführten. Um einen VersuchsleiterInneneffekt auszuschließen, wird untersucht, ob die Wirksamkeit der Maßnahme bei den beiden Lehrenden unterschiedlich ausfällt. Vermutet wird, dass es keinen Unterschied gibt, sodass die inhaltliche Hypothese wie folgt lautet:

H10: Die Lehrperson moderiert die Wirksamkeit der präventiven Maßnahme (Prä-Post) nicht.

Die aus H10 abgeleiteten statistischen Hypothesen lauten:

Hypothese 10: im Prä-Post-Vergleich

H0: $a_{VA} \neq 0$

H1: $a_{VA} = 0$

a_{VA} = Regressionskoeffizient VersuchsleiterInnenartefakt

5 Methodik und Evaluation

5.1 Forschungsdesign

Das Forschungsdesign besteht aus einem Prätest, einem Posttest und einem Follow-up-Test. Die durchgeführte Studie fand unter Alltagsbedingungen von präventiven Maßnahmen im Konstrukt freiwilliger Weiterbildung statt. Die EG absolvierte die konzipierte Maßnahme zur Prävention von Cybercrime, die KG erhielt lediglich eine Demonstration von möglichen Cyberangriffen. Die KG sowie die EG durchliefen die gleichen diagnostischen Verfahren, die an drei Messzeitpunkten innerhalb eines Monats angewandt wurden. Der erste Messzeitpunkt (t1) lag vor Beginn der präventiven Maßnahme, der zweite Messzeitpunkt (t2) unmittelbar nach der Durchführung der präventiven Maßnahme (gleicher Tag). Ein dritter Messpunkt (t3), welcher ca. 30 Tagen danach stattfand, versuchte die Stabilität der Wirkung der präventiven Maßnahme nachzuweisen (siehe Abbildung 40).

Das präventive Projekt „Der zweite Blick“ war ein ehrenamtliches Projekt, das jeder Bürgerin und jedem Bürger zur kostenlosen Teilnahme offenstand. Die TeilnehmerInnen dieser Maßnahme aus den unterschiedlichsten Bevölkerungsschichten wurden auf freiwilliger Basis für die vorliegende Studie rekrutiert und verdeckt in EG und KG eingeteilt. Die Gruppeneinteilung erfolgte nach dem Zufallsprinzip (Randomisierung).

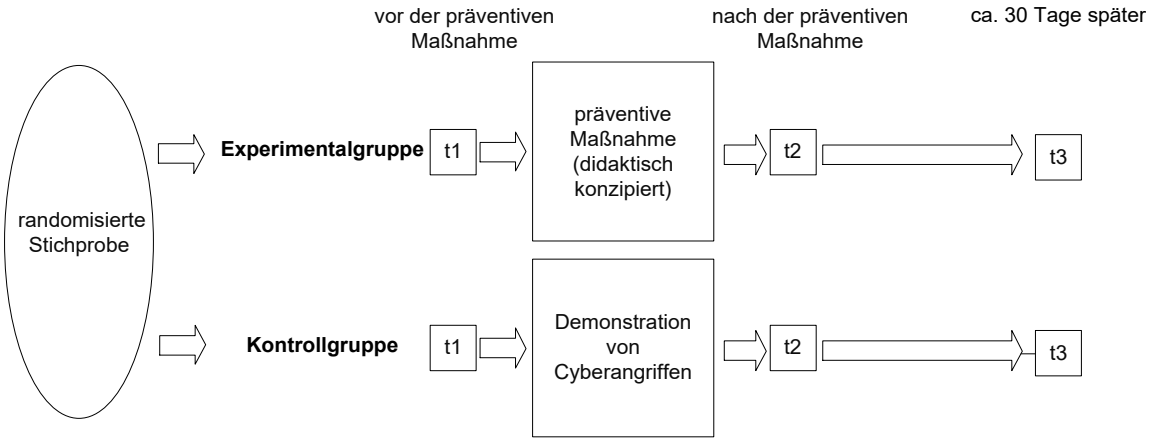


Abb. 40: Ablauf der Studie

Für die Untersuchung wurden unterschiedliche Variablen, deren Relevanz sich aus den vorher behandelten Theorien ergab, ausgewählt (siehe Tabelle 22).

Tab. 22: Abhängige Variablen der Untersuchung

Skala *Subskala*
soziodemografische Daten *Geschlecht* *Bildungsstand* *Alter*
Skala *Subskala*
Beweggründe für die Teilnahme *themenbezogene* *nicht themenbezogene*
Selbstwirksamkeitserwartung
Evaluation *Veranstaltungsorganisation* *Medien und Materialien* *Lehrperson* *allgemeine Bewertung*
geplantes Verhalten im Kontext von IT-Sicherheit *Einstellung* *Kontrollüberzeugung* *Urteilsfähigkeit* *Selbstwirksamkeit*
Weiterbildungsmotivation

Um diese Variablen operationalisieren zu können, bedurfte es Messinstrumente, die nachfolgend beschrieben werden.

5.2 Messinstrumente

Aus den oben beschriebenen abhängigen Variablen (siehe Kapitel 2.3) und den formulierten Hypothesen (siehe Kapitel 4) leiten sich die erforderlichen und auch verwendeten Messinstrumente ab. Für die zu untersuchenden Themenbereiche wurden aussagekräftige und standardisierte Diagnostikverfahren in Form von Fragebögen (F1-F3) ausgewählt, entwickelt und eingesetzt (t1-t3). Eine Übersicht bietet die Tabelle 23 mit einer Kurzbeschreibung.

Tab. 23: Messinstrumente zur Untersuchung der Wirksamkeit der Maßnahme

Skala *Subskala*	Messinstrumente	Anzahl Items	Reliabilität	Administration zum Messzeitpunkt mit Erhebungsinstrument		
	Fragebögen			F1 (t1)	F2 (t2)	F3 (t3)
soziodemografische Daten	Eigenentwicklung		--			
Geschlecht		1		x		
Bildungsstand		1		x		
Alter		1		x		
Beweggründe für die Teilnahme	Eigenentwicklung	6		x		
Selbstwirksamkeitserwartung	Jerusalem & Schwarzer (2019)	10	.88	x		
Evaluation	allgemeine Fragen der Evaluation		.			
Veranstaltungsorganisation		3			x	
Medien und Materialien		3			x	
Lehrperson		5			x	
allgemeine Bewertung		7			x	
geplantes Verhalten im Kontext von IT-Sicherheit	Hiemisch (2017)	26		x	x	x
Weiterbildungsmotivation	Gorges (2018)	14			x	x

Dabei bildet der Fragebogen F1 zum Messzeitpunkt t1 den Prä-Test, der Fragebogen F2 zum Messzeitpunkt t2 den Post-Test und der Fragebogen F3 zum Messzeitpunkt t3 den Follow-Up-Test ab.

5.2.1 Soziodemografische Daten (FK1)

Der Fragenkomplex zu den soziodemografischen Daten umfasst das Alter, die Bildung und das Geschlecht und befindet sich im Erhebungsinstrument zu t1 (siehe Anhang 6).

5.2.2 Fragenkomplex zur Weiterbildungsmotivation (FK2)

Der Fragenkomplex zur Weiterbildungsmotivation fokussiert die Weiterbildungsmotivation aus der Perspektive der Erwartung und der Bilanzierung (Gorges 2018). Das Antwortformat ist für beide Subskalen eine fünfstufige Likert-Skala mit den Polen „trifft gar nicht zu“ bis „trifft vollständig zu“ (siehe Tabelle 24).

Tab. 24: Skalen zur Weiterbildungsmotivation

Skala *Subskala*	Quelle	Anzahl Items	Messzeitpunkte			Antwortformat fünfstufige Likert-Skala
			t1	t2	t3	
Weiterbildungsmotivation Erfolgserwartung *Bilanzwert*	Gorges (2018)	 7 7	 x x		 x x	 x x

Die entsprechenden Items sind im Anhang 2 ersichtlich und Bestandteil des Fragebogens zu t1 (siehe Anhang 6).

5.2.3 Fragenkomplex zu den Beweggründen für die Teilnahme (FK3)

Das Besuchen präventiver Maßnahmen kann aus unterschiedlichen Beweggründen erfolgen. Der Wunsch nach sozialer Integration und Kommunikation begünstigt genauso wie das Streben nach beruflicher Weiterbildung die Teilnahme an freiwilligen Weiterbildungsangeboten. In Bezug auf die Beweggründe zur Teilnahme an der Präventionsmaßnahme „Der zweite Blick“ lassen sich themenbezogene und nicht themenbezogene Beweggründe unterscheiden. Beide Arten von Beweggründen wurden mit jeweils zwei Skalen erfasst und durch H2 überprüft.

Ein Beispielitem für themenbezogene Beweggründe lautet: „Weil es mir Spaß macht, mich für neue Dinge zu interessieren.“ Das Antwortformat ist für beide Subskalen eine fünfstufige Likert-Skala mit den Polen „trifft gar nicht zu“ bis „trifft vollständig zu“. Die beiden Skalen zu den Beweggründen sind Bestandteil des zum ersten Messzeitpunkt administrierten Fragebogens (siehe Anhänge 3 und 6).

5.2.4 Selbstwirksamkeitserwartung (FK4)

Die Skala zur allgemeinen Selbstwirksamkeitserwartung von Schwarzer und Jerusalem (1999) gilt bereits seit 20 Jahren als validiertes Erhebungsinstrument und wurde vollständig übernommen (siehe Anhang 4). Der Anwendungsbereich umfasst Erwachsene und Jugendliche und dient der Persönlichkeitsdiagnostik auf Gruppenebene, die in dieser Studie die vorhandene Homogenität der Selbstwirksamkeit der Teilnehmenden aufzeigen soll. Die Skala umfasst zehn Items und wurde anhand einer fünfstufigen Likert-Skala von „stimmt nicht“ bis „stimmt genau“ beantwortet. Ein Beispielitem lautet: „Wenn sich Widerstände auftun, finde ich Mittel und Wege, mich durchzusetzen“ (Schwarzer & Jerusalem 1999, S. 1). In der vorliegenden Studie wurde die Selbstwirksamkeitserwartung im Fragebogen zu t1 erhoben und sollte die allgemeine Selbstwirksamkeit operationalisieren.

5.2.5 Evaluation (FK5)

Die Skala ‚Evaluation' wurde aus allgemeinen Fragen zur Evaluation von Bildungsmaßnahmen von Erwachsenen gebildet (vgl. Anhang 5). Der Fragenkomplex versucht zum einen die Qualität der Veranstaltung und zum anderen die Qualität der/des Lehrenden zu bewerten. Die Fragen beziehen sich auf die Bewertung der Veranstaltungsorganisation (3 Items), der verwendeten Medien und Materialien (3 Items), der Lehrperson (5 Items) und auf die Präventionsmaßnahme allgemein (7 Items). Ein Beispielitem für die Bewertung der Lehrperson lautet: „Die Referentinnen und Referenten bezogen theoretische Ansätze auf die Praxis der Teilnehmenden."

5.2.6 Geplantes Verhalten (FK6)

Der Fragenkomplex zum geplanten Verhalten im Kontext von IT-Sicherheit wurde für diese präventive Maßnahme von der Universität Greifswald entwickelt (Hiemisch 2017), war Bestandteil der Erhebungsinstrumente zu allen drei Messzeitpunkten und ist im Anhang 1 einsehbar. Gemessen wurden die Einstellung zu sicherheitskonformem Verhalten, die Kontrollüberzeugung, die Urteilsfähigkeit und die Selbstwirksamkeit im Kontext von IT-Sicherheit der Teilnehmenden. Die Determinanten des geplanten Verhaltens wurden mit vier Skalen erfasst, mit jeweils neun Items für die Einstellung, fünf Items für die Kontrollüberzeugung, drei Items für die Urteilsfähigkeit und zwölf Items für die Selbstwirksamkeit im Kontext von IT-Sicherheit. Ein Beispielitem für die Einstellung lautet: „Ich finde es wichtig, darüber Bescheid zu wissen, wie man im Internet betrogen werden kann." Das Antwortformat ist für alle Subskalen, auch hier, eine fünfstufige Likert-Skala mit den Polen „trifft gar nicht zu" bis „trifft vollständig zu". Die beschriebenen Skalen zum geplanten Verhalten sind Bestandteil des zum ersten, zweiten und dritten Messzeitpunkt administrierten Fragebogens (siehe die Anhänge 6, 7 und 8). Dieser Fragenkomplex war empirisch noch nicht abgesichert und bedurfte einer später durchzuführenden explorativen Faktorenanalyse.

5.3 Untersuchungsdurchführung

Dieser Abschnitt zur Untersuchungsdurchführung beschreibt überblicksartig den Ablauf der Studie und geht dazu auf den Zeitplan und auf die Umsetzung der Maßnahme ein.

5.3.1 Zeitplan

Die Planungen der präventiven Maßnahme begannen im Jahr 2016 und wurden innerhalb eines Jahres sukzessiv weiter verbessert. Die demonstrierbaren Cyberangriffe wur-

den hierzu zielgruppenbezogen ausgewählt, didaktisch reduziert und auf ihre Anwendbarkeit geprüft. Anfang 2018 begann die Hauptstudie, in der die finale präventive Maßnahme erstmalig bekannt gegeben und beworben wurde (entsprechende Bekanntmachungen und Resonanzen sind in den Anhängen 9 und10 dargestellt).

5.3.2 Umsetzung der Maßnahme

Die Präventionsmaßnahme wurde am 21.02.2018 begonnen und am 20.12.2018 beendet. Die Maßnahme umfasste diverse Lerneinheiten, die später detailliert in dieser Arbeit behandelt werden. Der Veranstaltungsort und die Räumlichkeiten variierten und wurden von den VeranstalterInnen ausgewählt, festgelegt und kostenlos zur Verfügung gestellt. Die technischen Voraussetzungen wurden von der bzw. dem Lehrenden vorab geprüft und, wenn nötig, durch geeignete Maßnahmen kompensiert.

5.4 Statistische Analysen

Um die Daten elektronisch auswerten und statistische Analysen durchführen zu können, wurden die ausgefüllten Fragebögen in ein digitales Format umgewandelt und abgespeichert. Zum Einsatz kamen das Statistikprogramm SPSS der Firma IBM in der Version 22 sowie die Microsoft-Software für Tabellenkalkulation Excel in der Version 2016. Um statistische Aussagen treffen zu können, werden nachfolgend die erforderlichen statistischen Verfahren vorgestellt und deren Kriterien behandelt.

5.4.1 Explorative Faktorenanalyse (EFA)

Das allgemeine Ziel einer explorativen Faktorenanalyse (EFA) besteht darin, Variablen, die miteinander korrelieren, auf einer höheren Abstraktionsebene zu aussagekräftigen Faktoren zusammenzufassen (Bortz & Doering 2009). Zur Extraktion der Faktoren gibt es unterschiedliche Methoden. Eines der am häufigsten eingesetzten Verfahren ist die Hauptkomponentenanalyse (Principal Component Analysis PCA), mit der das Ziel verfolgt wird, einen möglichst großen Anteil der Gesamtvarianz in den Variablen durch möglichst wenige Faktoren, die sogenannten Komponenten, zu erklären (Moosbrugger & Kelava 2012). Die zentrale Fragestellung der Hauptkomponentenanalyse lässt sich wie folgt formulieren*: „Wie lassen sich die auf einen Faktor hoch ladenden Variablen durch einen Sammelbegriff zusammenfassen?“* (Backhaus et al. 2016, S. 413). Das zweite sehr häufig angewendete Verfahren ist die Hauptachsenanalyse (Principal Axis Factoring, PAF), die lediglich die gemeinsame Varianz der Variablen erklären soll (ebd., S. 412). Dabei werden die Zusammenhänge zwischen den Variablen auf latente Variablen, die extrahierten Faktoren, zurückgeführt. Die Hauptachsenanalyse sucht nach einer

Antwort auf die zentrale Frage: *„Wie lässt sich die Ursache bezeichnen, die für die hohen Korrelationen zwischen den Variablen verantwortlich ist?“* (ebd., S. 413).

Die Durchführung einer EFA ist an Voraussetzungen gebunden, die es vorab zu behandeln gilt. Grundsätzlich ist es notwendig, dass das Faktorenmodell theoretisch begründet werden kann und zu der zugrundeliegenden Fragestellung passt. Eine weitere Voraussetzung ist eine ausreichende Stichprobengröße. Die erforderliche Stichprobengröße ist abhängig von den Kommunalitäten der untersuchten Items, die wie folgt definiert sind: „Die Kommunalitäten beschreiben die Varianzanteile der einzelnen Variablen, die durch die extrahierten Faktoren erklärt werden können (Summe der quadrierten Ladungen einer Variablen über sämtlichen Faktoren)“ (Schwarz & Kohler 2019, S. 1). MacCallum et al. (1999) geben hierzu eine erforderliche Stichprobengröße von n = 60 an, wenn hohe Kommunalitäten der Items von mindestens $h^2 = .60$ erreicht werden. Für Bühner (2011) hingegen ist bei Kommunalitäten von $h^2 = .50$ eine Stichprobengröße von $n \geq 100$ akzeptabel. Mundfrom, Shaw und Lu Ke (2009) empfehlen vier Items pro Faktor (n = 500). Raithel (2008) wiederum setzt die Mindestanzahl auf drei Items pro Faktor, eine Sichtweise, die auch Bühner (2006) teilt.

Eine weiterhin zu beachtende Voraussetzung ist die Eignung der Daten für eine EFA. So müssen die in die Faktorenanalyse einfließenden Variablen ein metrisches Skalenniveau aufweisen, wobei auch Likert-Items zulässig sind, die mindestens fünfstufig sind (Lloret-Segura et al. 2014).

Des Weiteren wird die Interkorrelation der Items überprüft. Das Kaiser-Meyer-Olkin-Kriterium (KMO) ist dabei ein Maß für die Eignung der Korrelationsmatrix insgesamt. Das KMO-Kriterium nimmt Werte zwischen 0 und 1 an. Dabei werden die KMO-Werte wie in der Tabelle 25 abgebildet interpretiert.

Tab. 25: KMO-Koeffizient und Eignung der Daten (Bühner 2011, S. 347)

KMO-Koeffizient	Eignung der Daten für EFA
>0.9	sehr gut
0.80-0.89	gut
0.70-0.79	mittel
0.60-0.69	mäßig
0.50-0.59	schlecht
< 0.5	inkompatibel

Ein weiterer Indikator für die Dateneignung ist der MSA-Wert (Measure of Sampling Adequacy), der aufzeigt, welche Items in die Faktorenanalyse einfließen sollten. Kaiser und Rice schlagen hierzu Grenzwerte vor (siehe Tabelle 26).

Tab. 26: Grenzwerte nach Kaiser und Rice (1974, S. 112)

MSA	Eignung
0.90s	marvelous
0.80s	meritorious
0.70s	middling
0.60s	mediocre
0.50s	miserable
below 0.50	unacceptable

Zur Datenberechnung wird darüber hinaus der Bartlett-Test zur Dateneignung berechnet. Dieser überprüft, ob die Stichprobe einer Grundgesamtheit entstammt, in der die Variablen unkorreliert sind (Dziuban & Shirkey 1974). Ist das Ergebnis signifikant ($p < .05$), kann davon ausgegangen werden, dass sich die Daten für die Durchführung einer Faktorenanalyse eignen (Schwarz & Kohler 2019). Der entsprechende Wert von .05 wird damit in dieser Untersuchung als Alpha-Niveau festgelegt. Um einen Bartlett-Test durchführen zu können, müssen die Variablen in der Erhebungsgesamtheit allerdings einer Normalverteilung folgen (Backhaus et al. 2016).

Sind die Voraussetzungen für die Durchführung einer EFA erfüllt und ist die Extraktionsmethode festgelegt, wird im nächsten Schritt der EFA die Anzahl der Faktoren bestimmt. Hierbei spielen theoretische Überlegungen eine zentrale Rolle und es lassen sich unterschiedliche Extraktionskriterien und -verfahren heranziehen. Ein bekanntes Verfahren (Beer 2016) stellt das Kaiser-Guttman-Kriterium (Cattell 1966) dar, demzufolge alle Faktoren mit Eigenwerten größer als 1,0 als bedeutsam erachtet und extrahiert werden. Wobei der Eigenwert eines Faktors angibt, welcher Anteil der auf die Anzahl der Variablen normierten Gesamtvarianz durch diesen einen Faktor erklärt wird (Moosbrugger & Kelava 2012).

Ein weiteres, sehr verbreitetes Verfahren ist das Scree-Plot-Kriterium (Cattell 1966). Im Scree-Plot werden die Eigenwerte der Faktoren in einem Koordinatensystem auf der Y-Achse nach abnehmender Wertefolge angeordnet, während auf der X-Achse die Anzahl der Faktoren angegeben wird. An der Stelle, an der die Differenz der Eigenwerte zwischen zwei Faktoren am größten ist, entsteht ein Knick (Backhaus et al. 2016). Alle Faktoren hinter dem Knick, einschließlich des Faktors, der den Knick markiert, werden ignoriert. Denn extrahiert werden nur diejenigen Faktoren, die vor dem Knick sichtbar werden und deren Eigenwert > 1,0 ist (Moosbrugger & Kelava 2012).

Ein weiteres Verfahren zur Bestimmung der zu extrahierenden Faktoren ist die Parallelanalyse.

> „Die Idee der Parallelanalyse besteht darin, dass bei der Faktorenanalyse des empirischen Datensatzes so viele Faktoren beibehalten werden, wie es Eigenwerte gibt, die größer als die Eigenwerte des Zufallsdatensatzes sind. Anders ausgedrückt heißt dies, dass die Faktoren, die beibehalten werden sollen, wenigstens

> so viel Varianz aufklären sollen, wie sich bei der Analyse von Zufallsdaten ergibt“ (O’Connor 2000b, S. 5).

O’Connor (2000a) stellt hierzu die entsprechende Syntax für SPSS, SAS und MATLAB bereit, die jeweils von den Anwendenden nur noch für die individuellen Fragestellungen anzupassen ist. Um die extrahierten Faktoren besser interpretieren zu können, wird üblicherweise eine Rotation vorgenommen, wobei das gewählte Rotationsverfahren davon abhängt, ob man – theoretisch begründet – von korrelierten oder unkorrelierten Faktoren ausgeht. Bei unkorrelierten Faktoren wählt man ein orthogonales Verfahren, beispielsweise die Varimax-Rotation. Dabei wird der Rotationswinkel so errechnet, dass die Streuung der quadrierten Ladungen der Faktoren um ihre Mittelwerte maximiert wird, wodurch die Anzahl der Variablen mit einer hohen Ladung auf einem Faktor minimiert wird (Kosfeld o.J.). Das Verfahren der Varimax-Rotation strebt eine Einfachstruktur an, bei der eine möglichst geringe Anzahl von Variablen möglichst hoch auf den einzelnen Faktor lädt (Müller 2016). Wenn hingegen theoretische Anhaltspunkte (besonders in der Psychologie) vorliegen, die auf korrelierte Faktoren hinweisen (Moosbrugger & Kelava 2012, S. 332), wählt man eine oblique Rotation, beispielsweise das Oblimin- oder Promax-Verfahren. Die Oblimin-Rotation strebt die simultane Optimierung eines orthogonalen und eines obliquen Rotationskriteriums an (Bühner 2011). Bühner (2006) weist jedoch darauf hin, dass es sinnvoll sein kann, nacheinander sowohl oblique Verfahren (wie z.B. Promax) als auch orthogonale Verfahren (wie z.B. Varimax) zu berechnen und die Ergebnisse einander gegenüberzustellen. Denn zeigt sich bei beiden Verfahren die gleiche Zuordnung der Items zu den Faktoren, kann von einer stabilen Faktorenstruktur ausgegangen werden.

Im nächsten Schritt werden die rotierten Faktorladungen der einzelnen Items betrachtet. Dabei werden Items grundsätzlich demjenigen Faktor zugeordnet, auf den sie am höchsten laden. Als Kriterium für die Zuordnung zu einem Faktor gilt in der Forschung üblicherweise eine betragsmäßige Faktorladung > .30 als mindestens erforderlich; als hoch gilt eine Faktorladung ab einem Betragswert > .60 (Kline 1994, S. 6).

5.4.2 Zweifaktorielle Varianzanalyse mit Messwiederholung

Die Varianzanalyse (ANOVA) gilt als das wichtigste Verfahren zur Auswertung von Experimenten. Die univariate Varianzanalyse ist ein Verfahren, das es erlaubt, die Beziehung zwischen einer abhängigen metrischen Variable und einer oder mehreren unabhängigen nominalen Variablen mit einer oder mehr Ausprägungen zu untersuchen. So kann beispielsweise der Einfluss dreier unterschiedlicher Lehrmethoden auf den Lernerfolg analysiert werden (Kronthaler 2016).

Mithilfe der Varianzanalyse ist es auch möglich, zu untersuchen, wie sich die Ausprägung eines Merkmals zu verschiedenen Messzeitpunkten unterscheidet. Die unabhängige Variable ist hierbei die Zeit. Rasch et al. (2014) weisen auf die Vorteilhaftigkeit dieses Verfahren hin, da gegenüber mehreren Tests keine α-Fehler-Kumulierung auftritt, da nur ein Test erforderlich wird, sofern auf zusätzliche Post-Hoc-Vergleiche verzichtet wird.

In der vorliegenden Arbeit werden ANOVAs mit zwei unabhängigen Variablen – auch Faktoren genannt – berechnet, wobei ein Faktor ein Zwischensubjektfaktor ist und der andere ein Messwiederholungsfaktor. Die drei erhobenen Messzeitpunkte (t1, t2, t3) bilden den dreistufigen Messwiederholungsfaktor, und die Zugehörigkeit zu entweder der Experimental- oder der Kontrollgruppe stellt den zweistufigen Zwischensubjektfaktor dar. Demnach ist von einer zweifaktoriellen Varianzanalyse mit Messwiederholung auf einem Faktor zu sprechen. Interpretiert werden die Haupteffekte der beiden Faktoren sowie der Interaktionseffekt zwischen den Faktoren.

Auch das statistische Verfahren der Varianzanalyse hat Voraussetzungen, die erfüllt sein müssen, um es durchführen zu dürfen. Die Voraussetzungen der ANOVA mit Messwiederholung sind die Intervallskaliertheit der abhängigen Variablen, die Normalverteilung der abhängigen Variablen bzw. Residuen zu den einzelnen Messzeitpunkten und innerhalb der einzelnen Gruppen, die Sphärizität sowie die Varianzhomogenität zwischen den beiden Gruppen.

Für die Überprüfung der Normalverteilung bei größeren Fallzahlen ist der Chi²-Test (Viertl 1990) geeignet, für kleinere Fallzahlen hingegen der Kolmogorov-Smirnov-Test (Zöfel 2000). Abgesehen davon gilt die Varianzanalyse als recht robust gegen Abweichungen von der Normalverteilung (Zöfel 2000). Kuhlmei (2018) nennt als Bedingung der Robustheit der ANOVA bereits eine Stichprobengröße von $n \geq 30$ je Gruppe. Statistisch makellos ist bei fehlender Normalverteilung die Wahl von entsprechenden nonparametrischen Verfahren anstelle der parametrischen ANOVA bei gleichzeitiger Reduktion der Teststärke.

Die Voraussetzung der Sphärizität ist ab drei Messzeitpunkten relevant (Smigierski 2019), wobei eine Sphärizität besagt, dass die Varianzen der Differenzen zwischen jeweils zwei Messzeitpunkten homogen sind (Rasch et al. 2010). Als Testverfahren dient der Mauchly-Test auf Sphärizität, der jedoch empfindlich auf Verletzungen der Normalverteilung reagiert und bei kleineren Stichproben teilweise nicht signifikant wird, obwohl eine Verletzung der Sphärizität vorliegt, während er bei großen Stichproben eine Verletzung der Sphärizität anzeigt, die in Wirklichkeit nicht vorliegt (ebd. 2014). Sollte die Voraussetzung der Sphärizität verletzt sein, wird ein Korrekturfaktor ε auf die Freiheitsgrade der F-Tests angewendet. Als gängige Verfahren gelten die konservativere

Greenhouse-Geisser- und die progressivere Huynh-Feldt-Korrektur. Eine weitere Voraussetzung ist die Varianzhomogenität zwischen den beiden Gruppen, die anhand des Levene-Tests auf Gleichheit der Fehlervarianzen überprüft werden kann, wenn n ≥ 5 pro Gruppe (Kuhlmei 2018). Der Levene-Test testet die Nullhypothese, die besagt, dass die Varianzen der Gruppen sich nicht unterscheiden (Kronthaler 2016). Demnach kann von einer Varianzhomogenität ausgegangen werden, wenn der Levene-Test nicht signifikant wird (Stoetzer 2017), denn: „If Levene's test is significant at $p \leq .05$, then the variances are significantly different, and homogeneity of variances cannot be assumed" (Salkind 2007).

Sollte der Levene-Test eine starke Verletzung der Varianzhomogenität aufzeigen und sollten die verglichenen Gruppen sehr ungleich bzgl. ihrer Größe sein, führt dies zu einer Verzerrung des F-Tests der ANOVA. In diesem Fall muss auf alternative Testverfahren zurückgegriffen werden, die die Berechnung der F-Statistik und der zugehörigen Freiheitsgrade für Varianzheterogenität adjustieren, beispielsweise auf den Brown-Forsythe-Test oder den Welch-Test.

Ein Maß für die Effektstärke einer ANOVA ist Eta² (η^2), das den Anteil der aufgeklärten Varianz der Messwerte auf der Ebene der Stichprobe angibt (Rasch et al. 2014). Für eine zweifaktorielle ANOVA wird die korrigierte Effektstärke η_p^2 genannt und angegeben. Sie relativiert die Quadratsumme des Effektes an der Fehlervarianz und ist somit für Vergleiche geeignet (Hemmerich, 2019). Eine für die Einschätzung der Effektstärke hilfreiche Übersicht ist bei Hartig, Jude und Wagner (2008) zu finden, die sich selbst an Cohen (1988) anlehnen. Demnach gilt ein $.01 \leq \eta^2 \leq .06$ als geringer Effekt, $.06 \leq \eta^2 \leq .14$ gilt als mittelstarker Effekt und $\eta^2 \geq .14$ als großer Effekt, der auch bei Ellis (2010) so beschrieben wird. Dies sind jedoch gerundete Werte, da die Originalgrenzen auf Basis eines f-Wertes festgelegt wurden (ebd. 1988).

Die Effektstärke ist ein statistisches Maß, das dimensionslos und somit unabhängig von der Maßeinheit der ursprünglichen Daten und v.a. der Stichprobengröße ist (Cohen 1988). Auch vom angesetzten Signifikanzniveau ist die Effektstärke unabhängig (Vierbuchen 2015). Die Effektstärke besitzt eine praxisbezogene Bedeutung für die Beurteilung von Effekten (Bühner & Ziegler 2009), da diese anhand der Effektstärke in ihrer Höhe interpretiert und da verschiedene Effekte miteinander verglichen werden können. Für die Varianzanalyse bedeutet das, dass nicht nur gezeigt werden kann, ob ein signifikanter Unterschied zwischen den untersuchten Gruppen vorliegt, sondern auch, wie groß der Unterschied ist (Rasch et al. 2010).

5.4.3 Regressionsanalyse

Neben der Varianzanalyse kommt in der vorliegenden Studie auch die lineare Regressionsanalyse zum Einsatz, ein Instrument, welches in der Forschung sehr häufig zur Beantwortung von prognosebezogenen Forschungsfragen Anwendung findet (Kronthaler 2016). Die Regressionsanalyse untersucht, ob eine oder mehrere unabhängige Variable(n) einen statistisch signifikanten Einfluss auf eine oder mehrere abhängige Variable(n) hat/haben und wie stark dieser gegebenenfalls ist (Stoetzer 2017). Die Regression ist somit eine Vorhersageanalyse, die sich mathematisch die Partialkorrelation[37] von Variablen zunutze macht, um die Werte einer abhängigen Variable aus den Werten der unabhängigen Variable(n) vorherzusagen (Schäfer 2016). „Die vorhersagende Variable wird dabei als Prädiktor, die vorhergesagte Variable als Kriterium bezeichnet“ (ebd., S. 121).

Um eine Analyse von Moderatoreffekten durchführen zu können, wird eine multiple lineare Regression eingesetzt, das heißt eine Regressionsanalyse mit mehreren unabhängigen Variablen. Von einem Moderatoreffekt spricht man immer dann, wenn eine dritte Variable – die sogenannte Moderatorvariable – den Effekt eines Prädikators oder mehrerer Prädiktoren auf die unabhängige Variable beeinflusst (Urban & Mayerl 2018). „Eine Moderatorvariable beeinflusst also nicht die Ausprägung einer abhängigen Variablen, sondern den Effekt auf die Y-Variable“ (ebd., S. 325). Grafisch lässt sich das wie folgt veranschaulichen:

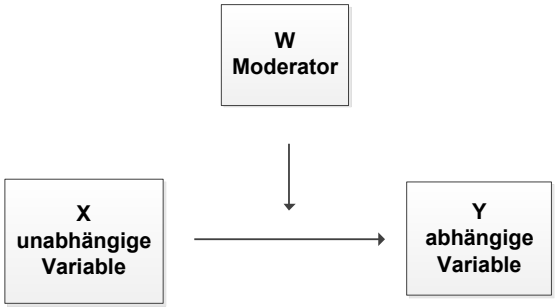


Abb. 41: Pfaddiagramm des Moderatoreffekts (Urban & Mayerl 2018)

Bezüglich des Regressionsmodells zur Analyse des Moderatoreffekts ergibt sich ein Modell mit drei Prädiktoren und einem Kriterium. Hierbei fungieren sowohl die unabhängige Variable als auch die Moderatorvariable als Prädiktor für die abhängige Variable. Zusätzlich wird das Produkt aus der unabhängigen und der Moderatorvariable als dritter Prädiktor in das Modell aufgenommen. Dies veranschaulicht Hayes in seiner statistischen Darstellung des Modells (siehe Abbildung 42).

[37] Partial ist sie deshalb, weil auf weitere gleichzeitige Korrelationen kontrolliert wird.

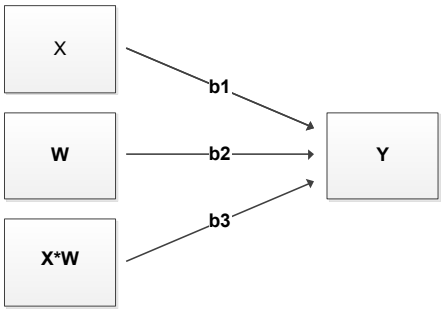


Abb. 42: Statistisches Diagramm des Regressionsmodells (Hayes 2018, S. 21)

Um eine multiple lineare Regressionsanalyse durchführen zu können, bedarf es der Erfüllung unterschiedlicher Voraussetzungen. Eine dieser Voraussetzungen ist die Annahme der Linearität der Zusammenhänge von abhängigen und unabhängigen Variablen (Kuß & Eisend 2010), die durch Scatterplots überprüft werden kann.

Als weitere Voraussetzung ist es notwendig, dass die einzelnen Prädiktoren in der multiplen Regression nicht zu hoch miteinander korrelieren; es darf keine Multikollinearität vorliegen. Diese Voraussetzung ist bei der Moderatoranalyse oft verletzt, da naturgemäß zwischen dem Produkt aus zwei metrischen Prädiktoren und den Prädiktoren selbst eine hohe Korrelation vorliegt. Oft wird deshalb empfohlen, die Prädiktoren zu zentrieren, um die Multikollinearität zu senken, die jedoch nach Hayes ein Mythos ist:

> „If you say this, you are just perpetuating a myth. Although mean-centering does reduce collinearity, this has no consequence on the estimation accuracy, hypothesis tests, or standard errors of regression coefficients in most circumstances you are likely to encounter“(Hayes 2018, S. 312).

Eine weitere wichtige Voraussetzung ist die Homoskedastizität der Residuen (Janssen & Laatz 2017) und deren Normalverteilung (Fromm & Baur 2008). Wenn diese Voraussetzungen nicht gegeben sind, muss damit strategisch umgegangen werden, wie es unter anderem von Janssen und Laatz (2017) empfohlen wird. Im Falle der fehlenden Normalverteilung der Residuen schlagen die Autoren bei positiver Schiefe eine logarithmische Transformation der y-Variablen und bei einer negativen Schiefe eine quadratische Transformation vor. Falls auch durch Transformationen keine Normalverteilung der Residuen erreicht wird, kann Bootstrapping verwendet werden. Auch die Heteroskedastizität kann teilweise mit Transformationen behoben werden. Ist das jedoch nicht möglich, sollten die Standardfehler und Signifikanzwerte anhand einer Methode geschätzt werden, welche gegenüber der Heteroskedastizität robust ist. Das ist die nach Hayes (2007)

inzwischen etablierte Methode. Es gibt verschiedene Schätzmethoden für diese sogenannten Heteroscedasticity-consistent Standard Errors (HCSE), die als HC0 bis HC5 bezeichnet werden: „Three alternative estimators, HC1, HC2, and HC3, are all asymptotically equivalent to HC0 but have far superior small sample properties relative to HC0“

(Long & Ervin 2000, S. 218). Weitere Untersuchungen von Darlington und Hayes (2017) haben gezeigt, dass HC3 und HC4 am besten funktionieren, wenn die Annahme der Homoskedastizität erfüllt ist. Untersuchungen von Witzke (2016) zeigen jedoch, dass es keine grundlegenden Unterschiede in der Signifikanz der Ergebnisse von HC4 zu HC0 bis HC3 gibt.

Die hier vorgenommene Analyse wurde diesbezüglich mit dem HCSE-Schätzer HC3 durchgeführt sowie mit einem Bootstrapping mit 5000 replizierten Stichproben, da dies laut Hayes (2018) in den meisten Anwendungsfällen ausreicht, um die Grenzen der Konfidenzintervalle ausreichend genau zu schätzen. Das Konfidenzintervall wurde mit 95 % (5 %-Signifikanzniveau) festgelegt. Die statistische Signifikanz wurde dann anhand dieser Konfidenzintervalle bestimmt. Da die statistische Signifikanz jedoch ebenfalls von der Stichprobengröße abhängt, waren die Konfidenzintervalle als alleiniges Merkmal unzureichend. Bei der Ermittlung der statistischen Signifikanz wurde deshalb die Effektstärke berechnet, die hier als Bestimmtheitsmaß bzw. als Determinationskoeffizient R^2 angegeben wird.

5.4.4 Umgang mit Fehlern erster und zweiter Art

Inferenzstatistische Berechnungen, mit denen Wahrscheinlichkeitsaussagen getroffen werden, sind oft fehlerbehaftet. Das hat zwei Gründe, denn bei der Entscheidung für oder gegen eine Hypothese kann es zu zwei Arten von statistischen Fehlentscheidungen kommen: Das Ablehnen der Nullhypothese, obwohl sie zutrifft, wird als Fehler erster Art (Krämer et al. 2018) oder als α-Fehler bezeichnet (Schäfer 2016). Das Nichtablehnen der Nullhypothese, obwohl sie falsch ist, wird als Fehler zweiter Art (Krämer et al. 2018) oder β-Fehler bezeichnet (Hornsteiner 2012). Eine Übersicht bietet die Tabelle 27.

Tab. 27: Fehlermöglichkeiten bei der Anwendung von Signifikanztests (Janssen & Laatz 2017, S. 317)

Entscheidung für	objektiv richtig	
	H0	H1
H0	richtig entschieden	Fehler 2. Art β-Fehler
H1	Fehler 1. Art α-Fehler	richtig entschieden

Vor diesem Hintergrund wird für statistische Entscheidungen ein Signifikanzniveau α festgelegt, das oft auch als Irrtumswahrscheinlichkeit bezeichnet wird (Urban & Mayerl 2011). Es entspricht der Wahrscheinlichkeit, einen Fehler erster Art zu begehen (Kähler 2004; Loviscach 2015). Üblicherweise wird in empirischen Studien α = .05 als Signifikanzniveau festgesetzt. „Die Wahl eines Signifikanzniveaus in Höhe von 5% bedeutet, dass man – ausgehend von vielen Stichprobenziehungen – in 5% der Stichproben bereit

ist, die richtige Hypothese H0 zugunsten von H1 zu verwerfen“ (Janssen & Laatz 2017, S. 313).

Werden mehrere voneinander unabhängige Signifikanztests mit derselben Stichprobe unter der gleichen globalen Fragestellung analysiert, besteht die Gefahr einer Alphafehlerkumulierung, also einer Inflation des Alphafehlers (Bortz, Lienert & Boehnke 2008). Dem muss durch eine Adjustierung des α-Niveaus entgegengewirkt werden. Ein mögliches Verfahren hierzu ist Fishers Least-Significant-Difference(LSD)-Test, der als liberaler Test beschrieben wird (George & Mallery 2019), da er dazu tendiert, zu viele Signifikanzen aufzuzeigen. Im Gegensatz dazu ist der Scheffé-Test konservativer (George & Mallery 2019). „Beim Scheffé-Test handelt es sich um einen robusten Test, d.h. er ist gegenüber Verletzungen der zu erfüllenden Voraussetzungen unempfindlich“ (Kähler 2004, S. 342). Ein weit verbreitetes und zugleich sehr konservatives Verfahren zur Adjustierung des Alphaniveaus beim multiplen Testen ist die Bonferroni-Prozedur. Hierbei wird das Alphaniveau durch die Gesamtzahl der durchgeführten Tests dividiert (George & Mallery 2019). Beachtet werden muss jedoch, dass eine α-Adjustierung immer eine Erhöhung der ß-Fehler-Wahrscheinlichkeit bedingt (Mengering 2011), sodass die Teststärke abnimmt.

In der vorliegenden Studie war eine α-Adjustierung nötig, da alle Signifikanztests der vielen Globalhypothesen an der gleichen Stichprobe vorgenommen wurden. Als Verfahren wurde die Adjustierung nach Bonferroni ausgewählt, da die Bonferroni-Korrektur konservativ ist und auch bei abhängigen Tests eingesetzt werden kann (Krauth 1973).

5.4.5 Umgang mit fehlenden Werten

Da die Studie mehrere Messzeitpunkte beinhaltete, fehlen von einigen Teilnehmenden Daten zum dritten Messzeitpunkt. Daher stellte sich die Frage, welche Daten in die Auswertung einfließen sollten. Hierzu gab es grundsätzlich zwei Möglichkeiten: Zum einen bot sich die Completer-Analyse an, die nur diejenigen Fälle in die Auswertung einbezieht, von denen von der Prä- über die Post- bis zur Follow-up-Erhebung vollständige Daten vorliegen. Zum anderen gab es die Möglichkeit der Intention-to-treat-Analyse (ITT), wobei alle Teilnehmenden eingeschlossen werden, die am Anfang die Intention geäußert hatten, an der Studie teilnehmen zu wollen, unabhängig davon, ob sie es im Verlauf der Studie tatsächlich taten (Berking & Rief 2012).

In der vorliegenden Auswertung kam die ITT-Analyse zum Einsatz, da so die Vergleichbarkeit von EG und KG erhalten blieb und der α-Fehler reduziert wurde (Kleist 2009). Sobald aber der dritte Messzeitpunkt mit in die Analyse aufgenommen wurde, wurden die dort fehlenden Teilnehmenden automatisch ausgeschlossen.

6 Ergebnisse

6.1 Darstellung der Stichprobe

Es nahmen 130 Teilnehmende in der EG und 165 Teilnehmende in der KG an der präventiven Veranstaltung teil. Davon gaben 108 Teilnehmende der EG und 110 der KG einen Fragebogen zu t1 und t2 ab. Die Abgabe erfolgte in 24 Veranstaltungen zwischen dem 21.02.2018 und dem 20.12.2018. 93 Teilnehmende der EG und 89 Teilnehmende der KG gaben darüber hinaus einen Fragebogen zu t3 zurück, sodass auch hier von einer hohen Teststärke auszugehen ist, da n > 50. Eine ausführliche Stichprobenbeschreibung ist in den Tabellen 28 und 29 und in der Abbildung 43 zu finden.

Tab. 28: Stichprobenbeschreibung hinsichtlich Gruppe, Geschlecht und Bildungsniveau

		KG			EG	
	Gesamt	männlich	weiblich	Gesamt	männlich	weiblich
n (t1)	110	52	58	108	52	56
Berufsausbildung		14	6		20	12
Fachhochschule		19	17		16	22
Hochschule		17	30		12	22
andere Bildung		2	5		4	0
n (t2)	110	52	58	108	52	56
Berufsausbildung		14	6		20	12
Fachhochschule		19	17		16	22
Hochschule		17	30		12	22
andere Bildung		2	5		4	0
n (t3)	89	40	49	93	51	42
Berufsausbildung		13	4		20	10
Fachhochschule		15	13		15	15
Hochschule		10	27		12	17
andere Bildung		2	5		4	0

Tab. 29: Stichprobenbeschreibung hinsichtlich des Alters

EG				KG			
n = 108				n = 110			
M	*SD*	*MIN*	*MAX*	*M*	*SD*	*MIN*	*MAX*
51.7	12.5	22	67	44.1	9.6	22	62

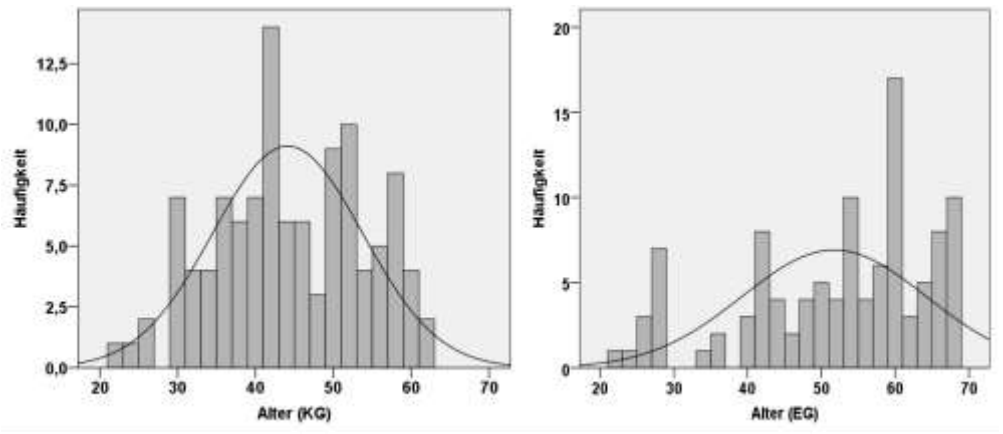


Abb. 43: Häufigkeitsverteilungen des Alters in der EG und der KG zu t1 und t2

Die Bildungsmotivation in der EG ist nach Bilanzwert[38] und Erfolgserwartung ausgeglichen und in beiden Gruppen annähernd gleich verteilt (siehe Tabelle 30).

Tab. 30: Motivation der Experimentalgruppe

		Motivation_Bilanzwert	Motivation_Erfolgserwartung
n	gültig	108	108
	fehlend	0	0
Mittelwert		2.7789	2.7006

Ähnliche Konstellationen sind in der KG vorhanden, wie in der Tabelle 31 deutlich wird.

Tab. 31: Motivation der Kontrollgruppe

		Motivation_Bilanzwert	Motivation_Erfolgserwartung
n	gültig	110	110
	fehlend	0	0
Mittelwert		2.8034	2.8303

6.2 Analyse der fehlenden Werte

Die Analyse der fehlenden Werte[39] zeigt keine fehlenden Werte zu t1 und t2 bei den untersuchten Variablen. Dies wurde dadurch erreicht, dass die ProbandInnen aufgefordert wurden, die eigenen Datensätze nachträglich auf Vollständigkeit zu überprüfen. Diese Maßnahme konnte jedoch zum Messzeitpunkt t3 nicht angewendet werden, sodass hier einige Datensätze fehlende Werte aufweisen. Diese Fälle wurden jedoch in die Auswertungen nicht mit einbezogen.

[38] Der Bilanzwert wird als proximaler Prädiktor der Fortbildungsteilnahme verstanden (Gorges et al. 2017).

[39] BenutzerInnendefinierte fehlende Werte.

6.3 Explorative Faktorenanalysen der neu entwickelten Erhebungsinstrumente

Nachfolgend wird für die neu eingesetzten Erhebungsinstrumente eine explorative Faktorenanalyse durchgeführt (siehe Tabelle 32).

Tab. 32: Entwickelte Messinstrumente

Skala *Subskala*	Quelle	Anzahl Items	Reliabilität	Administration zu Messzeitpunkt mit Erhebungsinstrument		
				F1 (t1)	F2 (t2)	F2 (t3)
geplantes Verhalten im Kontext von IT-Sicherheit	Hiemisch (2017)	26	.	x	x	x x x
Beweggründe für die Teilnahme	Eigenentwicklung	6		x		

6.3.1 Hauptkomponentenanalyse des Fragenkomplexes FK1

In die EFA flossen 26 Likert-skalierte-Items ein (siehe Tabelle 33). Als Verfahren wurde die Hauptkomponentenanalyse (PCA) gewählt. Die Stichprobengröße umfasst n = 218 und wurde und wird deshalb als ausreichend angesehen (Behnke 2015). Die Eignung der Daten wurde anhand des KMO-Werts überprüft. Dieser beträgt .79, die Daten sind somit mittelmäßig geeignet (siehe Tabelle 25). Der Bartlett-Test wird signifikant, χ^2 (325) = 2915.23, $p < .001$, woraufhin die Nullhypothese, die besagt, dass die Stichprobe aus einer Grundgesamtheit entstammt, in der die Variablen unkorreliert sind, verworfen werden kann. Diese Signifikanz ist jedoch kritisch zu betrachten, da keine Normalverteilung vorliegt (Bühner 2006). Wobei darauf hinzuweisen ist, dass bei $p < .001$ kaum Gefahr besteht, dass die Signifikanz derart verzerrt ist, dass es sprunghaft steigt.

Die MSA-Werte als Indikatoren, ob die einzelnen Items in die Faktorenanalyse einbezogen werden sollten, liegen überwiegend über 50. Eine Löschung aufgrund statistischer Kennwerte wird hier noch nicht empfohlen, weil die Items inhaltlich eine zentrale Bedeutung haben (Bühner 2006). Die Kommunalitäten aller Items liegen bei der Hauptkomponentenanalyse bei $h^2 > .50$. Schwache Items ($h^2 < .10$) lassen sich auch mit den Extraktionsmethoden Hauptfaktorenanalyse und Maximum Likelihood nicht identifizieren (siehe Tabelle 33). Demnach wurden alle Items in die Faktorenanalyse einbezogen.

Tab. 33: Kommunalitäten der Items zum geplanten Verhalten

Items	Analyse der Hauptkomponente		Hauptachsenfaktorenanalyse		Maximum Likelihood	
	anfänglich	Extraktion	anfänglich	Extraktion	anfänglich	Extraktion
m1_vor	1,000	,724	,672	,646	,672	,668
m2_vor	1,000	,654	,588	,576	,588	,569
m3_vor	1,000	,738	,589	,647	,589	,580
m4_vor	1,000	,666	,537	,520	,537	,471
m5_vor	1,000	,750	,714	,734	,714	,748
m6_vor	1,000	,658	,573	,515	,573	,504
m7_vor	1,000	,730	,629	,661	,629	,638
m8_vor	1,000	,730	,527	,581	,527	,577
m9_vor	1,000	,632	,421	,435	,421	,453
m10_vor	1,000	,739	,508	,668	,508	,642
m11_vor	1,000	,641	,587	,544	,587	,519
m12_vor	1,000	,669	,653	,608	,653	,616
lm13_vor	1,000	,569	,301	,170	,301	,126
m14_vor	1,000	,678	,650	,607	,650	,577
m15_vor	1,000	,782	,461	,624	,461	,999
m16_vor	1,000	,686	,680	,682	,680	,767
m17_vor	1,000	,753	,748	,751	,748	,800
m18_vor	1,000	,576	,341	,306	,341	,283
m19_vor	1,000	,745	,710	,711	,710	,719
m20_vor	1,000	,748	,687	,725	,687	,723
m21_vor	1,000	,679	,561	,510	,561	,473
lm22_vor	1,000	,648	,508	,547	,508	,546
lm23_vor	1,000	,598	,462	,395	,462	,385
m24_vor	1,000	,673	,511	,426	,511	,356
m25_vor	1,000	,762	,684	,732	,684	,750
m26_vor	1,000	,789	,702	,761	,702	,764

Bezüglich der Anzahl zu extrahierender Faktoren kommen die verschiedenen Vorgehensweisen zu unterschiedlichen Ergebnissen: Gemäß dem Kaiser-Guttman-Kriterium, das einen Eigenwert > 1.0 fordert, um einen Faktor zu extrahieren, lassen sich sieben Faktoren extrahieren, die eine Gesamtvarianz von 68.00 % für die Analyse der Hauptkomponente erklären.

Der Scree-Plot zeigt einen Knick beim vierten Faktor und ab dort einen nahezu parallelen Verlauf zur x-Achse (Komponentennummer), sodass von drei extrahierten Faktoren ausgegangen werden kann (siehe Abbildung 44).

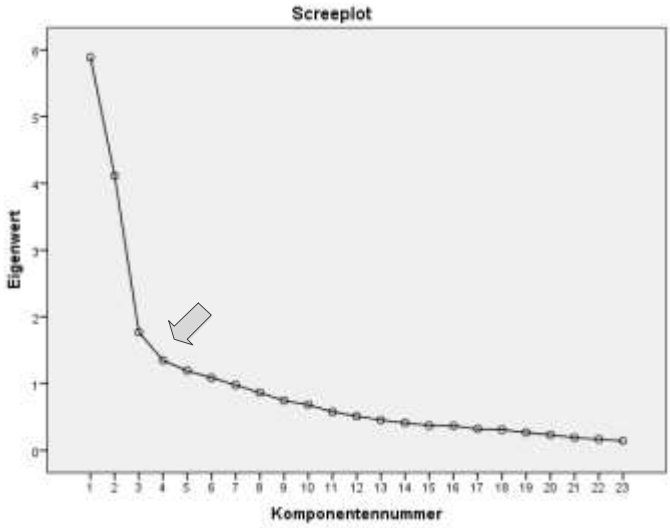


Abb. 44: Scree-Plot zum Fragenkomplex ‚geplantes Verhalten'

Gemäß der Parallelanalyse nach O'Connor, beruhend auf einer Hauptkomponentenanalyse mit einem 95 %-Konfidenzintervall, n = 218 Fällen, 26 einbezogenen Variablen und 1000 zufälligen Eigenwerten (ncases[40] = 218, nvars[41] = 26, ndatsets[42] = 1000, percent[43] = 95, kind[44] = 1), lassen sich gleichfalls drei Faktoren identifizieren (siehe Tabelle 34).

Tab. 34: Vergleich Eigenwertverlauf zufällig vs. empirisch

zufällig erzeugter Eigenwertverlauf	empirischer Eigenwertverlauf	Vergleich
1.695	6.258	<
1.586	4.305	<
1.500	2.033	<
1.431	1.41	>
1.367	1.31	>

Aufgrund der Übereinstimmung der Ergebnisse von Scree-Plot und Parallelanalyse werden im Folgenden drei Faktoren extrahiert und anschießend rotiert, da die subjektive Interpretation des Scree-Plots mit der Berechnung übereinstimmt.

Als Rotationsverfahren wurde gemäß der Empfehlung von Bühner zuerst das oblique Promax- und anschließend das orthogonale Varimax-Verfahren angewendet, um die Stabilität der Faktoren abzusichern (Bühner, 2011). Das Promax-Verfahren mit Kaiser-Normalisierung wurde mit einem Kappa mit dem Standardwert von 4 durchgeführt. Hinsichtlich der Konvergenzvalidität war die Faktorladung auf Nebenladungen

[40] Anzahl der Fälle.
[41] Anzahl der Zufallsvariablen.
[42] Anzahl der zufälligen Eigenwerte.
[43] Perzentil.
[44] Hauptkomponentenanalyse = 1, Hauptachsenanalyse = 2.

(„secondary loading“) zu überprüfen, also auf Faktorenladungen, die ebenfalls eine Ladung auf andere Faktoren zeigen (Raithel 2008). Items, die eine Nebenladung besitzen (> 0.3), wurden in der weiteren Analyse ignoriert.

Anschließend wurden die extrahierten Faktoren inhaltlich interpretiert in Einstellung, Selbstwirksamkeit im Kontext von IT-Sicherheit und Kontrollüberzeugung, wie es in der Tabelle 35 abgebildet ist.

Tab. 35: Faktorladung beim Fragenkomplex ‚geplantes Verhalten‘

Skalen/Items	Faktorladung (Varimax)	Faktorladung (Promax) Mustermatrix
Einstellung		
m1_vor (Ich finde es wichtig, darüber Bescheid zu wissen, wie man im Internet betrogen werden kann.)	.739	.754
m2_vor (Nur wenn ich mich regelmäßig informiere, kann ich verhindern, Betrügern im Netz zum Opfer zu fallen.)	.771	.774
m3_vor (Mir ist es wichtig, über Betrugs- und Manipulationsmöglichkeiten im Netz auf dem Laufenden zu bleiben.)	.732	.736
m4_vor (Ich versuche, mich regelmäßig über Möglichkeiten der Datensicherheit auf den neusten Stand zu bringen.)	.508	Nebenladung
m5_vor (Um mich wirksam gegen Betrug im Netz zu schützen, muss ich wissen, wie ich sicher mit meinen Daten umgehe.)	.808	.803
m6_vor (Datensicherheit ist keine einmalige Angelegenheit, sondern ein laufender Prozess, und muss immer wieder aktualisiert werden.)	.695	.691
m7_vor (Ich versuche meine Kenntnisse zu erweitern, wie ich mich vor Betrug mit dem Internet schützen kann.)	.697	.685
m8_vor (Von Zeit zu Zeit erkundige ich mich über neue Formen des Internetbetrugs, um nicht selbst Opfer zu werden.)	.560	.546
m21_vor (Die Sicherheit meiner Daten ist mir sehr wichtig.)	.563	.573
Selbstwirksamkeit im Kontext von IT-Sicherheit		
m9_vor (In der Regel sagt einem der gesunde Menschenverstand, wie man sich vor Betrug im Netz schützen kann.)	.500	.495
m10_vor (Es ist nicht schwer, über den Stand von Betrugs- und Manipulationsmöglichkeiten im Netz auf dem Laufenden zu bleiben.)	.545	.543
m11_vor (Ich kann mich gut gegen Betrug im Netz schützen.)	.706	.705
m12_vor (Mir fällt es leicht, mich regelmäßig über die Entwicklungen bei der Internetkriminalität zu informieren.)	.723	.718
m14_vor (Ich weiß, wie ich mich informieren muss, um vor Betrügereien im Netz sicher zu sein.)	.728	.721
m16_vor (Ich traue mir zu, mich effektiv vor Betrug im Netz zu schützen.)	.710	.706
m17_vor (Ich weiß, wie ich mich verhalten muss, um vor Tricksereien im Netz sicher zu sein.)	.802	.807
m19_vor (Mich regelmäßig darüber zu informieren, wie ich mich gegen Betrug im Netz schützen kann, fällt mir leicht.)	.808	.804
m20_vor (Ich weiß, was ich tun muss, um meine Daten vor Missbrauch zu schützen.)	.767	.771
m22_vor (Ich versuche bezüglich der Möglichkeiten, meine Daten zu schützen, auf dem Laufenden zu bleiben.)	Nebenladung	Nebenladung

Skalen/Items	Faktorladung (Varimax)	Faktorladung (Promax) Mustermatrix
m25_vor (Ich bin hinreichend informiert, um Internetbetrügern nicht auf den Leim zu gehen.)	Nebenladung	Nebenladung
m26_vor (Ich weiß genug, um nicht auf Tricks von Internetbetrügern hereinzufallen.)	.751	.741
Kontrollüberzeugung		
m13_vor (Im Alltag ist es mir zu aufwendig, auf dem neusten Stand zu bleiben, was Betrugsmöglichkeiten im Netz angeht.)	.408	.398
m15_vor (Im Umgang mit meinen Daten bin ich leichtsinnig.)	.604	.631
m18_vor (Mir ist es zu umständlich, sicher mit meinen Daten umzugehen, auch wenn ich eigentlich wüsste, wie es geht.)	.575	.804
m23_vor (In der Hektik des Alltags kommt die Datensicherheit bei mir zu kurz.)	.542	Nebenladung
m24_vor (Um mich wirksam gegen Betrug im Netz zu schützen, muss ich mich mit Maßnahmen der Datensicherheit auskennen.)	Nebenladung	Nebenladung

Auffällig ist, dass fünf Items im Rotationsverfahren Promax und drei Items im Rotationsverfahren Varimax Nebenladungen aufweisen.

Für das Varimax-Verfahren finden folgende Nebenladungen statt:

- Item: m22_vor zwischen Selbstwirksamkeit im Kontext von IT-Sicherheit und Einstellung (.375 – .455)
- Item: m25_vor zwischen Selbstwirksamkeit im Kontext von IT-Sicherheit und Kontrollüberzeugung (.723 – 328)
- Item: m24_vor zwischen Einstellung und Kontrollüberzeugung (.439 – 436).

Um eine höchstmögliche Konvergenzvalidität zu erreichen, wurden alle Items, die eine Nebenladung nach dem orthogonalen Rotationsverfahren aufweisen, in den weitergehenden Analysen ignoriert, da unabhängige Faktoren erzeugt wurden (Bühner 2006). Die so gebildeten Skalen wurden einer Reliabilitätsanalyse unterzogen, die quantifiziert, inwieweit die einzelnen Items der Skala das gleiche theoretische Konstrukt messen. Als Maßzahl gilt Cronbachs Alpha (α), ein Maß für die interne Konsistenz einer Skala (Schwarz 2012).

Die neugebildete Skala zum Thema Einstellung mit neun Items weist eine interne Konsistenz von α = .823 auf. Diese Reliabilität ist zufriedenstellend, da eine interne Konsistenz bereits ab .70 als ausreichend gut gilt (Cronbach 1990). Daher war es nicht notwendig, einzelne Items aus der Skala zu entfernen, um die Reliabilität anzuheben.

Die neu gebildete Skala zum Thema Selbstwirksamkeit im Kontext von IT-Sicherheit mit zehn Items weist eine interne Konsistenz von α = 0.89 auf. Die neu gebildete Skala zum Thema Kontrollüberzeugung mit drei Items weist eine interne Konsistenz von α = .64 auf und ist damit noch ausreichend, da Cronbachs Alpha bei kurzen Skalen automatisch niedriger ist. Die Abbildung 45 zeigt die finalen Skalen und die jeweils zugehörigen Items reflektiv.

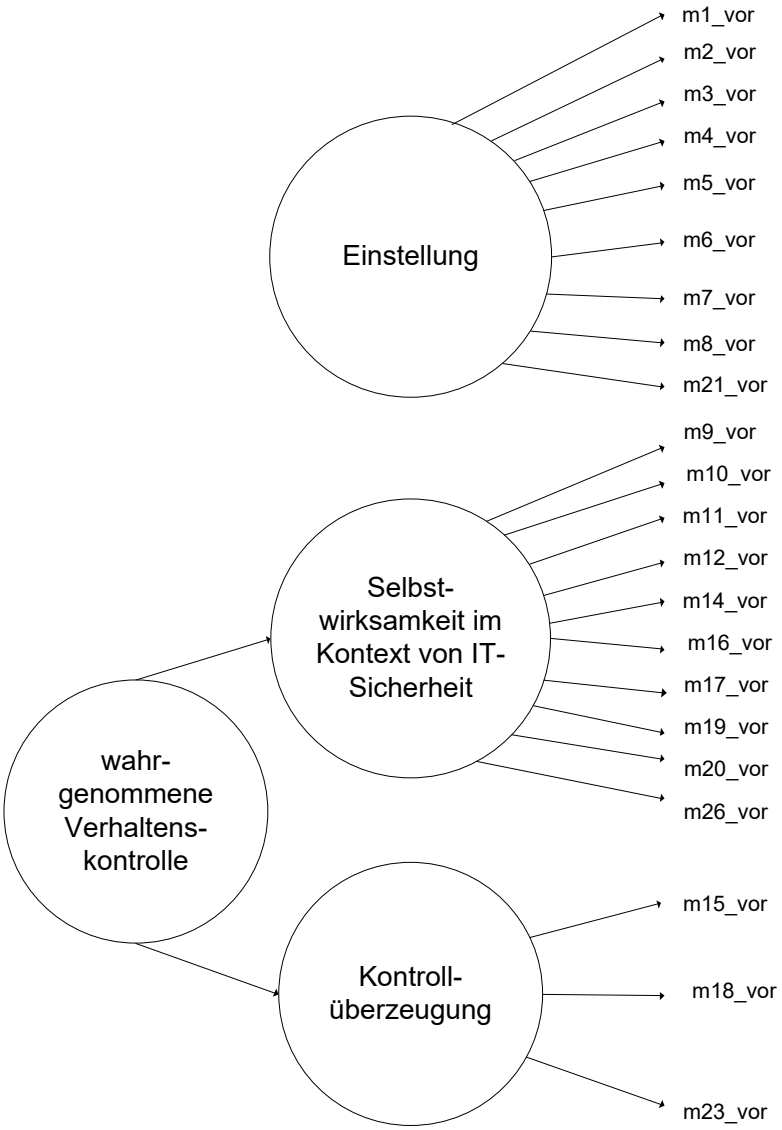


Abb. 45: Optimierte Faktorladung zu FK5

Die drei extrahierten Faktoren lassen sich dementsprechend als Skalen zu den Themen Einstellung, Selbstwirksamkeit und Kontrollüberzeugung im Kontext von IT-Sicherheit identifizieren. Es wurde erwartet, dass auch die Urteilsfähigkeit eine eigene Skala darstellen würde – jedoch lässt sich diese Erwartung nicht mit dem dreifaktoriellen Modell abbilden.

Fazit zu Hypothese H1

Die Skalen decken die Themen Einstellung, Selbstwirksamkeit im Kontext von IT-Sicherheit und Kontrollüberzeugung ab, jedoch nicht die Urteilsfähigkeit. Somit ist die Nullhypothese für die Urteilsfähigkeit zu akzeptieren und die Alternativhypothese für die Urteilsfähigkeit abzulehnen. Für die Skalen der Themen Einstellung, Selbstwirksamkeit und Kontrollüberzeugung im Kontext von IT-Sicherheit kann jedoch die Nullhypothese verworfen und die Alternativhypothese akzeptiert werden.

6.3.2 Hauptkomponentenanalyse des Fragenkomplexes FK2

Die Hauptkomponentenanalyse erfolgte sequenziell in der ersten Sequenz mit dem Kaiser-Guttman-Kriterium > 1 mit folgenden Items: d1, d2, d3, d4, d5, d6, d7.

Gemäß dem Kaiser-Guttman-Kriterium > 1 lassen sich zwei Faktoren extrahieren, die eine Gesamtvarianz von 53 % abdecken. Der KMO-Wert beträgt .63, die Sphärizität, geprüft durch den Bartlett-Test, weist ein χ^2= 268,93 bei 21 Freiheitsgraden (df) aus und wird somit signifikant (p < 0.01). Diese Signifikanz ist jedoch auch hier kritisch zu betrachten, da keine Normalverteilung vorliegt und der Test auch bei größeren Stichproben fast immer signifikant werden kann (Bühner 2006). Die MSA-Werte liegen alle über 5.

Die Kommunalität aller Items liegt bei der Analyse der Hauptkomponenten überwiegend bei h² > .5. Schwache Kommunalitäten (h² < .10) lassen sich jedoch für das Item d1 mit den Extraktionsmethoden Hauptfaktorenanalyse und Maximum Likelihood identifizieren (siehe Tabelle 36).

Tab. 36: Kommunalitäten der Items zu den Beweggründen für die Teilnahme

Hauptkomponentenanalyse			Hauptachsenfaktorenanalyse		Maximum Likelihood	
Item	anfänglich	Extraktion	anfänglich	Extraktion	anfänglich	Extraktion
d1	1.000	.248	.099	.082	.099	.060
d2	1.000	.447	.237	.269	.237	.237
d3	1.000	.662	.357	.589	.357	.600
d4	1.000	.482	.322	.338	.322	.342
d5	1.000	.561	.264	.325	.264	.340
d6	1.000	.720	.309	.807	.309	.999
d7	1.000	.594	.286	.311	.286	.284

Das Item d1 kann dementsprechend einem eigenen Konstrukt zugeordnet werden, nämlich der Betroffenheit durch einen Sicherheitsvorfall. Gemäß dem Scree-Plot-Kriterium ließen sich zwei Faktoren ermitteln (siehe Abbildung 46).

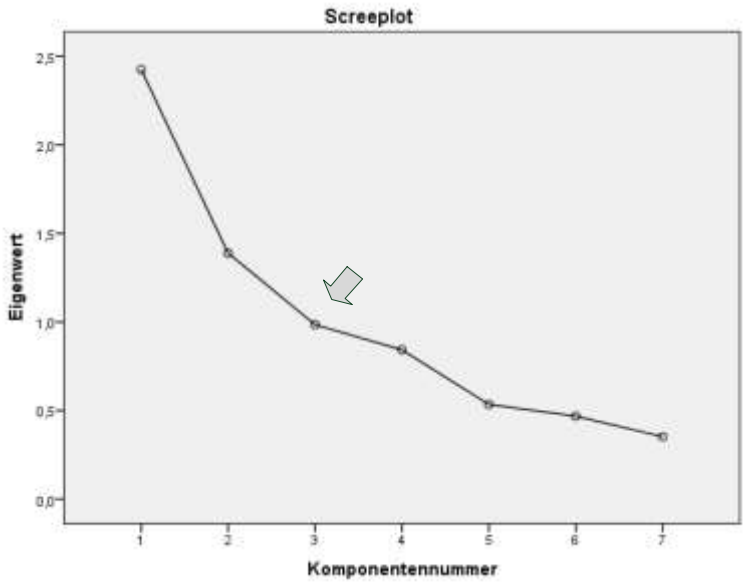


Abb. 46: Scree-Plot zum Fragenkomplex ‚Beweggründe für die Teilnahme'

Zu dem gleichen Ergebnis kam die Parallelanalyse nach O'Connor (ncases = 218, nvars = 7, ndatsets = 1000, percent = 95, kind = 1), wie aus der Tabelle 37 hervorgeht.

Tab. 37: Vergleich Eigenwertverlauf zufällig vs. empirisch

zufällig erzeugter Eigenwertverlauf	empirischer Eigenwertverlauf	Vergleich
1.259	2.374	<
1.150	1.340	<
1.066	0	>

Als Rotationsverfahren wurde auch hier das Promax- und anschließend das Varimax-Verfahren (Hauptkomponentenanalyse) verwendet, um die Stabilität der Faktoren abzusichern. Das Promax-Verfahren wurde mit Kappa 4 standardmäßig durchgeführt. Hinsichtlich der Konvergenzvalidität wurde ebenfalls die Faktorladung auf Nebenladungen überprüft. Items, die eine Mehrfachladung besitzen (> .3), wurden in der weiteren Analyse ignoriert. Wie in der Tabelle 38 ersichtlich wird, gab es allerdings keine Nebenladungen. Die Items wurden den gleichen Faktoren zugeordnet, was auf eine stabile Faktorenstruktur hinweist, die somit methodeninvariant wird. Die erzeugten Faktoren lassen sich den theoretischen Konstrukten themenbezogen und nicht themenbezogen zuordnen.

Tab. 38: Faktorladung – Beweggründe der Teilnahme

	Faktorladung Varimax	Faktorladung Promax Musterstruktur
themenbezogen: Ich nehme teil, weil …		
d2 (… mich das Thema interessiert.)	.701	.710
d3 (… die Kenntnisse, die ich erwerbe, mir im Alltag helfen.)	.820	.834
d4 (… es mir Spaß macht, mich für neue Dinge zu interessieren.)	.576	.530
d5 (… es mir beruflich nützt.)	.732	.750
nicht themenbezogen		
d6 (… ich mich kreativ betätigen möchte.)	.898	.927
d7 (… ich Menschen kennenlerne.)	.786	.785

Beurteilung der Reliabilität der Skala

Ohne Selektierung der entsprechenden Items (Reliabilitätserhöhung) ergibt sich für die komplette Skala ein Cronbachs α = .652. Sie liegt damit zwischen der Interpretation Fragwürdigkeit und Akzeptabilität (George & Mallery 2019). Eine Löschung von Items kann die Reliabilität nicht weiter erhöhen. Die Skala „nicht themenbezogen“ lädt auf zwei Items, nach Lang und Lüdtke (2005) sollte jedoch eine Skala aus mindestens drei Items bestehen.

Eine theoriebezogene Begutachtung der Faktorladung zeigt, dass das Item d4 der Skala „nicht themenbezogen“ zugeordnet werden kann, da es inhaltlich zu diesem Konstrukt (besser) passt (siehe Abbildung 47 zu den extrahierten Likert-Items und den zusammengefassten Likert-Skalen) und da d4 auch die niedrigste Faktorladung beim ursprünglichen Konstrukt hatte.

Die neugebildete Skala „themenbezogene Weiterbildung“ mit drei Items weist eine interne Konsistenz von α = .630 auf. Die Skala „nicht themenbezogene Weiterbildung“ mit drei Items weist eine ähnlich hohe interne Konsistenz von α =.639 auf. Die neugebildete Skala „Beweggründe für die Teilnahme“ mit drei Items weist eine interne Konsistenz von α = .640 aus, was noch ausreichend ist. Die Abbildung 47 zeigt die finalen Skalen und die jeweils zugehörigen Items reflektiv.

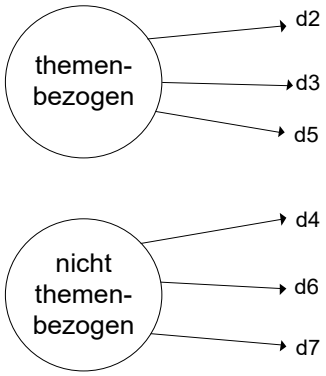


Abb. 47: Optimierte Faktorladung zu FK2

Fazit zur Hypothese H2

Die Skalen decken die themenbezogene und die nicht themenbezogene Teilnahme ab. Somit kann die Nullhypothese abgelehnt und die Alternativhypothese akzeptiert werden.

Nachfolgend werden die analysierten und vorhandenen Messinstrumente für die inferenzstatistische Auswertung eingesetzt und deren Ergebnisse präsentiert.

6.4 Inferenzstatistische Auswertung

Die inferenzstatistischen Auswertungen werden im Folgenden nach Hypothesenkomplexen geordnet und deren Ergebnisse werden dargestellt. Zuerst wird im Kapitel 6.4.1 die Wirksamkeit der präventiven Maßnahme im Vergleich zwischen der Experimental- und der Kontrollgruppe sowie im Prä-Post- und im Prä-Post-Follow-up-Vergleich untersucht (H3-H6). Anschließend werden im Kapitel 6.4.2 potenzielle Moderatoren, die die Wirksamkeit der präventiven Maßnahme beeinflussen können, überprüft (H7-H10).

6.4.1 Wirksamkeit der Maßnahme über die Zeit zwischen EG und KG

Der zweite Hypothesenkomplex (H3 bis H6) untersucht die Veränderung der Ausprägung der Zielkriterien der präventiven Maßnahme in der Experimentalgruppe im Vergleich zur Entwicklung der Kontrollgruppe.

Wirkung der Maßnahme auf die Einstellung (H3)

Es wurde angenommen, dass die Lernenden der EG ihre Einstellung stärker verändern würden als die Lernenden der Kontrollgruppe (H3). Diese Annahme wurde anhand einer zweifaktoriellen Varianzanalyse mit dem Zwischensubjektfaktor ‚Gruppenzugehörigkeit' (zu EG oder KG) und dem Messwiederholungsfaktor ‚Messzeitpunkt' mit der abhängigen

Variable ‚Einstellung' über zwei Messzeitpunkte (H3a) und über drei Messzeitpunkte (H3b) statistisch überprüft.

Dieses Vorgehen ist praktisch relevant, da die Rücklaufquote zu t1 und t2 direkt von der oder dem Lehrenden positiv beeinflusst werden konnte, im Gegensatz zum Zeitpunkt t3, der außerhalb der präventiven Maßnahme lag, sodass sich die Rücklaufquote verschlechterte (Bortz & Doering 2009). Gründe hierfür sind erfahrungsgemäß der zusätzliche Aufwand der Rücksendung (Langbehn 2010) sowie ein mangelndes Interesse an Evaluationen (Burkhardt 2001). Zusätzlich sollten deshalb später weitere Analysen mit einem weiteren Messzeitpunkt t3 erfolgen, da nur so die Messungen Entwicklungslinien abbilden konnten und eine Unterscheidung von Entwicklungen und Messfehlern möglich wurde (König 2018).

Bevor eine zweifaktorielle Varianzanalyse durchgeführt wurde, war zu prüfen, ob die Voraussetzungen für eine solche Analyse gegeben waren, also insbesondere eine Normalverteilung der Residuen. Die Normalverteilung in der EG ($p < .001$) und KG ($p < .001$) ist gemäß dem Kolmogorow-Smirnow-Test und dem Shapiro-Wilk-Test jedoch nicht gegeben, was allerdings bei der Zahl an Teilnehmenden nicht außergewöhnlich ist, da schon kleine Abweichungen von der NV den Test signifikant werden lassen. Lediglich in der KG zeigt sich eine Normalverteilung gemäß dem Kolmogorow-Smirnow-Test ($p =.163$). Aufgrund der Stabilität (Robustheit) der ANOVA ($n > 30$), die es erlaubt, mit einer Verletzung der Normalverteilung umzugehen (Bortz & Doering 2009), wurde die Untersuchung entsprechend fortgesetzt.

Die Untersuchung der Varianzhomogenität (Prä-Post-Vergleich) anhand des Levene-Tests zeigt in der EG und der KG für t1 $F(1,216) = .251$, $p = .617$ und für t2 $F(1,216) = 3.604$, $p = .002$. Das bedeutet, dass eine Varianzhomogenität nur für t1 gegeben ist. In gleich großen Gruppen und bei ausreichender Stichprobengröße sind jedoch Verletzungen der Varianzhomogenität unproblematisch (Schwarz & Enzler 2019), solange das Verhältnis 1,5 zwischen den untersuchten Gruppen nicht überschritten wird (Stevens 2002). In dieser Untersuchung liegt das Verhältnis bei 1.01, wie es sich aus den vorhandenen Stichprobengrößen ($n = 110$ vs. $n = 108$; siehe Tabelle 28) ergibt, sodass das Ergebnis somit als unproblematisch betrachtet werden kann.

Das Ergebnis der ANOVA im Prä-Post-Vergleich zeigt einen signifikanten Haupteffekt für die Gruppenzugehörigkeit ($F(1,216) = 16.388$, $p < .001$, $\eta^2 = .071$), wobei die Wahrscheinlichkeit, einen empirischen Faktor für die Gruppenzugehörigkeit mit 216 ProbandInnen zu finden, nur 7,1 % betrug. Nicht signifikant ist der Messwiederholungsfaktor, denn $F(1,216) = 1.730$, $p = .190$. Das bedeutet, dass sich die Einstellung der ProbandInnen (über beide Gruppen hinweg) über die Zeit nicht signifikant geändert hat. Aufgrund der Signifikanz des Interaktionsterms ist jedoch Vorsicht bei der Interpretation

der Haupteffekte geboten, da der Haupteffekt von der Interaktion gestört sein kann. Die Wechselwirkung zwischen den beiden Faktoren hat in diesem Fall einen hohen signifikanten Einfluss auf die Einstellung der Teilnehmenden ($F(1,216) = 9.389$, $p < .001$, $\eta_p^2 = .148$).

In der anschließenden Grafik (Abbildung 48) wird vor allem die Interaktion (= unterschiedlicher Entwicklungsverlauf der beiden Gruppen über die Zeit) sehr deutlich. Bei der EG nehmen die Werte über die Zeit zu, bei der KG jedoch ab. Da die Werte fast beim gleichen Ausgangspunkt starten (Faktor 1 = 1), kann zudem beobachtet werden, dass die Werte der Experimentalgruppe generell (unabhängig von der Zeit) größer sind als die der Kontrollgruppe.

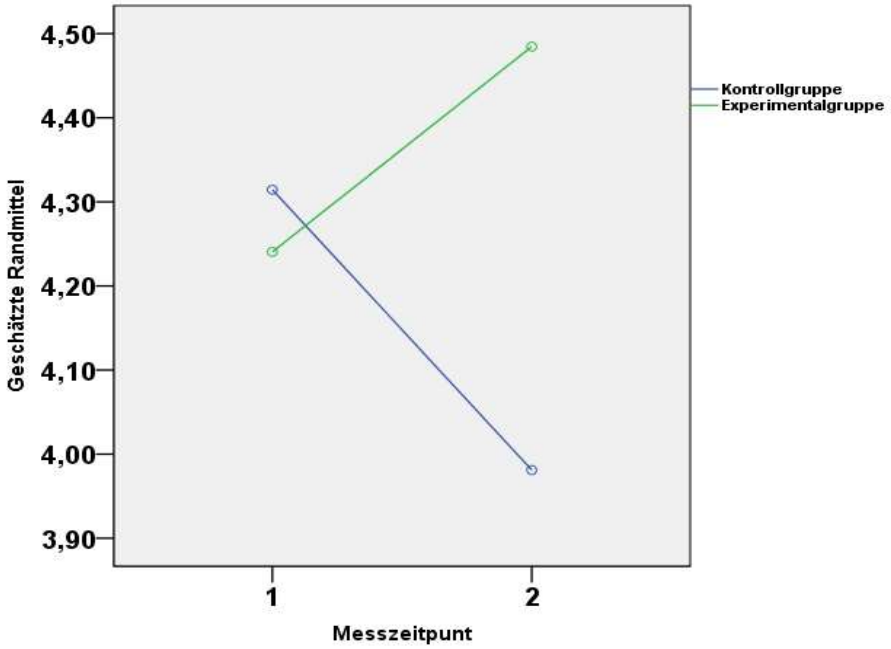


Abb. 48: Mittelwertvergleich der Einstellung der Teilnehmenden (EK/KG) zu t1 und t2

Nachfolgend dargestellt sind in der Tabelle 39 die Mittelwerte (M), Standardabweichungen (SD) und die Stichprobengröße (n).

Tab. 39: Vergleich EG und KG über zwei Messzeitpunkte im Hinblick auf das Merkmal ‚Einstellung'

		M	SD	n
t1	Kontrollgruppe	4.33	.53	110
	Experimentalgruppe	4.27	.58	108
t2	Kontrollgruppe	3.97	.62	110
	Experimentalgruppe	4.50	.48	108

Eine weitere Untersuchung erfolgte über alle Messzeitpunkte t1, t2 und t3 hinweg.

Die Untersuchung der Sphärizität anhand des Mauchly-Tests zeigt ein nicht signifikantes Ergebnis, da $\chi^2(2) = 1.412$, $p = .494$. Die Sphärizität ist somit gegeben. Die

Untersuchung der Varianzhomogenität (Prä-Post-Follow-up-Vergleich) anhand des Levene-Tests weist in der EG und KG zu t3 ein signifikantes Ergebnis auf ($F(1,180) = 17.745$, $p < .001$), nicht jedoch zu t2 ($F(1,180) = 2.342$, $p = .128$) und zu t1 ($F(1,180) = .682$, $p = .410$). Eine Varianzhomogenität ist somit nicht gegeben. Trotzdem sollte die ANOVA im Prä-Post-Follow-up-Vergleich durchgeführt werden, da die Gruppengröße annähernd gleich groß ist und die Varianzhomogenität somit kein Problem darstellt (Field, 2018). Das Verhältnis zwischen KG (n = 93) und EG (n = 89) liegt bei 1.04 und damit unter 1.5.

Das Ergebnis der ANOVA im Prä-Post-Follow-up-Vergleich zeigt einen signifikanten Haupteffekt für die Gruppenzugehörigkeit, da $F(1,180) = 101.937$, $p < .001$, $\eta_p^2 = .36$. Die Einstellungsänderung der Teilnehmenden in der Experimentalgruppe unterscheidet sich somit von der Einstellungsänderung der Teilnehmenden in der Kontrollgruppe.

Signifikant ist auch der Messwiederholungsfaktor ($F(2,360) = 4.311$, $p = .014$, $\eta_p^2 = .023$), was bedeutet, dass sich die Einstellung der ProbandInnen (über beide Gruppen hinweg) signifikant über die Zeit geändert hat. Außerdem hat die Wechselwirkung zwischen den beiden Faktoren einen signifikanten Einfluss auf die Einstellung der Teilnehmenden ($F(2,360) = 50.45$, $p < .001$, $\eta_p^2 = .21$). Die Veränderung der Einstellung über die Zeit verlief also in Abhängigkeit von der Gruppenzugehörigkeit zur EG beziehungsweise KG signifikant unterschiedlich, und die beobachteten Abweichungen scheinen systematisch zu sein.

In der folgenden Grafik ist ersichtlich, dass vor allem die Interaktion (= unterschiedlicher Verlauf der beiden Gruppen über die Zeit) sehr deutlich wird. Denn bei der EG nehmen die Werte über die Zeit zu, bei der KG jedoch ab. Da beide Werte fast beim gleichen Ausgangspunkt starten (Faktor 1 = 1), kann geschlussfolgert werden, dass die Einstellungsänderung der Experimentalgruppe generell (über die Zeit) größer ist als die der Kontrollgruppe (siehe Abbildung 49).

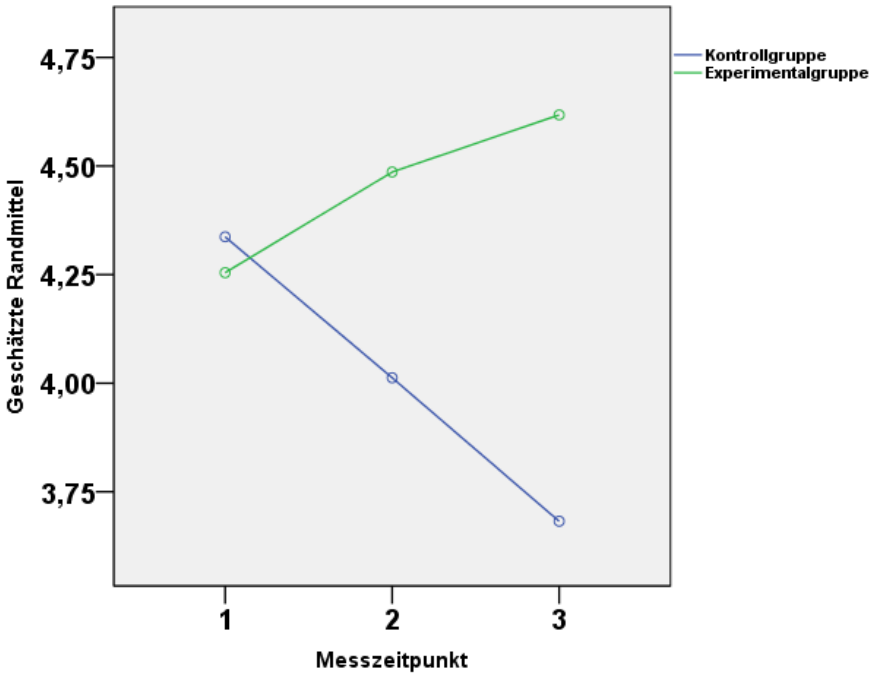


Abb. 49: Mittelwertvergleich der Einstellung der Teilnehmenden (EK/KG) zu t1, t2 und t3

In der folgenden Tabelle 40 dargestellt sind die Mittelwerte (M), Standardabweichungen (SD) und die Stichprobengröße (n).

Tab. 40: Vergleich EG und KG über drei Messzeitpunkte im Hinblick auf das Merkmal ‚Einstellung'

		M	SD	n
t1	Kontrollgruppe	4.33	.51	89
	Experimentalgruppe	4.25	.59	93
t2	Kontrollgruppe	4.01	.59	89
	Experimentalgruppe	4.48	.511	93
t3	Kontrollgruppe	3.68	.42	89
	Experimentalgruppe	4.61	.211	93

Fazit zur Hypothese H3ab

Die Lernenden der EG, die die präventive Maßnahme absolvierten, veränderten sowohl kurzfristig als auch längerfristig ihre Einstellung stärker als die Lernenden der KG, die nur Cyberangriffe präsentiert bekamen. Somit ist die Nullhypothese keines Unterschiedes abzulehnen und H3 zu akzeptieren.

Wirkung der Maßnahme auf die Urteilsfähigkeit (H4)

Die Untersuchung der Wirksamkeit der Maßnahme im Hinblick auf die Urteilsfähigkeit der Lernenden konnte nicht vorgenommen werden, da das Erhebungsinstrument die Urteilsfähigkeit nicht abbildet. Dies verwundert jedoch nicht, da mit den in den drei Pilotstudien erhobenen Daten die Urteilsfähigkeit ebenso wenig operationalisiert werden konnte.

Wirkung der Maßnahme auf die Kontrollüberzeugung (H5)

Es wurde angenommen, dass die Teilnehmenden der Experimentalgruppe ihre Kontrollüberzeugung stärker verändern würden als die an der Kontrollgruppe Teilnehmenden (H5). Diese Annahme wurde anhand einer zweifaktoriellen Varianzanalyse mit dem Zwischensubjektfaktor ‚Gruppenzugehörigkeit' (zur EG oder KG) und dem Messwiederholungsfaktor ‚Messzeitpunkt' mit der abhängigen Variable ‚Kontrollüberzeugung' über zwei Messzeitpunkte (H5a) und über drei Messzeitpunkte (H5b) statistisch überprüft.

Die Untersuchung der Varianzhomogenität (Prä-Post-Vergleich) anhand des Levene-Tests zeigt in der EG und der KG im Vergleich zwischen t1 ($F(1,216) = 6.564$, $p < .001$) und t2 ($F(1,216) = .404$, $p = .526$) ein signifikantes Ergebnis. Eine Varianzhomogenität ist somit nur für t2 gegeben. Auch hier wurde die ANOVA im Prä-Post-Follow-up-Vergleich durchgeführt, als Zusatzargument voneinander nur gering unterschiedlicher Varianzen (siehe Tabelle 40).

Das Ergebnis der ANOVA im Prä-Post-Vergleich zeigt einen signifikanten Haupteffekt für die Gruppenzugehörigkeit ($F(1,216) = 6.326$, $p = .013$, $\eta_p^2 = .028$): Die Kontrollüberzeugung der Teilnehmenden in der Experimentalgruppe unterscheidet sich deutlich von derjenigen der Teilnehmenden in der Kontrollgruppe. Signifikant ist ebenfalls der Messwiederholungsfaktor, da $F(1,216) = 40.727$, $p = .00$, $\eta_p^2 = .159$. Das bedeutet, dass sich die Kontrollüberzeugung der ProbandInnen (über beide Gruppen hinweg) signifikant über die Zeit verändert hat.

Die Wechselwirkung zwischen den beiden Faktoren zeigt einen signifikanten Einfluss auf die Kontrollüberzeugung der Teilnehmenden, denn $F(1,216) = 13.632$, $p < .001$, $\eta_p^2 = .005$. Die Veränderung der Kontrollüberzeugung der Teilnehmenden über die Zeit verlief dementsprechend in der EG und der KG unterschiedlich. In der Abbildung 50 wird ersichtlich, dass die KG von der präventiven Maßnahme stärker profitierte als die EG.

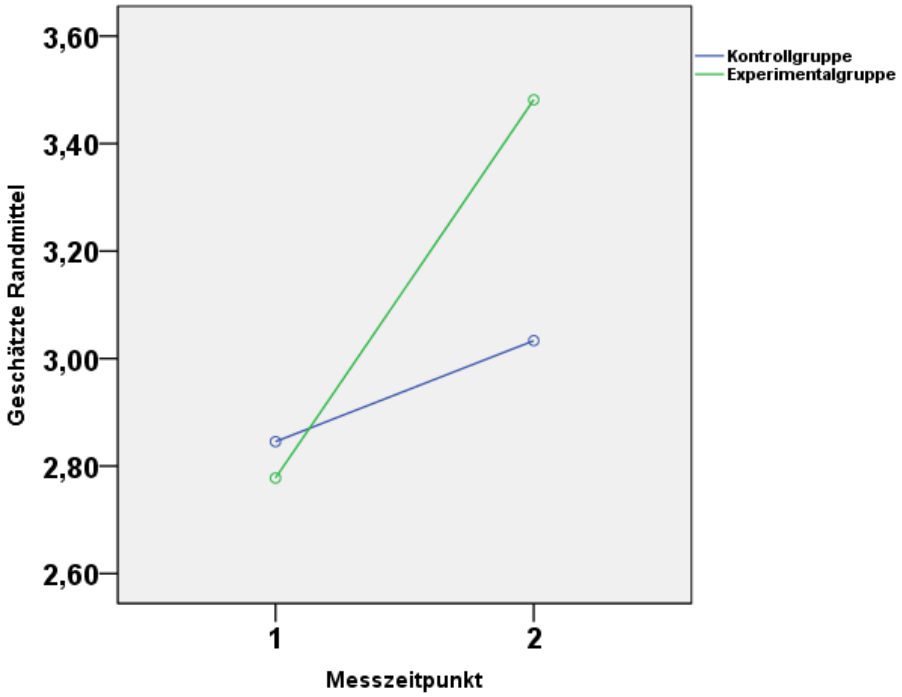


Abb. 50: Mittelwertvergleich der Kontrollüberzeugung der Teilnehmenden (EK/KG) zu t1 und t2

Nachfolgend sind die Ergebnisse in der Tabelle 41dargestellt als Mittelwerte (M), Standardabweichungen (SD) und Stichprobengröße (n).

Tab. 41: Vergleich EG und KG über zwei Messzeitpunkte im Hinblick auf das Merkmal ‚Kontrollüberzeugung'

		M	SD	n
t1	Kontrollgruppe	2.84	.67	110
	Experimentalgruppe	2.77	.83	108
t2	Kontrollgruppe	3.03	.74	110
	Experimentalgruppe	3.48	.76	108

Eine weitere Untersuchung erfolgte über alle Messzeitpunkte hinweg.

Die Untersuchung der Sphärizität anhand des Mauchly-Tests zeigt kein signifikantes Ergebnis, da $\chi^2(2) = 10.511$, $p = .005$. Die Sphärizität ist somit für H5 gegeben. Die Untersuchung der Varianzhomogenität anhand des Levene-Tests zeigt in der EG und KG zu t3 ein signifikantes Ergebnis ($F(1,180) = 6.181$, $p = .014$), nicht signifikant ist es aber für t2 ($F(1,180) = .772$, $p = 0.381$) und t3 ($F(1,180) = 1.793$, $p = 0.182$). Eine Varianzhomogenität ist somit nicht gegeben, was jedoch aufgrund der gleichen Gruppengröße vernachlässigt werden kann (siehe Tabelle 41).

Das Ergebnis der ANOVA im Prä-Post-Follow-up-Vergleich zeigt einen signifikanten Haupteffekt für die Gruppenzugehörigkeit, da $F(1,180) = 4.764$, $p = .006$, $\eta_p^2 = .041$. Signifikant ist auch der Messwiederholungsfaktor ($F(2,360) = 18.493$, $p < .001$, $\eta_p^2 = .93$),

was bedeutet, dass sich die Kontrollüberzeugung der ProbandInnen (über beide Gruppen hinweg) signifikant über die Zeit geändert hat. Die Wechselwirkung zwischen den beiden Faktoren hat ebenfalls einen signifikanten Einfluss auf die Kontrollüberzeugung der Teilnehmenden, da $F(2,360) = .46.829$, $p = .00$, $\eta_p^2 = .20$. Die Veränderung der Kontrollüberzeugung über die Zeit verlief dementsprechend in Abhängigkeit von der Gruppenzugehörigkeit zur EG beziehungsweise zur KG unterschiedlich. Bemerkenswert ist der unterschiedliche Verlauf in der EG und der KG zwischen den Messzeitpunkten t2 und t3, da die Kontrollüberzeugung der Teilnehmenden in der EG in diesem Zeitraum stark absank (siehe Abbildung 51).

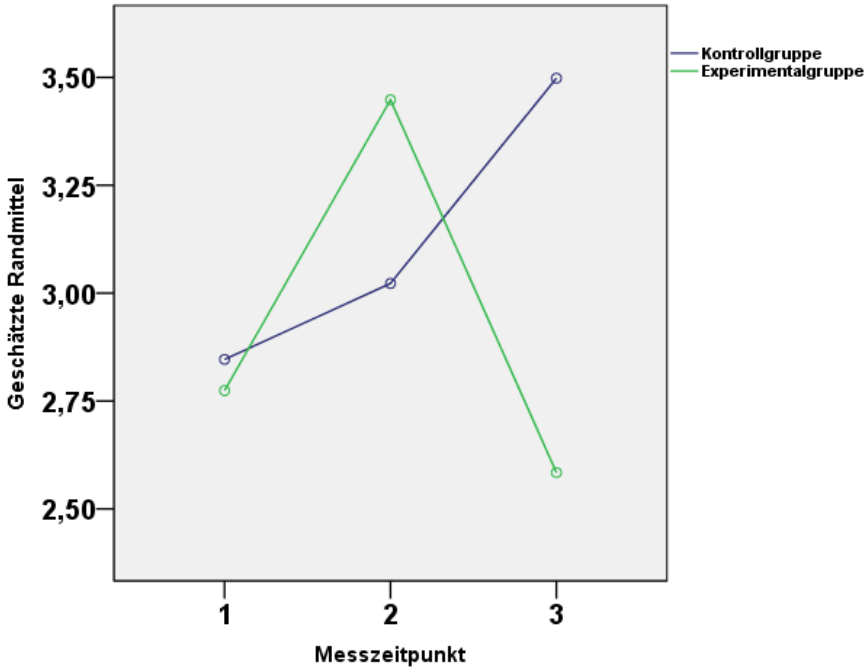


Abb. 51: Mittelwertvergleich der Kontrollüberzeugung der Teilnehmenden (EK/KG) zu t1, t2 und t3

Nachfolgend sind die Ergebnisse in der Tabelle 42 dargestellt als Mittelwerte (M), Standardabweichungen (SD) und Stichprobengröße (n).

Tab. 42: Vergleich EG und KG über drei Messzeitpunkte im Hinblick auf das Merkmal ‚Kontrollüberzeugung'

		M	SD	n
t1	Kontrollgruppe	2.84	.70	89
	Experimentalgruppe	2.77	.80	93
t2	Kontrollgruppe	3.02	.75	89
	Experimentalgruppe	3.44	.77	93
t3	Kontrollgruppe	3.49	.67	89
	Experimentalgruppe	2.58	.49	93

Fazit zur Hypothese H5ab

Die Lernenden der EG, die die präventive Maßnahme absolvierten, veränderten kurzfristig, jedoch nicht längerfristig ihre Kontrollüberzeugung stärker als die Lernenden der KG. Die Nullhypothese muss somit abgelehnt werden. Der Unterschied in der Veränderung der Kontrollüberzeugung zwischen den Lernenden der EG gegenüber denjenigen, die nur Cyberangriffe präsentiert bekamen (KG), widerspricht den Erwartungen (vgl. Kapitel 2.3.4 und 2.3.5) und bedarf einer weiteren Interpretation (siehe hierzu Kapitel 7.1.3). H5 wird abgelehnt.

Wirkung der Maßnahme auf die Selbstwirksamkeit im Kontext von IT-Sicherheit (H6)

In Anlehnung an lerntheoretische Konzepte zum Thema Selbstwirksamkeit wurde angenommen, dass die Lernenden der Experimentalgruppe ihre Selbstwirksamkeit im Kontext von IT-Sicherheit stärker verändern würden als die Lernenden der Kontrollgruppe (H6). Diese Annahme wurde anhand einer zweifaktoriellen Varianzanalyse mit dem Zwischensubjektfaktor ‚Gruppenzugehörigkeit' (zur EG oder KG) und dem Messwiederholungsfaktor ‚Messzeitpunkt' mit der abhängigen Variable ‚Einstellung' über zwei Messzeitpunkte (H6a) und über drei Messzeitpunkte (H6b) statistisch überprüft.

Die Untersuchung der Varianzhomogenität (Prä-Post-Vergleich) durch den Levene-Test ergab in der EG und der KG für t1 ($F(1,216) = 6.564$, $p = .011$) signifikante und für t2 ($F(1,216) = .404$, $p = .526$) nicht signifikante Ergebnisse. Eine Varianzhomogenität ist somit nicht gegeben. Da die Gruppengrößen annähernd gleich sind (siehe Tabelle 43), erfolgte jedoch trotz dieses Ergebnisses (wie in den anderen Untersuchungen) die Weiterführung der Analyse.

Das Ergebnis der ANOVA im Prä-Post-Vergleich zeigt einen signifikanten Haupteffekt für die Gruppenzugehörigkeit, da $F(1,216) = 6.326$, $p = .013$, $\eta_p^2 = .028$. Die Selbstwirksamkeit im Kontext von IT-Sicherheit der Teilnehmenden in der Experimentalgruppe unterscheidet sich also statistisch signifikant von derjenigen der Teilnehmenden in der Kontrollgruppe.

Ebenfalls signifikant ist der Messwiederholungsfaktor ($F(1,216) = 40.722$, $p < .001$, $\eta_p^2 = 0.159$), was bedeutet, dass sich die Selbstwirksamkeit im Kontext von IT-Sicherheit der ProbandInnen (über beide Gruppen hinweg) signifikant über die Zeit geändert hat. Die Wechselwirkung zwischen den beiden Faktoren hat ebenfalls einen signifikanten Einfluss auf die Selbstwirksamkeit im Kontext von IT-Sicherheit der Teilnehmenden ($F(1,216) = 13.632$, $p < .001$, $\eta_p^2 = .059$), woraus geschlussfolgert werden kann, dass die Veränderung der Selbstwirksamkeit im Kontext von IT-Sicherheit über die Zeit in

Abhängigkeit von der Gruppenzugehörigkeit zur EG beziehungsweise KG unterschiedlich verlief (siehe Abbildung 52).

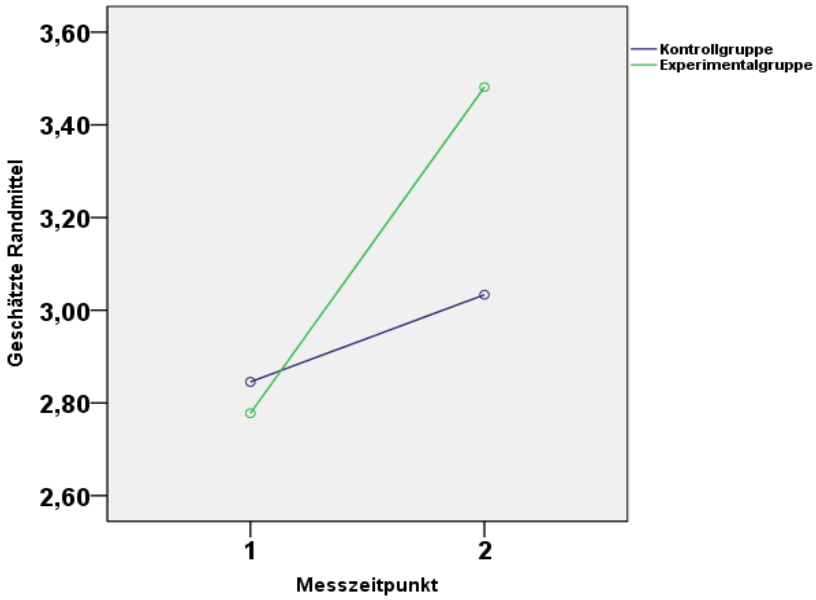


Abb. 52: Mittelwertvergleich der Selbstwirksamkeit im Kontext von IT-Sicherheit (EK/KG) zu t1 und t2

Nachfolgend sind die Ergebnisse in der Tabelle 43 als Mittelwerte (M), Standardabweichungen (SD) und Stichprobengröße (n) dargestellt.

Tab. 43: Vergleich EG und KG über zwei Messzeitpunkte im Hinblick auf das Merkmal ‚Bewertung der Kontrollmöglichkeiten'

		M	SD	n
t1	Kontrollgruppe	2.74	.70	110
	Experimentalgruppe	2.60	.72	108
t2	Kontrollgruppe	3.12	.53	110
	Experimentalgruppe	3.45	.57	108

Eine weitere Untersuchung erfolgte über alle Messzeitpunkte t1, t2 und t3 hinweg.

Die Untersuchung der Sphärizität anhand des Mauchly-Tests zeigt ein signifikantes Ergebnis, da $\chi^2(2) = 13.800$, $p = .001$. Die Sphärizität ist somit für H5b nicht gegeben, sodass eine Greenhouse-Geisser-Korrektur erforderlich war. Die Untersuchung der Varianzhomogenität (Prä-Post-Follow-up-Vergleich) anhand des Levene-Tests zeigt folgende Werte in der EG und der KG zu den drei Messzeitpunkten: t1: $F(1,180) = .023$, $p = .879$, t2: $F(1,180) = 1.152$, $p = .287$ und t3: $F(1,180) = .004$, $p = 9.51$. Die Varianzhomogenität ist somit für t1, t2 und t3 gegeben.

Das Ergebnis der ANOVA im Prä-Post-Follow-up-Vergleich zeigt einen signifikanten Haupteffekt für die Gruppenzugehörigkeit ($F(1,180) = 50.920$, $p = .000$, $\eta_p^2 = .221$). Die

Selbstwirksamkeit im Kontext von IT-Sicherheit der Teilnehmenden in der Experimentalgruppe unterscheidet sich also deutlich von derjenigen in der Kontrollgruppe.

Signifikant ist auch der Messwiederholungsfaktor ($F(2,360) = 79.182$, $p = .000$, $\eta_p^2 = .306$) mit der Greenhouse-Geisser-Korrektur, was bedeutet, dass sich die Selbstwirksamkeit der ProbandInnen (über beide Gruppen hinweg) signifikant über die Zeit geändert hat. Die Wechselwirkung zwischen den beiden Faktoren hat ebenfalls einen signifikanten Einfluss auf die Selbstwirksamkeit der Teilnehmenden, da $F(2,360) = 66.540$, $p = .000$, $\eta_p^2 = .27$.

Die folgende Abbildung 53 zeigt die unterschiedliche Entwicklung der Bewertung der Kontrollmöglichkeiten. Auffällig ist der Verlauf der Selbstwirksamkeit der Teilnehmenden der Kontrollgruppe zum Thema „Bewertung von Kontrollmöglichkeiten“, da dieser Wert unter die Anfangswerte sinkt. Demgegenüber zeigt der Verlauf bei der Experimentalgruppe eine Verbesserung gegenüber den Anfangswerten, und dies auch zum Messpunkt t3.

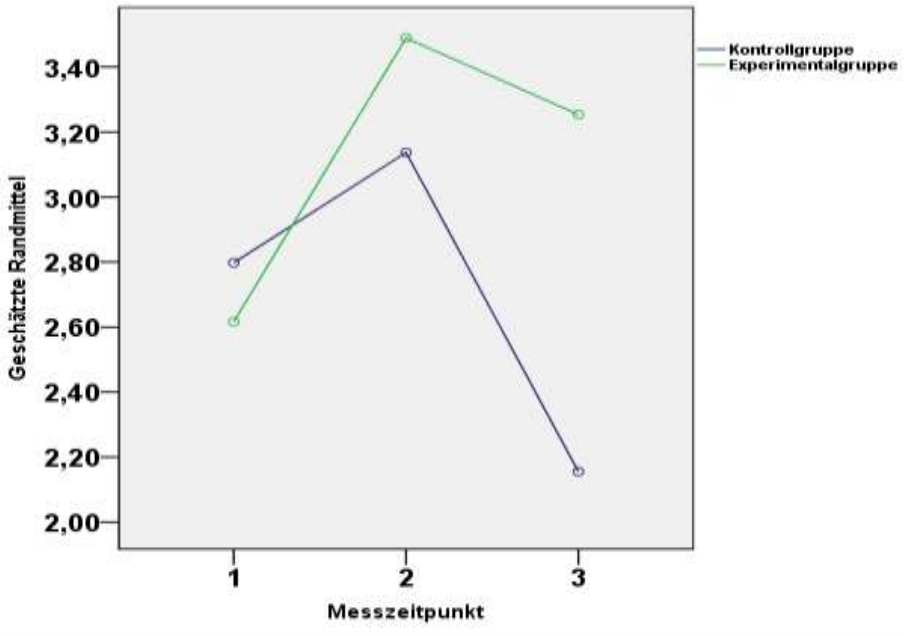


Abb. 53: Mittelwertvergleich der Selbstwirksamkeit im Kontext von IT-Sicherheit (EK/KG) zu t1, t2 und t3

Nachfolgend sind die Ergebnisse in der Tabelle 44 dargestellt als Mittelwerte (M), Standardabweichungen (SD) und Stichprobengröße (n).

Tab. 44: Vergleich EG und KG über drei Messzeitpunkte im Hinblick auf das Merkmal ‚Bewertung der Kontrollmöglichkeiten'

		M	SD	n
t1	Kontrollgruppe	2.797	.717	89
	Experimentalgruppe	2.616	.738	93
t2	Kontrollgruppe	3.137	.521	89
	Experimentalgruppe	3.489	.587	93
t3	Kontrollgruppe	2.155	.446	89
	Experimentalgruppe	3.253	.457	93

Fazit zur Hypothese H6ab

Die Lernenden der EG, die die präventive Maßnahme absolvierten, veränderten sowohl kurzfristig als auch längerfristig ihre Selbstwirksamkeit im Kontext von IT-Sicherheit stärker als die Lernenden der KG, die nur Cyberangriffe präsentiert bekamen. Somit kann die Hypothese H6 bekräftigt werden.

6.4.2 Moderatoren der Wirksamkeit der Maßnahme

In diesem Unterkapitel werden potentielle Moderatoren, die die Wirksamkeit der präventiven Maßnahme beeinflussen können, überprüft. Dabei werden die Ergebnisse der statistischen Analysen zu den Hypothesen H7 bis H10 umfassend dargestellt.

Alter als Moderator der Wirksamkeit der Maßnahme (H7)

Es wurde angenommen, dass die Wirksamkeit der Maßnahme (Prä-Post) bei den Lernenden der Experimentalgruppe und der Kontrollgruppe durch das Alter moderiert wird.

Moderatorvariablen, hier als W bezeichnet, verändern den Zusammenhang zwischen einer unabhängigen Variablen, die meist als X-Variable bezeichnet wird, und einer abhängigen Variablen, die meist als Y-Variable bezeichnet wird. Die statistische Überprüfung einer Moderation erfolgt durch die Berechnung einer multiplen linearen Regression, wobei die unabhängige Variable, die Moderatorvariable sowie das Produkt aus diesen beiden Variablen als Prädiktoren für die abhängige Variable einbezogen werden (siehe Abbildung 42). Die Moderatorvariable ist im vorliegenden Fall das Alter der ProbandInnen, das in Generationskohorten eingeteilt ist. Die unabhängige Variable ist die Teilnahme und die abhängige Variable ist die Wirksamkeit der Präventionsmaßnahme, operationalisiert als die Veränderung der Einstellung, des Verhaltens sowie der Selbstwirksamkeit der ProbandInnen zwischen den Erhebungszeitpunkten des Prä- und des Post-Tests. Hierfür wird für jede der abhängigen Variablen der Wert zum zweiten und der Wert zum ersten Messzeitpunkt berechnet, und die Differenz der Messwerte (Post –

Prä) wird anschließend als abhängige Variable verwendet. Diese Analyse erfolgte mithilfe des Process-Makros in der Version 3.4 (Hayes 2018) in SPSS. Separate Moderatoranalysen wurden jeweils für jede Kombination aus Moderatoren und abhängigen Variablen durchgeführt.

Vor Beginn der Analyse mussten die Voraussetzungen einer multiplen linearen Regression überprüft werden, wobei etwaigen Verletzungen der Homoskedastizitätsvoraussetzung – ebenfalls durch Process – durch die Anforderung heteroskedastizitätsinvarianter Schätzer begegnet werden konnte. In der vorliegenden Analyse wurde Bootstrapping eingesetzt, die Daten wurden zentriert und der Schätzer HC3 wurde nach Huber-White gewählt.

Eine weitere Voraussetzung, um das Verfahren einsetzen zu können, war die Unabhängigkeit der Residuen. Hier konnte jedoch aufgrund des Studiendesigns und Rechenmodells davon ausgegangen werden, dass in allen nachfolgenden Moderatormodellen die Beobachtungen unkorreliert sind.

Die erste Analyse fokussiert die Frage, wie der Effekt der Teilnahme auf die Einstellung der ProbandInnen durch ihr Lebensalter moderiert wird. Die Voraussetzung der Linearität zwischen den metrischen Prädiktoren und dem Kriterium wurde anhand von Streudiagrammen überprüft und kann laut der Ergebnisse als erfüllt angesehen werden. Zur Überprüfung der Multikollinearität wurden die beiden Prädiktoren ‚Teilnahme' und ‚Alter' (zentriert) sowie der Prädikator ‚Produkt aus Alter (zentriert) und Teilnahme' miteinander korreliert. Wie in der nachfolgender Tabelle 45 dargestellt, ergaben die Analysen jedoch keine starken Zusammenhänge zwischen den unabhängigen Variablen, da Korrelationen bis .8 akzeptiert wurden (Gehrke 2019) und viel niedrige Werte vorhanden waren. Diese Prüfung war essenziell, damit Variablen nicht redundant zur Varianzaufklärung beitragen konnten.

Tab. 45: Prüfung auf Multikollinearität

		Alter	Geschlecht	Bildung
Alter	Pearson-Korrelation	1	-.122	-.111
	Sig. (2-seitig)		.071	.102
	n	218	218	218
Geschlecht	Pearson-Korrelation	-.122	1	-.183**
	Sig. (2-seitig)	.071		.007
	n	218	218	218
Bildung	Pearson-Korrelation	-.111	-.183**	1
	Sig. (2-seitig)	.102	.007	
	n	218	218	218

**. Korrelation ist bei Niveau 0,01 signifikant (zweiseitig).

Die Ergebnisse zeigen, dass keine Multikollinearität vorliegt. Damit waren die Voraussetzungen für die folgenden drei Analysen erfüllt. Korrelationen der Residuen waren ebenfalls nicht vorhanden, wie aus der Tabelle 46 hervorgeht.

Tab. 46: Prüfung auf Autokorrelation Alter

Y-Variable	Durbin-Watson
Einstellung	1.96
Kontrollüberzeugung	2.00
Bewertung der Kontrollmöglichkeiten	2.01

Die Ergebnisse für die EG zeigen mit $R^2 = .15.$, $p < .001$, dass das Gesamtmodell signifikant ist und somit mit 15 % die Varianz der abhängigen Variable erklärt. Der Interaktionsterm als Prädiktor für die Wirkungsänderung vom ersten zum zweiten Messzeitpunkt zeigt sich jedoch nicht signifikant ($p = .92$). Und auch die Hinzunahme des Interaktionsterms als Prädiktor im Regressionsmodell als zusätzlich erklärte Varianz ist nicht signifikant, da R^2-Change = .00, $p = .92$. Somit war das Verfahren abzubrechen, da es keine signifikante Moderation in der EG gibt.

Die Ergebnisse für die KG zeigen mit $R^2 = .03.$, $p = .25$, dass das Gesamtmodell nicht signifikant ist und somit keinen Erklärungsbeitrag leistet. Der Interaktionsterm als Prädiktor für die Wirkungsänderung vom ersten zum zweiten Messzeitpunkt zeigt sich auch nicht signifikant, da $p = .12$. Und die Hinzunahme des Interaktionsterms als Prädiktor im Regressionsmodell als zusätzliche erklärende Variable ist ebenfalls nicht signifikant, da R^2-Change = .00, $p = .12$. Somit war das Verfahren auch hier abzubrechen, da es keine signifikante Moderation in der KG gibt.

Zusammenfassend ist festzuhalten, dass der Moderator Alter die Einstellungsänderung der ProbandInnen in der EG und KG durch die Teilnahme im Prä-Post-Vergleich nicht beeinflusst.

Die zweite Analyse bezieht sich auf die Moderation des Effektes der Teilnahme auf die Kontrollüberzeugung der ProbandInnen durch das Lebensalter. Da die Voraussetzung der Linearität erfüllt war und die Streudiagramme zwischen den metrischen Prädiktoren und dem Kriterium keine nichtlinearen Tendenzen zeigten, waren alle Voraussetzungen für die lineare Regressionsanalyse erfüllt.

Die Ergebnisse für die EG zeigen, dass das Gesamtmodell 13 % der Varianz der abhängigen Variable erklärt und auch hoch signifikant ist, denn $R^2 = .13$, $p = .00$. Der Interaktionsterm als Prädiktor für die Wirkungsänderung vom ersten zum zweiten Messzeitpunkt zeigt sich mit $p = .00$ gleichfalls signifikant. Und auch die Hinzunahme des Interaktionsterms als Prädiktor im Regressionsmodell als zusätzliche erklärende Variable ist signifikant, da $p = .00$. mit einer Varianzabdeckung von 6 %, R^2-Change = .06.

Werden die Daten dezentriert und einer Johnson-Neyman-Prozedur unterzogen, zeigt sich, dass die 22-33-Jährigen und auch die 60-67-Jährigen signifikant durch das Lebensalter im Prä-Post-Vergleich moderiert werden.

Tab. 47: Kontrollüberzeugung der Teilnehmenden der EG im Prä-Post-Vergleich

Lebensalter	Effect	se(HC3)	t	p	LLCI	ULCI	TG
22	1.28	0.55	2.35	***0.02****	0.20	2.36	I
24	1.18	0.51	2.31	***0.02****	0.17	2.18	I
27	1.07	0.47	2.28	***0.03****	0.14	2.01	I
29	0.97	0.44	2.23	***0.03****	0.11	1.84	I
31	0.87	0.40	2.17	***0.03****	0.08	1.66	I
33	0.77	0.37	2.10	***0.04****	0.04	1.49	I
36	0.66	0.33	2.01	0.05	0.01	1.32	I
36	0.64	0.32	1.98	0.05	0.00	1.28	I
38	0.56	0.30	1.89	0.06	-0.03	1.15	I
40	0.46	0.27	1.73	0.09	-0.07	0.99	C
42	0.36	0.24	1.51	0.13	-0.11	0.83	C
45	0.26	0.21	1.22	0.23	-0.16	0.67	C
47	0.15	0.19	0.82	0.41	-0.22	0.52	C
49	0.05	0.17	0.30	0.77	-0.29	0.39	C
51	-0.05	0.16	-0.32	0.75	-0.37	0.27	C
54	-0.15	0.16	-0.95	0.35	-0.47	0.17	C
56	-0.26	0.17	-1.50	0.14	-0.59	0.08	G
58	-0.36	0.19	-1.91	0.06	-0.73	0.01	G
58	-0.38	0.19	-1.98	0.05	-0.76	0.00	G
60	-0.46	0.21	-2.19	***0.03****	-0.88	-0.04	G
63	-0.56	0.24	-2.38	***0.02****	-1.03	-0.09	G
65	-0.66	0.27	-2.50	***0.01****	-1.19	-0.14	G
67	-0.77	0.30	-2.58	***0.01****	-1.36	-0.18	G

*Anmerkungen: * < .05, ** < .01*
LL = lower level
UL = upper level
CI = Confidenzintervall
TG = Technikgeneration gemäß Tabelle 13
I = Internetgeneration
C = Computergeneration
G = Generation der zunehmenden Haushaltstechnik

Die Ergebnisse für die EG zeigen, dass das Gesamtmodell keine Varianz erklärt und nicht signifikant ist, da $R^2 = .01$, $p = .75$. Auch der Interaktionsterm als Prädiktor für die Wirkungsänderung vom ersten zum zweiten Messzeitpunkt zeigt sich mit $p = .27$ nicht signifikant. Und das Gleiche gilt für die Hinzunahme des Interaktionsterms als Prädiktor im Regressionsmodell als zusätzlich erklärte Varianz, die mit R^2-Change = .00, $p = .82$ ebenfalls nicht signifikant ist.

Festzuhalten ist dementsprechend, dass der Moderator Alter die Kontrollüberzeugung der ProbandInnen in der EG, nicht jedoch der ProbandInnen in der KG beeinflusst.

Die dritte Analyse bezieht sich auf die Moderation des Effektes der Teilnahme auf die Selbstwirksamkeit im Kontext von IT-Sicherheit der ProbandInnen durch das Lebensalter. Die Voraussetzung der Linearität war erfüllt, denn Streudiagramme zwischen den metrischen Prädiktoren und dem Kriterium zeigten keine nichtlinearen Tendenzen.

Die Ergebnisse in der EG zeigen, dass das Gesamtmodell 21 % der Varianz der abhängigen Variable erklärt und signifikant ist, denn $R^2 = .21$, $p < .001$. Der Interaktionsterm als Prädiktor für die Wirkungsänderung vom ersten zum zweiten Messzeitpunkt zeigt sich mit $p = .88$ hingegen nicht signifikant. Und auch die Hinzunahme des Interaktionsterms als Prädiktor im Regressionsmodell als zusätzliche erklärende Variable ist nicht signifikant, da R^2-Change = .000, $p = .88$. Somit war das Verfahren abzubrechen, da es keine signifikante Moderation gibt.

Die Ergebnisse in der KG zeigen, dass das Gesamtmodell nicht signifikant ist, da $R^2 = .06$, $p = .05$. Auch der Interaktionsterm als Prädiktor für die Wirkungsänderung vom ersten zum zweiten Messzeitpunkt zeigt sich mit $p = .06$ nicht signifikant. Das Gleiche gilt für die Hinzunahme des Interaktionsterms als Prädiktor im Regressionsmodell als zusätzliche erklärende Variable, denn R^2-Change = .02, $p = .06$. Somit war das Verfahren abzubrechen, das es keine signifikante Moderation gibt.

Die Analyse zeigt dementsprechend, dass der Moderator Alter die Selbstwirksamkeit im Kontext von IT-Sicherheit der ProbandInnen sowohl in der KG als auch in der EG nicht beeinflusst.

Zusammenfassend sind die Ergebnisse in den Tabellen 48 und 49 dargestellt. Dabei stellt die Tabelle 48 die Ergebnisse für die KG vor.

Tab. 48: Moderation der AV durch das Lebensalter in der KG im Prä-Post-Vergleich

abhängige Variable				95 % CI			
	Prädiktor	β	se (HC3)	LL	UL	R^2	*P*
Einstellungs-änderung (n = 110)	Teilnahme	-.12	.13	-.39	-.14	.03	.36
	Alter	-.00	.00	-.01	.01		
	Teilnahme*Alter	-.02	.01	-.05	.00		.12
Kontrollüber-zeugung (n = 110)	Teilnahme	-.06	.16	-.38	.26	.01	.71
	Alter	-.01	.01	-.03	.00		
	Teilnahme*Alter	.00	.01	-.03	.04		.82
Selbstwirk-samkeit im Kontext von IT-Sicherheit (n = 110)	Teilnahme	-.10	.08	-.1.2	.06	.02	.05
	Alter	.01	.00	1.9	.01		
	Teilnahme*Alter	-.01	.01	-.1.8	.00		.06

Anmerkungen: * < .05, ** < .01
LL = lower level
UL = upper level
CI = Confidenzintervall

Eine Darstellung der Ergebnisse für die EG erfolgt in der Tabelle 49.

Tab. 49: Moderation der AV durch das Lebensalter in der EG im Prä-Post-Vergleich

abhängige Variable				95 % CI			
	Prädiktor	β	se (HC3)	LL	UL	R^2	*p*
Einstellungs-änderung (n = 108)	Teilnahme	-.37	.10	-.58	-.13	.15	.00**
	Alter	.00	.00	-.00	.01		
	Teilnahme*Alter	.00	.00	-.01	.01		.92
Kontrollüber-zeugung (n = 108)	Teilnahme	-.07	.16	-.39	.24	.13	.0*
	Alter	.01	.00	-.00	.02		
	Teilnahme*Alter	-.04	.01	-.07	-.01		.00*
Selbstwirk-samkeit im Kontext von IT-Sicherheit (n = 108)	Teilnahme	-.33	.12	-.56	-.08	.02	.00**
	Alter	.01	.00	.01	.03		
	Teilnahme*Alter	-.00	.01	-.02	-.01		.09

Anmerkungen: *< .05, **< .01
LL = lower level
UL = upper level
CI = Confidenzintervall

Nachfolgend werden die Analysen von t1 zu t3 dargelegt.

Die Ergebnisse für die Einstellung in der EG zeigen mit $R^2 = 37.$, $p < .001$, dass das Gesamtmodell signifikant ist und somit 37 % der Varianz der abhängigen Variablen erklärt. Der Interaktionsterm als Prädiktor für die Wirkungsänderung vom ersten zum dritten Messzeitpunkt zeigt ebenfalls eine Signifikanz von $p = .01$. Und auch die Hinzunahme des Interaktionsterms als Prädiktor im Regressionsmodell als zusätzliche erklärende Variable ist signifikant, da R^2-Change = .02, $p = .01$. Werden die Daten dezentriert und einer Johnson-Neyman-Prozedur unterzogen, zeigt sich eine Signifikanz ab dem Lebensalter von über 39 Jahren (siehe Tabelle 50).

Tab. 50: Einstellungsänderung zum Lebensalter der EG zum dritten Messzeitpunkt

Lebensalter	Effect	Se (HC3)	t	p	LLCI	ULCI	TG
22	0.03	0.23	0.11	0.91	-0.43	0.48	I
24	-0.01	0.22	-0.06	0.96	-0.44	0.42	I
27	-0.05	0.20	-0.25	0.81	-0.45	0.35	I
29	-0.09	0.19	-0.46	0.64	-0.46	0.29	I
31	-0.12	0.17	-0.71	0.48	-0.47	0.22	I
33	-0.16	0.16	-1.01	0.32	-0.48	0.16	I
36	-0.20	0.15	-1.35	0.18	-0.50	0.09	I
38	-0.24	0.14	-1.75	0.08	-0.51	0.03	C
39	-0.26	0.13	-1.99	0.05	-0.51	0.00	C
40	-0.28	0.12	-2.22	**0.03***	-0.52	-0.03	C
42	-0.31	0.11	-2.78	**0.01***	-0.54	-0.09	C
45	-0.35	0.10	-3.43	**0.00****	-0.55	-0.15	C
47	-0.39	0.09	-4.17	**0.00****	-0.57	-0.20	C
49	-0.43	0.09	-4.96	**0.00****	-0.60	-0.26	C
51	-0.46	0.08	-5.74	**0.00****	-0.62	-0.30	C
54	-0.50	0.08	-6.41	**0.00****	-0.66	-0.35	C
56	-0.54	0.08	-6.86	**0.00****	-0.69	-0.38	G
58	-0.58	0.08	-7.05	**0.00****	-0.74	-0.41	G
60	-0.61	0.09	-7.03	**0.00****	-0.79	-0.44	G
63	-0.65	0.10	-6.85	**0.00****	-0.84	-0.46	G
65	-0.69	0.10	-6.59	**0.00****	-0.90	-0.48	G
67	-0.73	0.12	-6.31	**0.00****	-0.96	-0.50	G

*Anmerkungen: * < .05, ** < .01*
LL = lower level
UL = upper level
CI = Confidenzintervall
t = Teststatistik für diesen Effekt
TG = Technikgeneration gemäß Tabelle 13
I = Internetgeneration
C = Computergeneration
G = Generation der zunehmenden Haushaltstechnik

Die Ergebnisse für die Einstellung in der KG zeigen mit $R^2 = 26.$, $p < .001$, dass das Gesamtmodell signifikant ist und somit mit 26 % die Varianz erklärt. Der Interaktionsterm als Prädiktor für die Wirkungsänderung vom ersten zum dritten Messzeitpunkt zeigt ebenfalls eine Signifikanz von $p = .02$. Und auch die Hinzunahme des Interaktionsterms als Prädiktor im Regressionsmodell als zusätzlich erklärte Varianz ist signifikant, da R^2-Change = .07, $p = .02$. Werden die Daten dezentriert und einer Johnson-Neyman-

Prozedur unterzogen, zeigt sich eine Signifikanz ab dem Lebensalter von über 41 Jahren (siehe Tabelle 51).

Tab. 51: Einstellungsänderung zum Lebensalter der KG zum dritten Messzeitpunkt

Lebensalter	Effect	Se (HC3)	t	p	LLCI	ULCI	G
22	0.56	0.45	1.24	0.22	-0.34	1.46	I
24	0.47	0.41	1.14	0.26	-0.35	1.29	I
26	0.38	0.38	1.01	0.31	-0.37	1.13	I
28	0.29	0.34	0.86	0.39	-0.38	0.96	I
30	0.20	0.30	0.66	0.51	-0.40	0.79	I
32	0.10	0.26	0.40	0.69	-0.42	0.63	I
34	0.01	0.23	0.06	0.96	-0.44	0.46	I
36	-0.08	0.19	-0.41	0.69	-0.46	0.31	I
38	-0.17	0.16	-1.04	0.30	-0.50	0.16	I
40	-0.26	0.14	-1.87	0.07	-0.54	0.02	C
40	-0.27	0.14	-1.99	0.05	-0.55	0.00	C
42	-0.35	0.13	-2.81	**0.01***	-0.60	-0.10	C
44	-0.45	0.12	-3.61	**0.00****	-0.69	-0.20	C
46	-0.54	0.13	-4.00	**0.00****	-0.80	-0.27	C
48	-0.63	0.16	-4.05	**0.00****	-0.94	-0.32	C
50	-0.72	0.18	-3.94	**0.00****	-1.09	-0.36	C
52	-0.81	0.22	-3.78	**0.00****	-1.24	-0.39	C
54	-0.90	0.25	-3.62	**0.00****	-1.40	-0.41	C
56	-1.00	0.29	-3.48	**0.00****	-1.57	-0.43	G
58	-1.09	0.32	-3.36	**0.00****	-1.73	-0.45	G
60	-1.18	0.36	-3.26	**0.00****	-1.90	-0.46	G
62	-1.27	0.40	-3.18	**0.00****	-2.07	-0.48	G

Anmerkungen: * < .05, ** < .01
LL = lower level
UL = upper level
CI = Confidenzintervall
t = Teststatistik für diesen Effekt
TG = Technikgeneration gemäß Tabelle 13
I = Internetgeneration
C = Computergeneration
G = Generation der zunehmenden Haushaltstechnik

Die zweite Analyse bezieht sich auf die Moderation des Effektes der Teilnahme auf die Kontrollüberzeugung der ProbandInnen durch das Lebensalter zum dritten Messzeitpunkt.

Die Ergebnisse in der EG zeigen, dass das Gesamtmodell keine Varianz erklärt und nicht signifikant ist, denn $R^2 = .06$, $p = .10$. Und auch der Interaktionsterm als Prädiktor für die Wirkungsänderung vom ersten zum dritten Messzeitpunkt zeigt sich mit $p = .18$ nicht signifikant. Die Hinzunahme des Interaktionsterms als Prädiktor im Regressionsmodell als zusätzliche erklärende Variable ist ebenfalls nicht signifikant, da R^2-Change $= .02$, $p = .18$.

Die Ergebnisse in der KG zeigen, dass das Gesamtmodell eine Varianzaufklärung leisten kann und signifikant ist, denn $R^2 = .12$, $p = .01$. Der Interaktionsterm als Prädiktor für die Wirkungsänderung vom ersten zum dritten Messzeitpunkt zeigt sich mit $p = .06$

allerdings nicht signifikant. Und auch die Hinzunahme des Interaktionsterms als Prädiktor im Regressionsmodell als zusätzlich erklärte Varianz ist nicht signifikant, da R^2-Change = .04, p = .06.

Die dritte Analyse bezieht sich auf die Moderation des Effektes der Teilnahme auf die Selbstwirksamkeit im Kontext von IT-Sicherheit der ProbandInnen durch das Lebensalter zum dritten Messzeitpunkt.

Die Ergebnisse in der EG zeigen, dass das Gesamtmodell eine hohe Varianz mit 35 % erklären kann und hoch signifikant ist, denn R^2 = .35, p < .001. Der Interaktionsterm als Prädiktor für die Wirkungsänderung vom ersten zum dritten Messzeitpunkt zeigt sich jedoch mit p = .15 nicht signifikant. Und auch die Hinzunahme des Interaktionsterms als Prädiktor im Regressionsmodell als zusätzliche erklärende Variable ist nicht signifikant, da R^2-Change = .01, p = .15.

Die Ergebnisse in der KG zeigen, dass das Gesamtmodell einen hohe Varianzanteil mit 20 % erklären kann und hoch signifikant ist, denn R^2 = .20, p < .001. Der Interaktionsterm als Prädiktor für die Wirkungsänderung vom ersten zum dritten Messzeitpunkt zeigt sich jedoch mit p = .25 nicht signifikant. Und auch die Hinzunahme des Interaktionsterms als Prädiktor im Regressionsmodell als zusätzliche erklärende Variable ist nicht signifikant (R^2-Change = .01, p = .25).

Zusammenfassend sind die Ergebnisse in den Tabellen 52 und 53 dargestellt.

Tab. 52: Moderation der AV durch das Lebensalter in der EG im Prä-Follow-up-Vergleich

abhängige Variable				95 % CI			
	Prädiktor	β	se (HC3)	LL	UL	R^2	*p*
Einstellungs-änderung (n = 93)	Teilnahme	-.46	.08	-.62	-.31	.37	.00
	Alter	-.01	.00	-.01	-.00		
	Teilnahme*Alter	-.01	.00	-.03	-.00		.01
Kontrollüber-zeugung (n = 93)	Teilnahme	-.07	.14	-.35		.06	.10
	Alter	.00	.00	-.00			
	Teilnahme*Alter	-.01	.01	-.04			
Selbstwirk-samkeit im Kontext von IT-Sicherheit (n = 93)	Teilnahme	-.41	.11	-.64	-.19	.35	.00
	Alter	.01	.00	.00	.02		
	Teilnahme*Alter	-0.1	.01	-.03	.00		.15

Tab. 53: Moderation der AV durch das Lebensalter in der KG im Prä-Follow-up-Vergleich

abhängige Variable				95 % CI			
	Prädiktor	β	se (HC3)	LL	UL	R^2	*p*
Einstellungs-änderung (n = 89)	Teilnahme	1.5	.89	-.20	3.34	.26	.00
	Alter	.19	.08	.02	.36		
	Teilnahme*Alter	-.04	.02	-.08	-.00	.07	.02
Kontrollüber-zeugung (n = 89)	Teilnahme	.33	.16	.04	.64		.01
	Alter	-.01	.01	.25	.00		
	Teilnahme*Alter	.04	.02	.06	.08		
Selbstwirk-samkeit im Kontext von IT-Sicherheit (n = 89)	Teilnahme	-.35	.16	-.69	-.02	.20	00
	Alter	.03	.01	.01	.05		
	Teilnahme*Alter	-.02	.02	-.08	.02		

Fazit zur Hypothese H7

Die Analyse des Moderators Alter auf die Wirksamkeit der Maßnahme zeigt einen signifikanten Effekt in der EG und KG für die Veränderung der Einstellung von t1 zu t3. Speziell in der Computergeneration und der Generation der zunehmenden Haushaltstechnik konnte die Einstellung verändert werden. Eine Verbesserung der Kontrollüberzeugung, wie sie in dem Prä-Post-Vergleich ermittelt worden war, konnte zu t3 nicht mehr beobachtet werden. Somit kann die Hypothese H7 eines verstärkenden Einflusses des Alters bekräftigt werden.

Bildungsniveau als Moderator der Wirksamkeit der Maßnahme (H8)

Es wurde angenommen, dass die Wirksamkeit der Maßnahme (Prä-Post-Follow-up) der Lernenden der Experimentalgruppe und der Kontrollgruppe durch das Bildungsniveau (nachfolgend als Bildung bezeichnet) verstärkt wird. Die Moderatorvariable ist damit für die entsprechenden Berechnungen die Bildung der ProbandInnen, die unabhängige Variable ist die Teilnahme. Die abhängige Variable ist die Wirksamkeit der Präventionsmaßnahme, operationalisiert als die Veränderung der Einstellung, des Verhaltens sowie der Selbstwirksamkeit der ProbandInnen im Kontext von IT-Sicherheit.

Die erste Analyse bezieht sich auf die Moderation des Effektes der Teilnahme auf die Einstellung der ProbandInnen durch die Bildung im Prä-Post-Vergleich. Sie zeigt, dass die Voraussetzung der Linearität erfüllt ist. Die Streudiagramme zwischen den metrischen Prädiktoren und dem Kriterium zeigen keine nichtlinearen Tendenzen, und eine Überprüfung der Autokorrelation zeigt keine bedenkliche Korrelation der Residuen (siehe Tabelle 54).

Tab. 54: Prüfung auf Autokorrelation des Moderators ‚Bildung'

Y-Variable	Durbin-Watson
Einstellung	1.96
Kontrollüberzeugung	2.02
Selbstwirksamkeit im Kontext von IT-Sicherheit	2.06

Die Ergebnisse für die Einstellungsänderung in der EG im Prä-Post-Vergleich zeigen mit $R^2 = 16.$, $p < .001$, dass das Gesamtmodell signifikant ist und 16 % der Varianz der abhängigen Variablen erklärt. Der Interaktionsterm als Prädiktor für die Einstellungsänderung vom ersten zum zweiten Messzeitpunkt zeigt keine Signifikanz ($p = .59$). Die Hinzunahme des Interaktionsterms als Prädiktor im Regressionsmodell als zusätzliche erklärende Variable ist ebenfalls nicht signifikant, da R^2-Change = .00, $p = .59$.

Die Ergebnisse für die Einstellungsänderung in der KG im Prä-Post-Vergleich zeigen mit $R^2 = 08.$, $p = .01$, dass das Gesamtmodell signifikant ist und 8 % Varianzaufklärung hat. Der Interaktionsterm als Prädiktor für die Einstellungsänderung vom ersten zum zweiten Messzeitpunkt zeigt keine Signifikanz ($p = .15$). Die Hinzunahme des Interaktionsterms als Prädiktor im Regressionsmodell als zusätzliche erklärende Variable ist ebenfalls nicht signifikant (R^2-Change = .02, $p = .15$).

Die zweite Analyse bezieht sich auf die Selbstwirksamkeit im Kontext IT-Sicherheit der ProbandInnen durch die Bildung.

Die Ergebnisse für die Änderung der Selbstwirksamkeit im Kontext IT-Sicherheit in der EG im Prä-Post-Vergleich zeigen ein $R^2 = .14.$, $p = .01$ und dementsprechend, dass das Gesamtmodell signifikant ist und mit 14 % die Varianz erklärt. Der Interaktionsterm als Prädiktor für die Änderung der Selbstwirksamkeit im Kontext IT-Sicherheit vom ersten zum zweiten Messzeitpunkt zeigt keine Signifikanz ($p = .14$). Die Hinzunahme des Interaktionsterms als Prädiktor im Regressionsmodell als zusätzliche erklärende Variable ist ebenfalls nicht signifikant, denn R^2-Change = .03, $p = .14$.

Die Ergebnisse für die Änderung der Selbstwirksamkeit im Kontext IT-Sicherheit in der KG im Prä-Post-Vergleich zeigen mit $R^2 = .04.$, $p = .20$, dass das Gesamtmodell nicht signifikant ist und keine Varianz erklärt. Der Interaktionsterm als Prädiktor für die Änderung der Selbstwirksamkeit im Kontext IT-Sicherheit vom ersten zum zweiten Messzeitpunkt zeigt keine Signifikanz ($p = .14$). Die Hinzunahme des Interaktionsterms als Prädiktor im Regressionsmodell als zusätzliche erklärende Variable ist ebenfalls nicht signifikant, da R^2-Change = .01, $p = .14$.

Die dritte Analyse, welche sich auf die Beeinflussung der Kontrollüberzeugung durch die Bildung bezieht, zeigt folgendes Ergebnis: Die Voraussetzung der Linearität ist erfüllt;

Streudiagramme zwischen den metrischen Prädiktoren und dem Kriterium zeigen keine nichtlinearen Tendenzen.

Die Ergebnisse für die Änderung der Kontrollüberzeugung in der EG im Prä-Post-Vergleich zeigen mit $R^2 = .05.$, $p = .14$, dass das Gesamtmodell nicht signifikant ist und keine Varianzaufklärung leisten kann. Der Interaktionsterm als Prädiktor für die Änderung der Kontrollüberzeugung vom ersten zum zweiten Messzeitpunkt zeigt keine Signifikanz ($p = .85$). Die Hinzunahme des Interaktionsterms als Prädiktor im Regressionsmodell als zusätzliche erklärende Variable ist ebenfalls nicht signifikant, denn R^2-Change = .00, $p = .85$.

Die Ergebnisse für die Änderung der Kontrollüberzeugung in der KG im Prä-Post-Vergleich zeigen mit $R^2 = .05.$, $p = .10$, dass das Gesamtmodell nicht signifikant ist und keine Varianzaufklärung leisten kann. Der Interaktionsterm als Prädiktor für die Änderung der Kontrollüberzeugung vom ersten zum zweiten Messzeitpunkt zeigt keine Signifikanz ($p = .85$). Die Hinzunahme des Interaktionsterms als Prädiktor im Regressionsmodell als zusätzliche erklärende Variable ist ebenfalls nicht signifikant (R^2-Change = .00, $p = .85$).

Zusammenfassend sind die Ergebnisse in den Tabellen 55 und 56 dargestellt.

Tab. 55: Moderation der AV durch die Bildung in der EG im Prä-Post-Vergleich

abhängige Variable				95% CI			
	Prädiktor	β	se (HC3)	LL	UL	*R²*	*p*
Einstellungs-änderung (n = 108)	Teilnahme	-.35	.09	-.54	-.15	.16	.00**
	Bildung	.09	.08	-.07	.25		
	Teilnahme* Bildung	-.07	.13	-.20	.35		.59
Kontrollüber-zeugung (n = 108)	Teilnahme	-.27	.22	-.72	.16	.05	.14
	Bildung	.17	.12	-.07	.42		
	Teilnahme* Bildung	.04	.23	-.41	.50		
Selbstwirk-samkeit im Kontext von IT-Sicherheit (n = 108)	Teilnahme	-.35	.12	-.60	-.11	.12	.01*
	Bildung	-.01	.09	-.19	.16		
	Teilnahme* Bildung	.25	.17	.08	.60		.14*

Anmerkungen: * < .05, ** < .01
LL = lower level
UL = upper level
CI = Confidenzintervall

Tab. 56: Moderation der AV durch die Bildung in der KG im Prä-Post-Vergleich

abhängige Variable				95% CI			
	Prädiktor	β	se (HC3)	LL	UL	R^2	*p*
Einstellungs-änderung (n = 110)	Teilnahme	-.06	.13	-.33	-.20	.16	.01*
	Bildung	.25	.09	-.07	.43		
	Teilnahme* Bildung	-.27	.18	-.64	.10		.15
Kontrollüber-zeugung (n = 110)	Teilnahme	.05	.15	-.24	.35	.05	.10
	Bildung	.24	.10	.03	.45		
	Teilnahme* Bildung	-.39	.21	-.82	.04		
Selbstwirk-samkeit im Kontext von IT-Sicherheit (n = 110)	Teilnahme	-.17	.09	-.35	.01	.04	.20**
	Alter	-.06	.06	-.18	.05		
	Teilnahme* Bildung	.18	.12	-.06	.44		

Anmerkungen: * < .05, ** < .01
LL = lower level
UL = upper level
CI = Confidenzintervall

Nachfolgend werden die Ergebnisse der Analysen von t1 zu t3 vorgestellt.

Die erste Analyse bezieht sich auf die Moderation des Effektes der Teilnahme auf die Einstellung der ProbandInnen durch die Bildung im Prä-Post-Follow-up-Vergleich. Hier zeigt sich, dass die Voraussetzung der Linearität erfüllt ist und dass die Streudiagramme zwischen den metrischen Prädiktoren und dem Kriterium keine nichtlinearen Tendenzen zeigen. Eine Überprüfung der Autokorrelation zeigt darüber hinaus keine bedenkliche Korrelation der Residuen (siehe Tabelle 54).

Die Ergebnisse für die Einstellungsänderung in der EG im Prä-Post-Follow-up-Vergleich zeigen mit R^2 = 32., p < .001, dass das Gesamtmodell signifikant ist und 32 % Varianzaufklärung leistet. Der Interaktionsterm als Prädiktor für die Einstellungsänderung vom ersten zum dritten Messzeitpunkt zeigt keine Signifikanz (p = .61). Die Hinzunahme des Interaktionsterms als Prädiktor im Regressionsmodell als zusätzliche erklärende Variable ist somit ebenfalls nicht signifikant, denn R^2-Change = .00, p = .61.

Die Ergebnisse für die Einstellungsänderung in der KG im Prä-Post-Follow-up-Vergleich zeigen mit R^2 = 29., p = .00, dass das Gesamtmodell signifikant ist und 29 % Varianzaufklärung leistet. Der Interaktionsterm als Prädiktor für die Einstellungsänderung vom ersten zum dritten Messzeitpunkt zeigt keine Signifikanz, da p = .10. Die Hinzunahme des Interaktionsterms als Prädiktor im Regressionsmodell als zusätzliche erklärende Variable ist somit ebenfalls nicht signifikant (R^2-Change = .01, p = .10).

Die Ergebnisse für die Änderung der Kontrollüberzeugung in der EG im Prä-Post-Vergleich zeigen mit R^2 = .05., p = .33, dass das Gesamtmodell nicht signifikant ist und keine

Varianzaufklärung leistet. Der Interaktionsterm als Prädiktor für die Änderung der Kontrollüberzeugung vom ersten zum dritten Messzeitpunkt zeigt keine Signifikanz (p = .29). Die Hinzunahme des Interaktionsterms als Prädiktor im Regressionsmodell als zusätzliche erklärende Variable ist somit ebenfalls nicht signifikant, da R^2-Change = .01, p = .29.

Die Ergebnisse für die Änderung der Kontrollüberzeugung in der KG im Prä-Post-Vergleich zeigen mit R^2 = .10., p < .001, dass das Gesamtmodell nicht signifikant ist und keine Varianzaufklärung leisten kann. Der Interaktionsterm als Prädiktor für die Änderung der Kontrollüberzeugung vom ersten zum dritten Messzeitpunkt zeigt keine Signifikanz (p = .46). Die Hinzunahme des Interaktionsterms als Prädiktor im Regressionsmodell als zusätzliche erklärende Variable ist somit ebenfalls nicht signifikant, da R^2-Change = .00, p = .46.

Die Ergebnisse für die Änderung der Selbstwirksamkeit im Kontext von IT-Sicherheit in der EG im Prä-Post-Vergleich zeigen eine Varianzaufklärung von R^2 = .33. für das Gesamtmodell. Der Interaktionsterm als Prädiktor für die Änderung der Kontrollüberzeugung vom ersten zum dritten Messzeitpunkt hat eine Signifikanz von p = .01. Die Hinzunahme des Interaktionsterms als Prädiktor im Regressionsmodell als zusätzliche erklärende Variable ist somit ebenfalls signifikant, denn R^2-Change = .06, p = .01.

Werden die Daten dezentriert und einer Johnson-Neyman-Prozedur unterzogen, zeigt sich, dass die Teilnehmenden mit einer Berufsausbildung (1), mit einer Fachhochschulausbildung (2) und teilweise mit einer Universitätsausbildung (3) im Gegensatz zu den Teilnehmenden ohne Ausbildung (4) die Selbstwirksamkeit im Kontext von IT-Sicherheit verändern konnten. Detailliert bedeutet dies, dass am Output (dargestellt in der Tabelle 57) erkennbar ist, dass mit einer höheren Ausprägung der Zahl bei Bildung eine Abschwächung des Effektes (aufgrund des Minus) erkennbar ist. Diese Abschwächung ist aber bei Bildung = 1 stärker als bei Bildung = 3, da der Effect-Wert bei Bildung = 1 stärker negativ ist als bei Bildung = 3. Somit kann daraus eine Abschwächung des Effektes mit zunehmender Bildung abgeleitet werden, allerdings nur zwischen der Berufs- und der Universitätsausbildung.

Tab. 57: Selbstwirksamkeit im Kontext von IT-Sicherheit zur Bildung in der EG zum t2

Bildung	Effect	se (HC3)	t	p	LLCI	ULCI
1	-0.92	0.14	-6.70	**0.00****	-1.20	-0.65
1	-0.87	0.12	-7.01	**0.00****	-1.12	-0.63
1	-0.82	0.11	-7.28	**0.00****	-1.04	-0.60
1	-0.77	0.10	-7.42	**0.00****	-0.97	-0.56
2	-0.71	0.10	-7.33	**0.00****	-0.91	-0.52
2	-0.66	0.10	-6.94	**0.00****	-0.85	-0.47
2	-0.61	0.10	-6.26	**0.00****	-0.80	-0.42
2	-0.56	0.10	-5.39	**0.00****	-0.76	-0.35
2	-0.50	0.11	-4.49	**0.00****	-0.73	-0.28
2	-0.45	0.12	-3.64	**0.00****	-0.70	-0.21
3	-0.40	0.14	-2.90	**0.00****	-0.67	-0.13
3	-0.35	0.15	-2.27	**0.03***	-0.65	-0.04
3	-0.32	0.16	-1.99	0.05	-0.64	0.00
3	-0.29	0.17	-1.75	0.08	-0.63	0.04
3	-0.24	0.19	-1.31	0.20	-0.61	0.13
3	-0.19	0.20	-0.94	0.35	-0.59	0.21
3	-0.14	0.22	-0.62	0.54	-0.58	0.30
3	-0.09	0.24	-0.36	0.72	-0.56	0.39
4	-0.03	0.26	-0.13	0.90	-0.54	0.48
4	0.02	0.28	0.07	0.94	-0.53	0.57
4	0.07	0.29	0.25	0.81	-0.51	0.66
4	0.12	0.31	0.40	0.69	-0.50	0.75

Anmerkungen: * < .05, ** < .01*
LL = lower level
UL = upper level
CI = Confidenzintervall
t = Teststatistik für diesen Effekt

Die Ergebnisse für die Änderung der Selbstwirksamkeit im Kontext von IT-Sicherheit in der KG im Prä-Post-Vergleich zeigen eine Varianzaufklärung von R^2 = .13 für das Gesamtmodell. Der Interaktionsterm als Prädiktor für die Änderung der Kontrollüberzeugung vom ersten zum dritten Messzeitpunkt besitzt eine Signifikanz von p = .04. Die Hinzunahme des Interaktionsterms als Prädiktor im Regressionsmodell als zusätzliche erklärende Variable ist somit ebenfalls signifikant (R^2-Change = .04, p = .04).

Werden die Daten auch hier dezentriert und einer Johnson-Neyman-Prozedur unterzogen, zeigt sich, dass die Teilnehmenden mit einer Berufsausbildung (1), mit einer Fachhochschulausbildung (2) und teilweise mit einer Universitätsausbildung (3) im Gegensatz zu den Teilnehmenden ohne Ausbildung (4) die Selbstwirksamkeit im Kontext von IT-Sicherheit verändern konnten. Detailliert bedeutet dies auch hier, dass am Output (dargestellt in der Tabelle 58) erkennbar ist, dass mit einer höheren Ausprägung der Zahl bei Bildung eine Abschwächung des Effektes (aufgrund des Minus) erkennbar ist. Diese Abschwächung ist aber bei Bildung = 1 stärker als bei Bildung = 3, da der

Effect-Wert für Bildung = 1 stärker negativ ist als bei Bildung = 3. Somit ist eine Abschwächung des Effektes mit zunehmender Bildung zu erkennen, allerdings auch hier nur zwischen der Berufs- und der Universitätsausbildung.

Tab. 58: Selbstwirksamkeit im Kontext von IT-Sicherheit zur Bildung in der KG zum t2

Bildung	Effect	se (HC3)	t	p	LLCI	ULCI
1	-1.20	0.36	-3.31	**0.00****	-1.93	-0.48
1	-1.13	0.33	-3.40	**0.00****	-1.79	-0.47
1	-1.06	0.30	-3.50	**0.00****	-1.66	-0.46
1	-0.99	0.27	-3.61	**0.00****	-1.53	-0.44
2	-0.92	0.25	-3.71	**0.00****	-1.41	-0.43
2	-0.85	0.22	-3.80	**0.00****	-1.29	-0.40
2	-0.78	0.20	-3.84	**0.00****	-1.18	-0.37
2	-0.70	0.18	-3.81	**0.00****	-1.07	-0.34
2	-0.63	0.17	-3.66	**0.00****	-0.98	-0.29
2	-0.56	0.17	-3.34	**0.00****	-0.90	-0.23
3	-0.49	0.17	-2.88	**0.01***	-0.83	-0.15
3	-0.42	0.18	-2.33	**0.02***	-0.78	-0.06
3	-0.37	0.19	-1.99	0.05	-0.75	0.00
3	-0.35	0.19	-1.78	0.08	-0.74	0.04
3	-0.28	0.21	-1.29	0.20	-0.70	0.15
3	-0.21	0.24	-0.86	0.39	-0.68	0.27
3	-0.13	0.26	-0.51	0.61	-0.66	0.39
3	-0.06	0.29	-0.21	0.83	-0.64	0.52
4	0.01	0.32	0.03	0.98	-0.63	0.65
4	0.08	0.35	0.23	0.82	-0.62	0.78
4	0.15	0.38	0.40	0.69	-0.61	0.91
4	0.22	0.42	0.54	0.59	-0.60	1.05

Anmerkungen: * < .05, ** < .01
LL = lower level
UL = upper level
CI = Confidenzintervall
t = Teststatistik für diesen Effekt

Eine Zusammenfassung der Moderation für die EG findet sich in der folgenden Tabelle 59.

Tab. 59: Moderation der AV durch die Bildung in der EG im Prä-Post-Follow-up-Vergleich

abhängige Variable				95% CI			
	Prädiktor	β	se (HC3)	LL	UL	R^2	*p*
Einstellungs-änderung (n = 93)	Teilnahme	-.50	.09	-.69	-.32	32	00**
	Bildung	.06	.07	-.07	.21		
	Teilnahme*Bildung	-.06	.12	-.30	.18		.61
Kontrollüber-zeugung (n = 93)	Teilnahme	-20	.15	-.51	.10	.05	.33
	Bildung	.04	.10	-.15	.25		
	Teilnahme*Bildung	-.199	.18	-.57	.17		
Selbstwirk-samkeit im Kontext von IT-Sicherheit (n = 93)	Teilnahme	-.54	.10	-.75	-.34	.33	00**
	Alter	-.09	.08	-.25	.06		
	Teilnahme*Bildung	.34	.13	.08	.61		.01*

Anmerkungen: * < .05, ** < .01
LL = lower level
UL = upper level
CI = Confidenzintervall

Eine Zusammenfassung der Moderation für die KG findet sich in der folgenden Tabelle 60.

Tab. 60: Moderation der AV durch die Bildung in der KG im Prä-Post-Follow-up-Vergleich

abhängige Variable				95% CI			
	Prädiktor	β	se (HC3)	LL	UL	R^2	*p*
Einstellungs-änderung (n = 110)	Teilnahme	-.45	.12	-.69	-.21	.29	.00**
	Bildung	.30	.07	.16	.45		
	Teilnahme*Bildung	-.25	.15	-.56	.05		
Kontrollüber-zeugung (n = 110)	Teilnahme	.41	.15	.09	.72	.10	00**
	Bildung	-.15	.12	-.39	.09		
	Teilnahme*Bildung	-.16	.22	-.62	.28		
Selbstwirk-samkeit im Kontext von IT-Sicherheit (n = 110)	Teilnahme	-.54	.16	-.88	-.21	.13	.00**
	Alter	-.06	.10	-.27	.13		
	Teilnahme *Bildung	.47	.23	.01	.94		.04*

Anmerkungen: * < .05, ** < .01
LL = lower level
UL = upper level
CI = Confidenzintervall

Fazit zur Hypothese H8

Die Analyse des Einflusses des Moderators Bildung auf die Wirksamkeit zeigt einen signifikanten Moderatorseffekt, der sich verringert, je höher die Bildung ist. Somit ist die Nullhypothese zu akzeptieren und H8 zu verwerfen.

Geschlecht als Moderator der Wirksamkeit der Maßnahme (H9)

Es wurde angenommen, dass die Wirksamkeit der Maßnahme (Prä-Post) bei den Lernenden der Experimentalgruppe und der Kontrollgruppe durch das Geschlecht moderiert wird.

Die erste Analyse bezieht sich auf die Moderation des Effektes der Teilnahme auf die Einstellung der ProbandInnen durch das Geschlecht. Hier zeigen die Befunde, dass die Voraussetzung der Linearität erfüllt ist und dass die Streudiagramme zwischen den metrischen Prädiktoren und dem Kriterium keine nichtlinearen Tendenzen zeigen.

Die Ergebnisse für die Einstellungsänderung in der EG im Prä-Post-Vergleich zeigen ein $R^2 = 16.$, $p < .001$ und insofern, dass das Gesamtmodell signifikant ist und 16 % Varianzaufklärung leistet. Der Interaktionsterm als Prädiktor für die Einstellungsänderung vom ersten zum zweiten Messzeitpunkt zeigt keine Signifikanz ($p = .81$). Die Hinzunahme des Interaktionsterms als Prädiktor im Regressionsmodell als zusätzliche erklärende Variable ist ebenfalls nicht signifikant, denn R^2-Change = .00, $p = .81$.

Die Ergebnisse für die Einstellungsänderung in der KG im Prä-Post-Vergleich zeigen mit $R^2 = 10.$, $p = .01$, dass das Gesamtmodell signifikant ist und 10 % der Varianz aufklärt. Der Interaktionsterm als Prädiktor für die Einstellungsänderung vom ersten zum zweiten Messzeitpunkt zeigt keine Signifikanz ($p = .34$). Die Hinzunahme des Interaktionsterms als Prädiktor im Regressionsmodell als zusätzliche erklärende Variable ist ebenfalls nicht signifikant, denn R^2-Change = .00, $p = .34$.

Die Ergebnisse für die Änderung der Selbstwirksamkeit im Kontext IT-Sicherheit in der EG im Prä-Post-Vergleich zeigen ein $R^2 = .13.$, $p = .02$ und damit, dass das Gesamtmodell nicht signifikant ist und nur 2 % der Varianz aufklärt. Der Interaktionsterm als Prädiktor für die Änderung der Selbstwirksamkeit im Kontext IT-Sicherheit vom ersten zum zweiten Messzeitpunkt zeigt keine Signifikanz ($p = .48$). Die Hinzunahme des Interaktionsterms als Prädiktor im Regressionsmodell als zusätzliche erklärende Variable ist ebenfalls nicht signifikant, da R^2-Change = .00, $p = .48$.

Die Ergebnisse für die Änderung der Selbstwirksamkeit im Kontext IT-Sicherheit in der KG im Prä-Post-Vergleich zeigen mit $R^2 = .02.$, $p = .41$, dass das Gesamtmodell nicht signifikant ist und nur 2 % der Varianz der abhängigen Variable erklärt. Der Interaktionsterm als Prädiktor für die Änderung der Selbstwirksamkeit im Kontext IT-Sicherheit vom ersten zum zweiten Messzeitpunkt zeigt keine Signifikanz ($p = .85$). Die Hinzunahme des Interaktionsterms als Prädiktor im Regressionsmodell als zusätzliche erklärende Variable ist ebenfalls nicht signifikant, da R^2-Change = .00, $p = .85$.

Die Ergebnisse für die Änderung der Kontrollüberzeugung in der EG im Prä-Post-Vergleich zeigen mit $R^2 = .05$., $p = .21$, dass das Gesamtmodell nicht signifikant ist und keine Varianz der abhängigen Variable erklären kann. Der Interaktionsterm als Prädiktor für die Änderung der Kontrollüberzeugung vom ersten zum zweiten Messzeitpunkt zeigt keine Signifikanz, da $p = .69$. Die Hinzunahme des Interaktionsterms als Prädiktor im Regressionsmodell als zusätzliche erklärende Variable ist ebenfalls nicht signifikant (R^2-Change = .00, $p = .69$).

Die Ergebnisse für die Änderung der Kontrollüberzeugung in der KG im Prä-Post-Vergleich zeigen ein $R^2 = .03$., $p = .26$ und somit, dass das Gesamtmodell nicht signifikant ist und keine Varianzaufklärung der abhängigen Variable leisten kann. Der Interaktionsterm als Prädiktor der Änderung der Kontrollüberzeugung vom ersten zum zweiten Messzeitpunkt zeigt keine Signifikanz ($p = .11$). Die Hinzunahme des Interaktionsterms als Prädiktor im Regressionsmodell als zusätzliche erklärende Variable ist ebenfalls nicht signifikant (R^2-Change = .01, $p = .11$).

Tab. 61: Moderation der AV durch das Geschlecht in der EG im Prä-Post-Vergleich

abhängige Variable				95 % CI			
	Prädiktor	β	se (HC3)	LL	UL	*R²*	*p*
Einstellungs-änderung (n = 108)	Teilnahme	-.40	.09	-.58	-.21	.16	.00**
	Geschlecht	-.17	.12	-.42	.07		
	Teilnahme* Geschlecht	.04	.18	-.32	.41		
Kontrollüber-zeugung (n = 108)	Teilnahme	-.33	.25	-.84	.177	.05	.21
	Geschlecht	-.22	.23	-.68	.23		
	Teilnahme* Geschlecht	-.199	.50	-1.2	.80		
Selbstwirk-samkeit im Kontext von IT-Sicherheit (n = 108)	Teilnahme	-.37	.13	-.63	-.10	.13	.02*
	Geschlecht	-.19	.14	-.48	.09		
	Teilnahme* Geschlecht	-.18	.26	-.71	.33		

Anmerkungen: * < .05, ** < .01
LL = lower level
UL = upper level
CI = Confidenzintervall

Tab. 62: Moderation der AV durch die Bildung in der KG im Prä-Post-Vergleich

abhängige Variable				95 % CI			
	Prädiktor	β	se (HC3)	LL	UL	R^2	*p*
Einstellungs-änderung (n = 110)	Teilnahme	-.07	-.54	-.34	.19	.10	0.01*
	Geschlecht	-.43	-3.01	-.72	-.14		
	Teilnahme* Geschlecht	.02	-.95	-.27	.79		
Kontrollüber-zeugung (n = 110)	Teilnahme	.04	.14	-.25	-.33	.03	.26
	Geschlecht	-.24	.18	-.60	.11		
	Teilnahme* Geschlecht	.47	.29	-.12	1.06		
Selbstwirk-samkeit im Kontext von IT-Sicherheit (n = 110)	Teilnahme	-.13	.08	-.31	.03	.02	.41
	Geschlecht	-.07	.10	-.28	.12		
	Teilnahme* Geschlecht	.03	.17	-.30	.37		

Anmerkungen: * < .05, ** < .01
LL = lower level
UL = upper level
CI = Confidenzintervall

Nachfolgend werden die Ergebnisse der Analysen im Prä-Post-Follow-up-Vergleich vorgestellt.

Die Ergebnisse für die Einstellungsänderung in der EG im Prä-Post-Follow-up-Vergleich zeigen ein R^2 = 35., p < .001 und aufgrund dessen, dass das Gesamtmodell signifikant ist und mit 35 % die Varianz erklärt. Der Interaktionsterm als Prädiktor für die Einstellungsänderung vom ersten zum dritten Messzeitpunkt zeigt keine Signifikanz (p = .52). Die Hinzunahme des Interaktionsterms als Prädiktor im Regressionsmodell als zusätzliche erklärende Variable ist somit ebenfalls nicht signifikant (R^2-Change = .00, p = .52).

Die Ergebnisse für die Einstellungsänderung in der KG im Prä-Post-Follow-up-Vergleich zeigen mit R^2 = 17., p < .001, dass das Gesamtmodell signifikant ist und mit 17 % die Varianz erklärt. Der Interaktionsterm als Prädiktor für die Einstellungsänderung vom ersten zum dritten Messzeitpunkt zeigt hingegen keine Signifikanz, denn p = .82. Die Hinzunahme des Interaktionsterms als Prädiktor im Regressionsmodell als zusätzliche erklärende Variable ist somit ebenfalls nicht signifikant (R^2-Change = .00, p = .82).

Die Ergebnisse für die Änderung der Kontrollüberzeugung in der EG im Prä-Post-Follow-up-Vergleich zeigen ein R^2 = .03., p = .60 und insofern, dass das Gesamtmodell nicht signifikant ist und keinen signifikanten Erklärungsbeitrag leisten kann. Der Interaktionsterm als Prädiktor für die Änderung der Kontrollüberzeugung vom ersten zum dritten Messzeitpunkt zeigt keine Signifikanz (p = .75). Die Hinzunahme des Interaktionsterms als Prädiktor im Regressionsmodell als zusätzliche erklärende Variable ist ebenfalls nicht signifikant, da R^2-Change = .00, p = .75.

Die Ergebnisse für die Änderung der Kontrollüberzeugung in der KG im Prä-Post-Follow-up-Vergleich zeigen mit $R^2 = .10.$, $p = .02$, dass das Gesamtmodell signifikant ist und eine Varianz der abhängigen Variable von 10 % erklären kann. Der Interaktionsterm als Prädiktor für die Änderung der Kontrollüberzeugung vom ersten zum dritten Messzeitpunkt zeigt keine Signifikanz ($p = .11$). Die Hinzunahme des Interaktionsterms als Prädiktor im Regressionsmodell als zusätzliche erklärende Variable ist ebenfalls nicht signifikant, denn R^2-Change = .02, $p = .11$.

Die Ergebnisse für die Änderung der Selbstwirksamkeit im Kontext IT-Sicherheit in der EG im Prä-Post-Follow-up-Vergleich zeigen ein $R^2 = .35.$, $p = .00$ und damit, dass das Gesamtmodell signifikant ist und 35 % der Varianz der abhängigen Variable erklärt. Der Interaktionsterm als Prädiktor für die Änderung der Selbstwirksamkeit im Kontext IT-Sicherheit vom ersten zum dritten Messzeitpunkt zeigt eine Signifikanz von $p < .001$. Die Hinzunahme des Interaktionsterms als Prädiktor im Regressionsmodell als zusätzliche erklärende Variable ist ebenfalls hoch signifikant, da R^2-Change = .09, $p < .001$.

Werden die Daten auch hier dezentriert und einer Johnson-Neyman-Prozedur unterzogen, zeigt sich, dass die Teilnehmer im Gegensatz zu den Teilnehmerinnen die Selbstwirksamkeit verändern konnten (siehe Tabelle 63).

Tab. 63: Bedingte Effekte des Prädiktors ‚Selbstwirksamkeit' im Kontext IT-Sicherheit in der EG bei Werten des Moderators ‚Geschlecht'

gender	Effect	se (HC3)	t	p	LLCI	ULCI
weiblich	-0,12	0,20	-0,58	0,57	-0,52	0,29
männlich	-0,81	0,11	-7,27	0,00**	-1,03	-0,59

Anmerkungen: * < .05, ** < .01
LL = lower level
UL = upper level
CI = Confidenzintervall
t = Teststatistik für diesen Effekt

Die Ergebnisse für die Änderung der Selbstwirksamkeit im Kontext IT-Sicherheit in der KG im Prä-Post-Follow-up-Vergleich zeigen mit $R^2 = .17.$, $p < .001$, dass das Gesamtmodell signifikant ist und 17 % der Varianz der AV erklärt. Der Interaktionsterm als Prädiktor für die Änderung der Selbstwirksamkeit im Kontext IT-Sicherheit vom ersten zum dritten Messzeitpunkt zeigt eine Signifikanz von $p = .03$. Die Hinzunahme des Interaktionsterms als Prädiktor im Regressionsmodell als zusätzliche erklärende Variable ist ebenfalls hoch signifikant, denn R^2-Change = .04, $p = .03$.

Werden die Daten auch hier dezentriert und einer Johnson-Neyman-Prozedur unterzogen, zeigt sich, dass die Teilnehmer im Gegensatz zu den Teilnehmerinnen die Selbstwirksamkeit verändern konnten (siehe Tabellen 64 und 65).

Tab. 64: Bedingte Effekte des Prädiktors ‚Selbstwirksamkeit' im Kontext IT-Sicherheit in der KG bei Werten des Moderators ‚Geschlecht'

gender	Effect	se (HC3)	t	p	LLCI	ULCI
weiblich	-0,17	0,20	-0,82	0,41	-0,56	0,23
männlich	-0,94	0,31	-3,07	0,00**	-1,55	-0,33

Anmerkungen: * < .05, ** < .01
LL = lower level
UL = upper level
CI = Confidenzintervall
t = Teststatistik für diesen Effekt

Tab. 65: Moderation der AV durch das Geschlecht in der EG im Prä-Post-Follow-up-Vergleich

abhängige Variable				95 % CI			
	Prädiktor	β	se (HC3)	LL	UL	R^2	*p*
Einstellungs-änderung (n = 93)	Teilnahme	-.49	.09	-.67	-.32	.35	.00**
	Geschlecht	.26	.10	.04	.48		
	Teilnahme* Geschlecht	-.11	.18	-.48	.24		
Kontrollüber-zeugung (n = 93)	Teilnahme	-.19	.15	-.50	.12	.03	.60
	Geschlecht	-.03	.17	-.38	.32		
	Teilnahme* Geschlecht	-.10	.32	-.74	.54		
Selbstwirk-samkeit im Kontext von IT-Sicherheit (n = 93)	Teilnahme	-49	.11	-.71	-.27	.35	.00**
	Geschlecht	.11	.13	-.14	.38		
	Teilnahme* Geschlecht	-.69	.23	-1.15	-.23		.00**

Anmerkungen: * < .05, ** < .01
LL = lower level
UL = upper level
CI = Confidenzintervall

Tab. 66: Moderation der AV durch das Geschlecht in der KG im Prä-Post-Follow-up-Vergleich

abhängige Variable				95 % CI			
	Prädiktor	β	se (HC3)	LL	UL	R^2	*p*
Einstellungs-änderung (n = 89)	Teilnahme	-.54	.16	-.87	-.21	.17	.00
	Geschlecht	-.07	.17	-.42	.26		
	Teilnahme* Geschlecht	-.07	.35	-.78	.62		
Kontrollüber-zeugung (n = 89)	Teilnahme	.50	.16	.17	.83	.10	.02
	Geschlecht	-.12	.20	-.52	.27		
	Teilnahme* Geschlecht	.54	.34	-.14	1.22		
Selbstwirk-samkeit im Kontext von IT-Sicherheit (n = 89)	Teilnahme	-.51	.17	-.86	-.16	.17	.00
	Geschlecht	-.31	.20	-.71	.08		
	Teilnahme* Geschlecht	-.77	.36	-1.50	-.04		.03

Anmerkungen: * < .05, ** < .01
LL = lower level
UL = upper level
CI = Confidenzintervall

Fazit zur Hypothese H9

Die Analyse des Moderators Geschlecht auf die Wirksamkeit zeigt einen signifikanten Moderatorseffekt, der bei den Teilnehmern den Effekt der Selbstwirksamkeit nicht nur signifikant sondern auch negativer als bei den Teilnehmerinnen beeinflusst. Somit kann die Hypothese H9 bekräftigt werden.

VersuchsleiterInnenartefakt als Moderator der Wirksamkeit der Maßnahme (H10)

Um die Objektivität abzusichern, wurde die präventive Maßnahme durch zwei Lehrende durchgeführt. Es wurde diesbezüglich angenommen, dass die Wirksamkeit der Maßnahme (Prä-Post) nicht von der Durchführung durch den Dozenten oder die Dozentin abhängt.

Die Ergebnisse zeigen, dass das Gesamtmodell 12 % der Varianz erklärt, denn $R^2 = .12$, $p = .00$. Gleichfalls fungiert der Moderator mit $p = .06$ als signifikanter Prädiktor für die Veränderung im Verhalten der ProbandInnen. Der Interaktionsterm erklärt im Regressionsmodell keinen signifikanten zusätzlichen Varianzanteil (R^2-Change = .00, $p = .66$). Die Dozentin und der Dozent hatten also scheinbar einen Einfluss. Das R^2 ändert sich nicht wirklich, was jedoch nicht den Effekt negiert, der durch β ausgedrückt wird. Da dieser positiv ist, hatte die Dozentin/der Dozent mit der höheren Kodierung (z.B. 1) gegenüber der Dozentin/dem Dozenten mit der niedrigeren Kodierung (z.B. 0) einen positiven Effekt (i.H.v. 0.16) auf die AV.

Tab. 67: Moderation der AV durch den Dozenten/die Dozentin

abhängige Variable				95 % CI			
	Prädiktor	β	se (HC3)	LL	UL	*R²*	*p*
Wirkung	Teilnahme	-.32	.08	-.47	-.16	.12	.00**
(n = 182)	DozentIn	.16	.06	.03	.28		.06
	DozentIn*	-.05	.13	-.32	.21		.66

*Anmerkungen. * < .05, ** < .01*
LL = lower level
UL = upper level
CI = Confidenzintervall

Fazit zur Hypothese H10

Da die Analyse des Moderators ‚DozentIn' auf die Selbstwirksamkeit keinen signifikanten Moderatoreffekt zeigt, kann die Hypothese H10 akzeptiert werden.

7 Interpretation und Diskussion

Dieses Kapitel fasst die gewonnenen Forschungsergebnisse zusammen und vergleicht diese mit bereits vorhandenen Forschungsständen.

7.1 Interpretation und Diskussion der Ergebnisse

In diesem Unterkapitel 7.1 werden die Ergebnisse unter Berücksichtigung des derzeitigen Forschungsstands interpretiert.

7.1.1 Einstellung im Kontext von IT-Sicherheit

Die Veränderung der Einstellung lässt sich bereits im Prä-Post-Vergleich signifikant nachweisen, denn hier zeigt sich ein hoch signifikanter Haupteffekt für die Gruppenzugehörigkeit. Beide Untersuchungen machen ebenfalls eine signifikante Wechselwirkung zwischen den beiden Faktoren deutlich. Der visualisierte Mittelwertverlauf zeigt, dass sich die Einstellung in der KG nicht nur verschlechterte, sondern unter den Ausgangspunkt sank. Demgegenüber zeigte sich in der EG eine stetige Verbesserung der Einstellung. Geschlussfolgert werden kann dementsprechend, dass präventive Maßnahmen, die die Einstellung verbessern sollen, unbedingt didaktisch zu konzipieren und einem Training anzuschließen sind. Findet diese didaktische Konzeption und das Involvieren eines Trainings nicht statt, verschlechtert sich die Einstellung, sodass die Maßnahme einen unerwünschten negativen Effekt hat. Diese Erkenntnis besitzt eine hohe praktische Relevanz, da präventive Maßnahmen oft als sogenannte „HackerInnenshows“ einem breiten Publikum präsentiert werden (Allgeier CORE Group GmbH 2020), ohne jedoch ein Training einzuschließen.

Gleichfalls konnte gezeigt werden, dass Erhebungen vor und nach der präventiven Maßnahme unzureichend sind und eines weiteren Messzeitpunkts bedürfen.

Forschungsbezogene Blickrichtungen zeigen auf, dass sich das im Rahmen dieser Arbeit erzielte Forschungsergebnis mit den Forschungsergebnissen von SanNicolas-Rocca, Schooley und Spears (2014) und der DSV-Gruppe (2006) kongruent zeigen, in deren Rahmen ebenfalls auf interaktive Elemente in der Didaktik verwiesen wird. Forschungsergebnisse von Khan et al. (2011), denen zufolge durch eine reine Präsentation und durch Diskurse eine Verhaltensänderung bewirkt werden kann, können für den Prädiktor Einstellung jedoch nicht bestätigt werden.

7.1.2 Selbstwirksamkeit im Kontext von IT-Sicherheit

Die Betrachtung der Selbstwirksamkeit im Kontext von IT-Sicherheit zeigt im Prä-Post-Vergleich einen signifikanten Haupteffekt für die Gruppenzugehörigkeit, der sich hoch

signifikant auch im Prä-Post-Follow-up-Vergleich nachweisen lässt. Die Wechselwirkung zwischen den beiden Faktoren hat ebenfalls einen signifikanten Einfluss auf die Selbstwirksamkeit im Kontext von IT-Sicherheit der Teilnehmenden, was der Prä-Post-Follow-up-Vergleich bestätigt. Die Betrachtung des Mittelwertverlaufs (siehe Abbildung 52) zeigt, dass beide Gruppen ihre Selbstwirksamkeit im Kontext von IT-Sicherheit während der Maßnahme (also zwischen t1 und t2) verbessern konnten. Auffällig ist jedoch, dass der Wert in der Kontrollgruppe zum dritten Messzeitpunkt unter den Ausgangswert fällt. Das prozedurale Wissen, das im Training angeeignet wurde, hatte daher mit hoher Wahrscheinlichkeit einen signifikanten Effekt auf die Selbstwirksamkeit im Kontext von IT-Sicherheit. Ebenfalls sichtbar wird, dass präventive Maßnahmen im Kontext von Cybercrime, die kein Training beinhalten, die Selbstwirksamkeit sogar soweit verschlechtern können, dass die diesbezüglichen Werte unter den Ausgangswert fallen. Dies deutet ebenfalls darauf hin, dass präventive Maßnahmen, wenn sie die Selbstwirksamkeit im Kontext von IT-Sicherheit verbessern sollen, unbedingt ein Training beinhalten sollten, sodass ein von Winkelmann (2011) postuliertes „Ressourcen stärkendes Training“ zu involvieren ist. Studien von Bandura (1991), welche im Kapitel 2.3.4 erörtert wurden, verweisen hierauf bereits und zeigen auf, dass die eigene Erfahrung die stärkste Wirkung auf die Selbstwirksamkeit hat, was sich auch im Kontext von Schutzmaßnahmen im Kontext von Cybercrime widerspiegelt. Bemerkenswert ist weiterhin der Moderator Geschlecht, der bei den in die Untersuchung einbezogenen Männern nicht nur signifikant, sondern auch negativ ausfällt, und dabei negativer als bei den Frauen. Dies kann damit erklärt werden, dass vorhandene Erfahrungen mit Cybercrime in der evaluierten Maßnahme unterschätzt wurden. Es zeigt sich dementsprechend, dass präventive Maßnahmen in der Lage sind, vorhandene Kompetenzen widerzuspiegeln, und dass darauf geachtet werden sollte, dass gerade männliche Teilnehmer nicht an Selbstwirksamkeit verlieren. Möglich wäre dies durch anschließende Veranstaltungen, die eigenen Erfahrungen einen Raum bieten, z.B. im Kontext von Trainings.

Ein weiterer Prädiktor für die Verhaltensintension ist die Kontrollüberzeugung, auf die nun eingegangen wird.

7.1.3 Kontrollüberzeugung im Kontext von IT-Sicherheit

Der Prä-Post-Vergleich zur Kontrollüberzeugung zeigt einen signifikanten Haupteffekt für die Gruppenzugehörigkeit. Da der Messwiederholungsfaktor ebenfalls signifikant ist, bedeutet dies, dass sich die Kontrollüberzeugung der ProbandInnen (über beide Gruppen hinweg) signifikant über die Zeit geändert hat und eine hohe Effektstärke besitzt. Die Wechselwirkung zwischen den beiden Faktoren zeigt einen signifikanten Einfluss auf die Kontrollüberzeugung der Teilnehmenden, jedoch mit einer geringen Effektstärke.

Ergebnisse im Prä-Post-Follow-up-Vergleich bestätigen die signifikanten Ergebnisse, weisen jedoch höhere Effektstärken aus. So zeigt sich der Messwiederholungsfaktor nicht nur hoch signifikant, sondern auch mit einer hohen Effektstärke. Bemerkenswert ist auch der Mittelwertverlauf, denn hier zeigt sich im Prä-Post-Vergleich eine stärkere positive Veränderung der Kontrollüberzeugung in der EG gegenüber der KG, wobei dieser Wert in der EG jedoch im Prä-Post-Follow-up-Vergleich massiv absinkt, während sich die Kontrollüberzeugung in der KG verbessert. Sehr bemerkenswert ist dementsprechend, dass die KG ohne Training die Kontrollüberzeugung gegenüber der EG verbessern konnte. Was die Interpretation dieses Effektes anbelangt, so lässt sich vermuten, dass das Training die Kontrollüberzeugung in der EG verschlechterte, weil die konzipierte Trainingsmaßnahme die Kompliziertheit nicht auflösen konnte und diesbezüglich die Kontrollüberzeugung langfristig verschlechterte. Würde dieser Effekt einer zukünftigen statistischen Überprüfung standhalten, zum Beispiel durch die Messung von Kontrollüberzeugungen anhand weiterer Skalen, wie es Kovaleva et al. (2012) beschreiben, würde das auf die Notwendigkeit eines „Auffangens“ der Teilnehmenden hinweisen, um Wirkungen erzielen zu können, die für die Einzelnen gewinnbringend sind. Praktisch relevant wäre es unter anderem, zu prüfen, welche Trainingsmethoden mit welchen Inhalten zielgruppenbezogen implementiert werden müssten. Überlegt werden sollte, inwieweit Inhalte nicht innerhalb eines kurzen Zeitraums als Gesamtpaket präsentiert, sondern langfristig sequentiell angeboten werden könnten, um die Kontrollüberzeugung langfristig beeinflussen und die Kompliziertheit reduzieren zu können. Forschungsergebnisse von Bahrick, Bahrick und Wittlinger (1975) zeigen bereits auf, dass durch „stapelndes Lernen“ die Behaltensleistung verbesset werden kann, was laut des InfoSec-Institutes auch im Kontext von präventiven Maßnahmen zur IT-Sicherheit genutzt werden könnte (Infosec 2014). Um jedoch zu klären, ob diese Maßnahmen die Kontrollüberzeugung beeinflussen, bedarf es weiterer Studien, die die sinnvolle Sequenzierung der Trainingseinheiten in Anzahl und Länge in den Blick nehmen und im Kontext der wahrgenommenen Verhaltenskontrolle beleuchten. Das Ergebnis der hier zentralen Evaluationsstudie zeigt allerdings bereits deutlich, dass eine Differenzierung zwischen der Kontrollüberzeugung und der Selbstwirksamkeit angebracht ist. Denn TeilnehmerInnen, die Cybersicherheit als sinnlos betrachten, werden das Verhalten genauso wenig ändern wie TeilnehmerInnen, die nicht wissen, wie sie sich vor Cyberangriffen schützen können.

7.1.4 Moderation der AV durch das Lebensalter

In der Prä-Post-Auswertung des Moderators Lebensalter zeigte sich dessen signifikante Auswirkung auf das Merkmal Einstellung und auf die Bewertung der Selbstwirksamkeit im Kontext von IT-Sicherheit in unterschiedlichen Altersgruppen. So moderiert das Alter

in der EG die Kontrollüberzeugung in den Altersgruppen 22-33 Jahre (verstärkend) und 60-67 Jahre (schwächend), nicht jedoch signifikant in der KG. Die 34-60-Jährigen besitzen möglicherweise durch die Nutzung medialer Produkte eigene Strategien, um die Kontrollüberzeugung zu reflektieren. Da die Einstellungsänderung ebenfalls in der Altersgruppe 40-67 Jahre in der EG und in der Altersgruppe 42-67 Jahre in der KG moderiert wird (zunehmend geschwächt), ist davon auszugehen, dass mit zunehmendem Alter das Wissen zum Thema Cybercrime aufgrund der Komplexität/Kompliziertheit und Aktualität durch eigene Lernbestrebungen wie z.B. Lebenslanges Lernen oder Mediennutzung nicht mehr von selbst generiert werden kann. Hier wäre also eine Unterstützung angemessen, die, wenn angeboten und genutzt, positive Wirkungen zeigen kann. Die deutsch-amerikanische Studie „Digitisation A Quantitative and Qualitative Market Research Elicitation“ der Unternehmung PWC (2018), in die 408 Befragte involviert waren, unterstreicht die Moderation des Lebensalters in dem Bereich der Digitalisierung, denn den Befunden zufolge haben bereits 39-65-Jährige Angst, nicht mit dem erforderlichen Wissen über digitale Innovationen mithalten zu können. Da die Kommunikation bei den 20-30-Jährigen überwiegend digital erfolgt (Porschen 2020), sind die Ergebnisse der Studie schlüssig, da jede Altersgruppe ein Kommunikationsbedürfnis besitzt und ein Kommunikationsmedium nutzen muss, das kompatibel zum anderen ist.

7.1.5 Moderation der AV durch das Bildungsniveau

Die Betrachtung der Bildung als Moderator zeigt keine Signifikanz zu den Merkmalen Einstellungsänderung und Kontrollüberzeugung. Signifikant wird die Prä-Post-Follow-up-Auswertung des Moderators Bildung auf die Selbstwirksamkeit im Kontext von IT-Sicherheit mit einer Varianzaufklärung von 33 % für die EG und 13 % für die KG. Besonders profitierten Teilnehmende, die keine akademische Ausbildung hatten, von der besuchten Maßnahme. Die Teilnehmenden ohne Ausbildung konnten hingegen die Selbstwirksamkeit im Kontext von IT-Sicherheit nicht verbessern. Damit wird auch hier der sogenannte Matthäus-Effekt (Merton 1968) für die präventive Maßnahme im Kontext von Cybercrime bedingt untermauert. Dieser wurde bereits in unterschiedlichen Studien nachgewissen und gilt als wissenschaftlich abgesichert. Damit wird praktisch signifikant,[45] welchen Beitrag präventive Unterstützungsangebote leisten können, um eine Verbesserung der Chancengleichheit zu erreichen, die bereits frühkindlich beeinflusst wird. Empfehlungen hierzu sind unter anderem bei Ribolits (2006) zu finden, der darauf verweist, dass es durch „differenzierte Angebote gelingt, über unterschiedliche

[45] „Vom Konzept der statistischen Signifikanz ist das der praktischen Signifikanz zu trennen“ (Fischer 2001, S. 228).

Anspracheformen Lernerfolge für verschiedene Zielgruppen zu ermöglichen“ (ebd., S. 80). Bemerkenswert ist, dass bei den Teilnehmenden mit einer höheren Ausprägung der Ausbildung eine Abschwächung des Effektes erkennbar ist, sodass eine abnehmende Abschwächung des Effektes mit zunehmender Bildung unterstellt werden kann – allerdings nur zwischen Berufs- und Universitätsausbildung. Damit wird deutlich, dass Bildungsangebote in dieser Form aus dem Blickwinkel der Mittelschicht konzipiert werden können und Wirkungen zeigen, damit jedoch nicht den Bedarfen der Gesamtgesellschaft entsprechen (Ribolits 2006). Besteht der Anspruch, präventive Maßnahmen im Kontext von Cybercrime für Teilnehmende mit einer Hochschulausbildung zu fokussieren, die die Selbstwirksamkeit stärken und nicht schwächen, ist eine andere Konzipierung unabdingbar.

7.1.6 Moderation der AV durch das Geschlecht

Die Betrachtung des Geschlechts als Moderator zeigt im Prä-Post-Follow-up-Vergleich, dass sich eine hoch signifikante Beziehung zwischen dem Geschlecht und dem Prädiktor Selbstwirksamkeit im Kontext IT-Sicherheit der Teilnehmer in der EG und KG zeigt, während dies für die Teilnehmerinnen nicht gilt. Männer mögen leichter den Zugang zur Technik finden (Schiersmann 1987), z.B. aufgrund der sozialisationsbedingten Geschlechterdifferenzierung (Kahlert & Mischau 2000), werden jedoch in der Selbstwirksamkeit im Kontext IT-Sicherheit negativ beeinflusst. Bei den Teilnehmern ist der Koeffizient nicht nur signifikant, sondern auch negativer als bei den Teilnehmerinnen. Vergeschlechtlichte Erschließungsprozesse, die Teilnehmern die Selbstwirksamkeit im Kontext IT-Sicherheit ermöglichen, bedürfen im Prozess der Konzipierung von präventiven Maßnahmen daher einer besonderen Beachtung. Konzipierungen dieser Art sind in der Praxis jedoch schwierig. Hilfsmittel wie das von Blickhäuser und Bargen (2008) entwickelte „Fit for Gender Mainstreaming“ mögen einen ersten Einstieg in die gendersensible Konzipierung liefern, werden jedoch von Budde und Venth (2010) kritisch gesehen, da auf diese Weise Stereotype in die Konzeption einfließen können. Andere Lösungsvorschläge legen Gindl und Hefler (2006, S. 1) vor, die „gendersensible Didaktik nicht als die Anwendung bestimmter Methoden oder Inhalte, sondern als eine bewusste Erweiterung der Aufmerksamkeit auf alle Fragen, die sich im Zusammenhang mit dem Geschlechterverhältnis in der Gestaltung von Lernprozessen ergeben“, ansehen. Beide Autoren verweisen bezüglich der geschlechtersensitiven Didaktik auf grundlegende Aspekte, die auch in der allgemeinen Didaktik zu finden sind (z.B. auf den Zugang zu bestehenden Ressourcen und das Schaffen von Lernmöglichkeiten), und erweitern diese durch Genderintegrität und Genderkompetenz. Die Antwort auf die Frage, welche

Methoden genau wirkungsvoll sind, bleiben die Autoren jedoch schuldig, sodass weitere Forschungen hierzu erforderlich sind.

7.1.7 Die Bedeutung des VersuchsleiterInnenartefakts

Werden Forschungsdaten im Feld durch die Versuchsleiterin oder den Versuchsleiter selbst erhoben, sind die Forschungsergebnisse ggf. verzerrenden Beeinflussungen ausgesetzt. Um diesen Effekt zu beachten, wurden in der Untersuchung zwei Lehrende eingesetzt, die zu diesem Zeitpunkt den gleichen akademischen Grad besaßen. In der Moderatoranalyse zeigte sich, dass die Lehrenden in diesem Fall jedoch keinen Einfluss auf das Forschungsergebnis hatten. Damit kann davon ausgegangen werden, dass die analysierte Wirkung unabhängig von den Dozierenden ist. Diese Überprüfung war essentiell, da sie zu den Gütekriterien der Validität zählt, die Bortz und Döring (2006, S. 83) wie folgt beschreiben: „Eine Maßnahme, die die Beeinträchtigung der internen Validität von Untersuchungen durch Versuchsleiterartefakte in Grenzen hält, ist die Standardisierung der Untersuchungsbedingungen und vor allem des Versuchsleiterverhaltens“.

7.2 Methodendiskussion

Die Methodendiskussion behandelt die wichtigen Aspekte des Themas dieser Arbeit. Hierzu wird die konzipierte präventive Maßnahme final reflektiert und einer kritisch-konstruktiven Diskussion unterzogen. Eine Reflexion des hier verschriftlichten methodischen Vorgehens wird anhand der einzelnen Schritte vorgenommen.

7.2.1 Entwicklung der präventiven Maßnahme

Die Konzipierung einer präventiven Maßnahme ist ein aufwendiger Prozess, der didaktische Methoden in den fachlichen Kontext von Cybercrime setzt. Dabei gilt es, die Zielgruppe sowie die vorhandenen praktischen und rechtlichen Rahmenbedingungen zu berücksichtigen bzw. einzuhalten. Denn eine adressatInnenorientierte Medienkompetenzvermittlung für Erwachsene kann nur gelingen, wenn einschlägige Theorien mit aktuellen Studien in Relation gesetzt und bei der Konzipierung beachtet werden. Die unterschiedlichen Forschungsergebnisse zu der Frage, wie ein sicherheitskonformes Verhalten möglich wird, sind durch die diversen Forschungsergebnisse im Kontext Sensibilisierung und Cybercrime zu ergänzen und in dieser Arbeit auch herausgehoben.

Die Konzipierung der evaluierten Maßnahme erfolgte nach didaktischen Prinzipien in Anlehnung an das SETA-Framework (Whitman & Mattord 2017). Wie bereits im Abschnitt zu dem Elaboration-Likelihood-Modell erläutert wurde, weisen Jonas, Stroebe und Hewstone (2014) darauf hin, dass RezipientInnen die Argumente, die in einer Präsentation enthalten sind, kritisch überprüfen, was durch die Verarbeitungsmotivation und

durch die Verarbeitungsfähigkeit bedingt ist. Um die bei den Teilnehmenden vorhandene Verarbeitungsfähigkeit nicht zu überfordern und an vorhandenes Vorwissen anschließen zu können, wurden einfache Cyberangriffe ausgewählt, präsentiert, Gegenmaßnahmen besprochen und in der Experimentalgruppe auch trainiert. Die Erfordernis eines Trainings ergab sich unter anderem aus dem Modell der Elaborationswahrscheinlichkeit, das voraussagt, dass eine Persuasion, die auf einer systematischen Verarbeitung (d.h. auf der zentralen Route) beruht, beständiger ist als eine Persuasion, die durch eine periphere oder heuristische Verarbeitung induziert wird (Jonas et al. 2014; siehe auch Tabelle 8).

Bei der Kommunikation mit den Teilnehmenden wurde darauf geachtet, mittels der Präsentation aktueller Fakten abgesicherte Argumente einfließen zu lassen (siehe Abbildung 3). Eine abschließende Evaluation (siehe Anhang 11) zeigte, dass die Maßnahme von den Teilnehmenden als gelungen angesehen wurde.

Bemerkenswert ist, dass den Befunden zufolge ein sehr kurzes Training eine Wirkung erzielen kann und darüber hinaus dazu beiträgt, dass sich Faktoren wie Einstellungen und Selbstwirksamkeit im Kontext von IT-Sicherheit nicht weiter verschlechtern, und dass sich, wenn ein Training zu kurzgefasst ist, Werte der Kontrollüberzeugung auch verschlechtern können. Die erhobenen Daten weisen zudem darauf hin, dass präventive Maßnahmen ohne Training zu IT-Sicherheitsrisiken zu unbekannten Nebenwirkungen führen können. Sollten sich diese Ergebnisse generalisieren lassen, so ist von „HackerInnenshows“ ohne anschließendes Training dringend abzuraten.

Ableitung fachdidaktischer Prinzipien

> „Ein rein theoretisches Problem – ein Problem der reinen Wissenschaft – besteht immer darin, eine Erklärung zu finden – die Erklärung einer Tatsache oder eines Phänomens oder einer merkwürdigen Regelmäßigkeit oder einer merkwürdigen Ausnahme“ (Popper 1999, S. 136).

Fachdidaktische Ableitungen sind für PraktikerInnen essenziell, um wirkungsbezogene Vorüberlegungen anstellen zu können.

Die Möglichkeit, exemplarische, gegenwartsbezogene und zukunftsbedeutende Inhalte auswählen zu können und auch simulieren zu dürfen,[46] lässt laut Schröder (2002) einen horizontalen und vertikalen Transfer zu, also eine Übertragung von einem Sachverhalt auf einen anderen Sachverhalt sowie eine Übertrag des Sachverhaltes auf sinnvolle Problemlösungen. Bezogen auf das hier behandelte Thema wird es daher mit einer präventiven Maßnahme für die Teilnehmenden im besten Fall möglich, Analogien

[46] Diese Möglichkeit besteht, solange dies auf einer privaten Infrastruktur erfolgt.

anhand von unterschiedlichen Cyberangriffen zu erkennen und erlernte Schutzmaßnahmen auf konkrete Fälle zu adaptieren. Um entsprechende Beispiele vortragen zu können, bedarf es neben der technischen Kompetenz der bzw. des Dozierenden einer Sequenzierung von sinnvoll aufeinander aufbauenden Lerninhalten, die von den Teilnehmenden erkannt werden muss. Reich (1977, S. 41) weist in diesem Zusammenhang darauf hin, dass diesbezüglich allerdings keine allgemeingültige Abfolge gegeben werden kann: „Es gibt sozusagen keine eindeutige Reihen- oder Bestimmungsfolge der am Unterricht beteiligten Faktoren, so dass die Ableitung der didaktischen Grundlagen aus bestimmten kausal hergeleiteten Sachzusammenhängen unmöglich ist“. Eine weitere Perspektive führt Klafki (1964) an, der die Bedeutung des Inhaltes für die Lernenden in den zu betrachtenden Fokus zieht (vgl. dazu Kapitel 2.5.2). Beispiele von Cyberangriffen sind demzufolge so auszuwählen, dass Bedrohungen von Cyberkriminellen fokussiert werden und den Teilnehmenden deutlich wird, dass sie selbst möglicherweise betroffen sein könnten. Solche zukunftsbezogenen Bedeutungen einzubeziehen, ist zwar schwierig, jedoch nicht unmöglich, denn Sicherheitsvorfälle sind in den meisten Fällen eine „Blaupause“ für weitere Sicherheitsvorfälle. Haben die Teilnehmenden das technische Konstrukt eines Sicherheitsvorfalls verstanden, sind also auch adaptive Fokussierungen möglich. Hierzu ist es erforderlich, eine kognitive Auseinandersetzung stattfinden zu lassen, die Prochaska und Prochaska (2016) in der zweiten Phase der Metaperspektive der Teilnehmenden verankern und die Eagly und Chaiken (1993) im HSM-Modell deutlich machen, wie es im Kapitel 2.3.2 deutlich wurde.

7.2.2 Untersuchungsdurchführung

Für die Durchführung der präventiven Maßnahme waren der Autor dieser Arbeit und eine weitere Dozentin verantwortlich. Dabei zeigte sich auf der Grundlage der Befunde in der Wirksamkeit der Maßnahme kein Unterschied zwischen den beiden Dozierenden, sodass die Durchführungsobjektivität als gegeben angesehen werden kann.

In der vorliegenden Untersuchung standen Faktoren der Verhaltensänderung und deren positive Beeinflussung durch die Teilnahme an der Präventionsmaßnahme im Fokus. Diese Faktoren sind unter anderem Bestandteil der Theorie des überlegten Handelns von Ajzen und Fishbein (1980). In dieser Theorie werden weitere Faktoren identifiziert, die das Verhalten beeinflussen können, etwa soziale Normvorstellungen oder die Bewertung der Konsequenzen. Es hätte jedoch den Rahmen dieser Arbeit überzogen, alle Einflussfaktoren auf die Verhaltensänderung zu untersuchen. Deshalb wurde der Fragebogen durch eine Fokussierung auf bestimmte Aspekte in einem akzeptablen Umfang für die Teilnehmenden gehalten.

Im Prozess der Erhebung zeigte sich zunächst, dass die Beantwortung der Fragen zur allgemeinen Selbstwirksamkeit Misstrauen erweckte. Hier kamen bei den Teilnehmern und Teilnehmerinnen Bedenken auf, dass Angaben zur allgemeinen Selbstwirksamkeit in andere Kontexte gesetzt und somit missbraucht werden könnten. Diesem Misstrauen konnte jedoch begegnet werden, indem die abgegebenen Fragebögen jeweils in andere Stapel von Fragebögen gelegt wurden und indem durch den Dozierenden und die Dozierende explizit auf die Anonymität der Befragung und Datenauswertung hingewiesen wurde. Die Teilnehmenden hatten genügend Zeit, die Fragebögen zu beantworten, da diese vor und nach der Veranstaltung bearbeitet wurden und sich die Beschäftigung mit den Fragebögen somit nicht auf die Veranstaltungslänge auswirkte. Dadurch wurde allen Teilnehmenden die Möglichkeit geboten, alle Fragen beantworten zu können. Zusätzlich wurden die Teilnehmenden nach der Erhebung der Daten gebeten, die Vollständigkeit ihres Fragebogens zu prüfen. Tatsächlich führten diese Maßnahmen dazu, dass in den Fragebögen kaum fehlende Werte zu finden waren, wobei die wenigen fehlenden Werte auf die fehlerhafte Beantwortung der Fragen zurückzuführen waren (Kreuze über statt in den vorgesehenen Kästchen). Fragebögen von Teilnehmenden, die älter als 67 und jünger als 18 Jahre waren, wurden aussortiert und in den Analyseprozess nicht einbezogen.

Am dritten Messzeitpunkt, der 30 Tage nach der Teilnahme an der Maßnahme stattfand, wurde der Fragebogen jedoch nicht von allen Teilnehmenden ausgefüllt. Positiv wirkte es sich auf die Rücklaufquote allerdings aus, dass Veranstaltungen, die mit den gleichen Teilnehmenden in einem anderen Kontext (Vereine, Selbsthilfegruppen) stattfanden, zur letzten Datenerhebung genutzt werden konnten.

Die Datenerhebung, ursprünglich als Online-Erhebung konzipiert,[47] zeigte im ersten Prä-Test praktische Schwächen. So waren PCs nicht vorhanden und die Nutzung der privaten Kommunikationsmittel wie Smartphones hätte den Aufwand für die Datenerhebung weiter erhöht.

Das Sample umfasst eine große Bandbreite der unterschiedlichsten Bevölkerungsschichten und kann somit als gelungene Auswahl angesehen werden. Die Fragebögen wurden gemäß den Empfehlungen von Moosbrugger und Kelava (2012) im Vorfeld auf leichte Verständlichkeit, einfache Durchführbarkeit und kurze Lösungszeit überprüft. Die leichte Verständlichkeit wurde dadurch erreicht, dass auf Verneinungen (und doppelte Verneinungen) in den Fragestellungen sowie auf Fachtermini aus der Welt der IT-Sicherheit verzichtet wurde. Fragen, die Wertungen enthalten, wurden ebenso vermieden wie das partikulare Zulassen von auf Vorwissen beruhenden Antwortmöglichkeiten.

[47] Diese ist im Internet einsehbar unter: http://www.educationcamp.de/testfragen/.

7.2.3 Auswertung der Daten

Bei der Auswahl der statistischen Methoden wurde darauf geachtet, dass übliche statistische Verfahren für statistische Fragestellungen genutzt wurden. Die Priorität lag in der Vermeidung der Gefahr einer Alphafehlerkumulierung bzw. einer Inflation des Alphafehlers. Hierzu wurde das Verfahren der Varianzanalyse mit Messwiederholung genutzt. Auf den Einsatz nichtparametrischer Tests wurde hingegen bewusst verzichtet, da die Stichprobengröße als ausreichend angesehen werden kann.

In der Darstellung der Ergebnisse wurde auch die Entwicklung zwischen dem Messzeitpunkt t1 und dem Messzeitpunkt t2 skizziert. Diese Analyse besitzt zwar nach König (2018) keine Relevanz, um Entwicklungslinien statistisch abbilden, jedoch eine praktische Signifikanz, die den Lehrenden deutlich machen kann, dass Auswertungen vor und nach Veranstaltungen für die Interpretation von Entwicklungen unzureichend sein können, wenn ein dritter Messzeitpunkt nicht implementiert wird. Um die Beeinflussung unterschiedlicher Variablen zu überprüfen, wurde das PROCESS Makro genutzt, das diverse Einstellungsmöglichkeiten und die Funktionalität besitzt, unterschiedliche Heteroskedastizität-Schätzer auszuwählen und zu benutzen. Für die Moderation wurde der HCSE-Schätzer HC3 gewählt, der der Empfehlung von Hayes (2018) entspricht.

Ein wesentliches Ziel der gewählten quantitativen Vorgehensweise war es, geeignete Messinstrumente zu entwickeln oder zu benutzen, die das, was gemessen werden sollte, auf einer (numerischen) Skala so genau wie möglich abbildeten (Schäfer 2016). Hierzu wurde in der vorliegenden Untersuchung primär auf vorhandene Messinstrumente (Fragebögen) zurückgegriffen, um die Validität und Reliabilität abzusichern. Um die Variablen

- Einstellung,
- Kontrollüberzeugung,
- Selbstwirksamkeit im Kontext von IT-Sicherheit und
- themenbezogene/nicht themenbezogene Teilnahme

zu operationalisieren, wurde hingegen ein neues Messinstrument genutzt, da zu diesen Themen keine bekannten Messinstrumente im Kontext Cybercrime existierten.

Die gewählten Skalen wurden für alle zu operationalisierenden Variablen als fünfstufige Likert-Skala ausgelegt, deren Abstände zwischen den Kategorien als gleich groß interpretiert werden können (Urban & Mayerl 2011) und in deren Rahmen eine geringe Anzahl als bedenklich angesehen wird (Lloret-Segura et al. 2014). Denn zwar weist von Berry (1993, S. 47) darauf hin, dass bei fünf oder weniger Abstufungen nicht von metrischen Daten ausgegangen werden kann:

> “In particular, when a quantitative ordered discrete variable takes on a wide range of values (as does the number of employees in an organization), it is probably reasonable to treat the variable as if it were continuous. In contrast, it is clearly

> inappropriate to treat any ordered discrete variable with a small number of values (say, five or fewer) as continuous.",

Doering und Bortz (2016) verweisen jedoch auf die Demotivation und Anstrengung für die Untersuchungspersonen, die bei zu vielen Antwortmöglichkeiten entstehen können, und empfehlen für eine psychometrische Kurzskala eine drei- bis fünfstufige Unterteilung.

Eine Betrachtung der Validität, verbunden mit der Frage, ob ein Messinstrument tatsachlich das misst, was es messen soll, wird zum „Ausdruck für die Angemessenheit der Operationalisierung eines Begriffs" (Alemann 1977, S. 85) oder eines theoretischen Konstrukts.[48] Das bedeutete für die Untersuchung, ein valides Messinstrument einzusetzen. Die Auswahl einer manifesten Variablen, die ein theoretisches Konstrukt repräsentiert bzw. indiziert, wird als Operationalisierung bezeichnet (Fahrenberg 2002), die als Vorschrift fungiert, wie theoretischen Begriffen bestimmte beobachtbare Sachverhalte zugeordnet werden können (Stoetzer 2017), und die letztendlich eine Überführung des empirischen Relativs in ein numerisches Relativ darstellt[49] (Schäfer 2016). Eine theoretische Dimensionsbildung ist zwar prinzipiell möglich (Burzan 2008), sollte jedoch durch eine Faktorenanalyse abgesichert werden (Kuß & Eisend 2010). Hierzu wurden in dieser Arbeit der Scree-Test nach Cattell (1966) und zusätzlich die Parallelanalyse nach O'Connor (2000a) gewählt, die zu gleichen Ergebnissen kommen.

Fahrenberg (2002, S. 352) weist weiter darauf hin, dass Definitionen durch die Auswahl von unabhängigen bzw. abhängigen Variablen sowie durch die Verwendung von bestimmten Untersuchungsparadigmen per fiat („so sei es") erfolgen und diesbezüglich fehlerbehaftet sind. Typische Fehler nach Fahrenberg sind bereits im Kapitel 4.11 beschrieben worden. Um diese Fehler zu minimieren, wurde bei der Formulierung der im Fragebogen enthaltenden Items darauf geachtet, dass die Bedeutung des Konstrukts mit den verwendeten Variablen getroffen wird. Zudem wurde geprüft, ob die Variablen selbst jeweils auch tatsächlich inhaltlich zum Konstrukt gehören. Eine darauffolgende statistische Überprüfung der internen Konsistenz erfolgte durch die Ermittlung und Angabe der statistischen Messgröße $\alpha = .64$, die jedoch nur durchschnittlich ist.

Die Untersuchung des neu eingesetzten Messinstruments zeigt, dass sich die Faktorladungen durch zwei unterschiedliche Verfahren abgrenzen und durch die Zuweisung von fokussierten Skalen überwiegend untersetzen lassen, sodass von einem validen

[48] „Konstrukte sind Begriffe, die theoretisch sinnvoll erscheinen, um etwas Interessantes zu beschreiben, was nicht direkt beobachtbar oder messbar (also latent) ist und erst durch andere Variablen erschlossen werden muss" (Schäfer 2016, S. 21).

[49] In der Psychologie wird dieses Problem der Überführung als Repräsentationsproblem bezeichnet (Bortz & Doering 2009; Kähler 2004).

Messinstrument ausgegangen werden kann. Gleichwohl sollte seine Reliabilität in weiteren Studien überprüft werden, damit die statistische Messgröße α untersetzt wird. Die Erhebung der Daten fand zu allen Messzeitpunkten in schriftlicher Form statt, was ökonomischer und darüber hinaus unabhängiger von den Befragungsleitenden ist als eine mündliche Befragung (Sedlmeier & Renkewitz 2013). Die Entkopplung eines möglichen VersuchsleiterInneneffektes wurde dadurch erreicht, dass zwei Dozierenden die präventive Maßnahme durchführten.

8 Fazit und Ausblick

> „There is a growing belief that awareness training is so ineffective that it shouldn't even be performed at all" (Watson, Mason & Ackroyd 2014, S. 341).

Aktuelle Entwicklungen zeigen auf, dass die mangelnde Aufmerksamkeit der meisten Internetnutzenden beim Thema Informationssicherheit gravierende Auswirkungen haben können. Denn es gilt: Jede/r, die/der digitale Medien nutzt, kann von Cyberangriffen betroffen sein. Wird eine adressatInnenorientierte Medienkompetenz definiert und behandelt, bleibt jedoch allzu oft die Informationssicherheit unberücksichtigt (Lange & Bötticher 2015). Der Glaube, allein durch Sanktionen, niedergeschrieben in Sicherheitsleitlinien, und durch Wissen über Gefahren sicherheitskonformes Verhalten absichern zu können, ist unrealistisch, wie die internationalen Studien, die im Kapitel 2.3.10 behandelt wurden, zeigen. Präventive Maßnahmen sind hingegen ein möglicher Schritt in die Richtung eines bewahrpädagogischen Ansatzes für Erwachsene, um Einstellungen und Selbstwirksamkeit im Kontext von IT-Sicherheit zu verbessern und letztendlich ein sicherheitskonformes Verhalten möglich werden zu lassen.

Die Erklärung von Verhaltensweisen, die als sicherheitskonform eingestuft werden können, hängt von vielen Variablen ab. Ein Versuch, diese durch Operationalisierung „einzurahmen", kann durch unterschiedliche Theorien bereits heute vorgenommen werden. In dieser Arbeit konnte gezeigt werden, dass wichtige Variablen, um sicherheitskonformes Verhalten zu gewährleisten, in unterschiedlichen Richtungen durch präventive Interaktionen veränderbar sind. Bemerkenswert ist, dass sich operationalisierte Variablen eines sicherheitskonformen Verhaltens durch präventive Maßnahmen in beide Richtungen verändern können und dass damit auch unerwünschte Seiteneffekte eintreten, die eine kontraproduktive Wirkung haben können. So zeigte sich, dass Selbstwirksamkeit im Kontext von IT-Sicherheit nicht nur verstärkt, sondern auch geschwächt werden und darüber hinaus vom Bildungsgrad und Geschlecht moderiert werden kann. Präventive Maßnahmen vorab auf ihre Wirksamkeit zu überprüfen, sollte daher zu einem festen Bestandteil evidenzbasierter präventiver Maßnahmen werden. Denn auch wenn die Ergebnisse in den möglichen Dimensionen zurückbleiben, zeigt sich die Wirksamkeitsbandbreite einer präventiven Maßnahme im Kontext von Cybercrime, wenn Präsentationen didaktisch geplant und durch Trainings komplettiert werden.

Da Erkenntnisse im hermeneutischen Sinne stets zu weiteren Fragestellungen führen, wirft auch diese Arbeit zwangsläufig neue Fragestellungen auf. Praxisbezogen relevant wäre zu überprüfen, inwieweit die operationalisierten Variablen ein tatsächliches Verhalten im Kontext von Cybercrime beeinflussen und inwieweit dieses persistent beibehalten wird. Die Theorie von Prochaska und Diclemente (1983), welche im Kapitel

2.3.9 behandelt wurde, zeigt bereits auf, dass Verhalten, das länger als sechs Monate beibehalten wird, auch langfristig beibehalten wird. Zukünftige Forschungsergebnisse[50] könnten darüber Auskunft geben, ob bzw. inwieweit eine zyklische Wiederholung von präventiven Maßnahmen in der Lage ist, persistentes Verhalten, das sicherheitskonform ist, abzusichern. Eine solche festgelegte Regelmäßigkeit von Datenschutzunterweisungen findet sich bis heute jedoch kaum in Gesetzen. In den Empfehlungen des BSI bleiben sie auf ein „sollte“ ohne Training reduziert (BSI 2019). Sind keine Forschungsergebnisse vorhanden, bleibt daher eine erforderliche zeitliche Sequenzierung von präventiven Maßnahmen ungewiss – mit der Konsequenz eines unbekannten Verhaltens und dessen Persistenz. Die Folgen sind bekannt und zeigen sich durch nonkonformes Verhalten im Kontext der IT-Sicherheit und in den damit verbundenen möglichen Sicherheitsvorfällen. Ergänzend ist darauf hinzuweisen, dass das Lebenslange Lernen vorwissengeleitet ist und präventive Maßnahmen einen Beitrag in diese Richtung leisten können. Weinberg (2004) weist in diesem Zusammenhang darauf hin, dass die Lernenden primär einsehen müssen, dass es etwas zu lernen gibt, das zwar unbekannt, aber auch wert ist, gelernt zu werden. Real dargestellte Cyberangriffe besitzen das Potenzial, technischen Cybercrime erlebbar zu machen und in diesem Sinne dazu beizutragen, dass Angriffe erfolglos verlaufen. Denn: „An attack event will not be successful if the victim is stronger than the attacker in Infrastructure and Capability“ (Al-Mohannadi et al. 2016, S. 76). Die Auseinandersetzung mit Schutzmaßnahmen versetzt die Teilnehmenden in die Lage, über die Behandlung von möglichen Sicherheitsdefiziten durch die Nutzung digitaler Medien entscheiden zu können und eigene Konsequenzen zu reflektieren. Sind derartige Konstellationen hingegen nicht bekannt, kann eine Entscheidung nur noch für die Zukunft getroffen werden. Gerade technisch weniger versierte Menschen sind sich dieser Gefahren oft nicht bewusst.

Sonderpädagogische Unterstützung und Bildung, um auch Menschen mit Behinderung einen Zugang zu und die Teilhabe an der Medienvielfalt zu ermöglichen, kann nur gelingen, wenn technische Komplexität nicht delegiert, sondern die Kompliziertheit aufgelöst wird, damit bewahrpädagogische Medienbildung stattfinden und weitergegeben werden kann. Findet diese Unterstützung nicht statt, verschärft sich die Ausgrenzung von Menschen, die es nicht aus eigener Kraft schaffen, im digitalen Zeitalter Schritt zu halten. Es gilt somit, die Bedeutungshaftigkeit zum Unterrichtsgegenstand ‚IT-Sicherheit‘ zu entwickeln, die zukunftsorientiert sinnvoll ist und damit das Verständnis pädagogischer Professionalität plakatiert (Handwerk 2020). Medienkompetenz, die erforderlich ist, um die Digitalisierung im Bildungsbereich weiter voranzutreiben (Langner 2019), zu

[50] Diese könnten bspw. durch Screening-Verfahren gewonnen werden.

erlangen, ohne jedoch ein Verständnis für IT-Sicherheit zu haben, lässt eine Fokussierung auf die Verfügbarkeit entstehen, die unzureichend ist, jedoch holistisch[51] erforderlich wird, wenn digitale Medien zum Einsatz kommen sollen. Wird dies ebenfalls nicht beachtet, verschärft sich die digitale Kluft zwischen Menschen mit und ohne Behinderungen, die ohnehin aufgrund der langsamen Entwicklung zugänglicher unterstützender Technologien, digitaler Plattformen und elektronischer Schulungen bereits vorhanden ist (Hamburg & Lütgen 2019).

[51] Ein „Ausfall“ des WLAN-Netzes ist bereits ausreichend, um digitale Bildungsmaßnahmen massiv zu stören.

Literaturverzeichnis

Abawajy, J. (2012). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology – Behaviour & IT*, 33. 239

Abels, S. (2011). *LehrerInnen als „Reflective Practitioner", Reflexionskompetenz für einen demokratieförderlichen Naturwissenschaftsunterricht*. Wiesbaden: Springer VS

Abts, D. & Mülder, W. (2017). *Grundkurs Wirtschaftsinformatik: Eine kompakte und praxisorientierte Einführung*. Wiesbaden: SpringerVieweg

ADV-Arbeitsgemeinschaft (2016). Leitfaden zur Prüfung eines Internetauftritts. Veröffentlicht unter: *https://studylibde.com/doc/8312167/leitfaden-zur-prüfung-eines-internetauftritts* (heruntergeladen am 28.06.2019)

Africa-University (2019). website. Veröffentlicht unter: *http://www.africau.edu/images/* (heruntergeladen am 23.06.2020)

AG Frankfurt/Main, 17.02.2016 - 380 C 2838/15 (75)

AG Frankfurt/Main, 24.03.2016 - 32 C 3377/15 (72)

Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. In: Kuhl, J. & Beckmann, J. (Hrsg.). *Action control: From cognition to behavior.* Berlin: Springer. S. 11-39

Ajzen, I. (2001). Nature and Operation of Attitudes. *Annual review of psychology,* 52(02). 37

Ajzen, I. (2005). *Attitudes, Personality, and Behavior*. Berkshire: Open University Press

Ajzen, I. (2015). Consumer attitudes and behavior: the theory of planned behavior applied to food consumption decisions. *Rivista di Economia Agraria*, 70(01). 122

Ajzen, I. & Fishbein, M. (1980). *Understanding Attitudes and Predicting Social Behavior*. New Jersey: Prentice-Hall

Albrecht, F. (2018). *Informations- und Kommunikationsrecht: Lehrbuch für das gesamte IT-Recht*. Stuttgart: Kohlhammer

Ali, M. M. (2016). Determinants of Preventing Cyber Crime: a Survey Research. Veröffentlicht unter: *https://researchleap.com/wp-content/uploads/2016/08/Determinants-of-Preventing-Cyber-Crime-a-Survey-Research.pdf* (heruntergeladen am 21.12.2019)

Allgeier CORE Group GmbH (2020). Die Hacker kommen. Veröffentlicht unter: *https://die-hacker-kommen.de/* (heruntergeladen am 17.02.2020)

Al-Mohannadi, H., Ali Mirza, Q. K., Namanya, A. P., Awan, I., Cullen, A. & Pagna Diss, J. (2016). *Cyber-Attack Modeling Analysis Techniques: An Overview*. Vienna: IEEE.

Alsbih, A. & Mentel, J. (2019). Cyberkriminalität: Abwehrstrategien gegen neue Bedrohungsszenarien. Veröffentlicht unter: *https://www.tecchannel.de/archiv/pdf_tco/2019/leseprobe_01.pdf* (heruntergeladen am 23.08.2020)

Ammon, S. (2006). *Commitment, Leistungsmotivation, Kontrollüberzeugung und erlebter Tätigkeitsspielraum von Beschäftigten in Unternehmen und Behörden im Vergleich*. Berlin: Lit

Anding, A. (2002). *Bildung im Alter:* Bildungsinteressen und -aktivitäten älterer Menschen. Beitrag zur Bildungstheorie des Alters. Leipzig: Ille & Riemer

Andric, T. (2017). *The Complete Cyber Security Course*. Volume I: Hackers Exposed. Isleworth: StationX Ltd.

Årnes, A. (2018). *Digital Forensics*. Hoboken, New Jersey: John Wiley & Sons

Arnold, R. (2007). *Ich lerne, also bin ich*: Eine systemisch-konstruktivistische Didaktik. Heidelberg: Carl Auer

Arnold, W., Eysenck, H. J. & Meili, R. (1971). *Lexikon der Psychologie*. Freiburg im Breisgau: Herder

Aufenanger, S. (2001). Multimedia und Medienkompetenz – Forderungen an das Bildungssystem. In: Aufenanger, S., Schulz-Zander, R. & Spanhel, D. (Hrsg.). *Jahrbuch Medienpädagogik 1.* Wiesbaden: VS Verlag für Sozialwissenschaften. S. 119-120

Aulerich, G., Burow, A. O., Fischer, E., Keiser, S. & Schicke, H. (2004). *Kompetenzorientierte Lerngestaltung:* Ein Konzept zur Personalentwicklung und Professionalisierung in Weiterbildungseinrichtungen. Berlin: Arbeitsgemeinschaft Betriebliche Weiterbildungsforschung e. V./Projekt Qualifikations Entwicklungs-Management

Autorengruppe Bildungsberichterstattung (2016). *Bildung in Deutschland 2016*. Bielefeld: Bertelsmann Verlag

Avast (2016). Avast Wi-Fi Hack Experiment Demonstrates “Reckless” Behavior of Mobile World Congress Attendees. Veröffentlicht unter: *https://press.avast.com/en-us/avast-wi-fi-hack-experiment-demonstrates-reckless-behavior-of-mobile-world-congress-attendees* (heruntergeladen am 15.06.2018)

Baacke, D. (1996). Medienkompetenz als Netzwerk. Reichweite und Fokussierung eines Begriffs, der Konjunktur hat. *Medien praktisch*, 20. 8

Backhaus, K., Erichson, B., Plinke, W. & Weiber, R. (2016). *Multivariate Analysemethoden* (14. Aufl.). Berlin: Springer Gabler

Baeriswyl, F. (2013). Einführung in die Pädagogische Psychologie II, FS_ Vorlesung 19: Selbstkonzept und Attributionen. Veröffentlicht unter: *www.common-web.unifr.ch/artsdean/pub/gestens/f/as/files/4655/28547_092249.pdf* (heruntergeladen am 05.08.2018)

Bahrick, H. P., Bahrick, P. O. & Wittlinger, R. P. (1975). Fifty years of memory for names and faces: A cross-sectional approach. *Journal of Experimental Psychology: General*, 104(1). 54-75

Balci, E. (2016). Keylogger. Veröffentlicht unter: *https://github.com/EgeBalci/Keylogger* (heruntergeladen am 06.08.2018)

Bandura, A. (1976). *Lernen am Modell*. Stuttgart: Klett

Bandura, A. (1977). *Social Learning Theory*. New York: General Learning Press

Bandura, A. (1979). *Sozial-kognitive Lerntheorie*. Stuttgart: Klett-Cotta

Bandura, A. (1991). Self-Regulation of Motivation Through Aticipatory and Self-Reactive Mechanisms. In: Dienstbier, R. A. (Hrsg.). *Perspectives on motivation.* (Bd. 38). Lincoln: University of Nebraska Press. S. 70-80

Bandura, A. (1994). Self-efficacy. Veröffentlicht unter: *https://www.uky.edu/~eushe2/Bandura/Bandura1994EHB.pdf* (heruntergeladen am 20.04.2019)

Bandura, A. (1997). *Self efficacy*: The exercise of control. New York: Freeman

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. Veröffentlicht unter: *http://firstmonday.org/article/view/1394/1312* (heruntergeladen am *12.01.2018*)

Bartels, K. (1996). *Was die Philologen lieben.* 27 Wortgeschichten. Darmstadt: Wissenschaftliche Buchgesellschaft

Bartz, H. & Tippelt, R. (2004). Weiterbildung und soziale Milieus in Deutschland. Bielefeld: Bertelsmann. S. 13

Bässmann, J. (2015). Täter im Bereich Cybercrime: Eine Literaturanalyse. Veröffentlicht unter: *https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/Publikationsreihen/Forschungsergebnisse/2015TaeterImBereichCybercrime.pdf* (heruntergeladen am 20.04.2019)

Beck, E., Baer, M., Guldimann, T., Bischoff, S., Brühwiler, C. & Müller, P. (2008).

Adaptive Lehrkompetenz. Münster: Waxmann

Becker, A. S. & Mahler, T. (2019). Wie Forscher Cyberangriffe verhindern wollen. *kma - Klinik Management aktuell*, 24(01). 70-71

Becker, L. (2019). Telefonbetrug: Apple-Support-Rufnummer soll Kunden täuschen. Veröffentlicht unter: *https://www.heise.de/mac-and-i/meldung/Telefonbetrug-Apple-Support-Rufnummer-soll-Kunden-taeuschen-4267143.html%0A* (heruntergeladen am *12.01.2020*)

Beer, R. (2016). Dimensionsreduktion - Hauptkomponentenmethode. In: Schwertz, H., Beer, R., Benischek, I. & Forstner-Ebhart, A. (Hrsg.). *Einführung in das qualitativ orientierte Forschen* (4. Aufl.). Wien: Facultas. S. 78-86

Behnke, J. (2015). *Logistische Regressionsanalyse.* Eine Einführung. Wiesbaden: Springer

Beise, M. & Schäfer, U. (2016). *Deutschland digital*: Unsere Antwort auf das Silicon Valley. Frankfurt am Main: Campus

Bekemeier, M. (2011). Qualitätsanforderungen an Weiterbildnerinnen und Weiterbildner. In: Weiterbildungsinitiative Frühpädagogische Fachkräfte (Hrsg.): *Kinder in den ersten drei Lebensjahren* (Band 2). Bad Heilbrunn: WiFF Wegweiser Weiterbildung. S. 136-144

Benenson, Z., Gassmann, F. & Landwirth, R. (2016). Unpacking Spear Phishing Susceptibility. Veröffentlicht unter: *http://www.cl.cam.ac.uk/%7B~%7Drja14/shb17/benenson.pdf* (heruntergeladem am 20.05.2019)

Benenson, Z., Landwirth, R. & Gassmann, F. (2016). Exploiting Curiosity and Context. Veröffentlicht unter: *https://pdfs.semanticscholar.org/055f/50567fff4d17ef0f6f6a8921d353f096c7d2.pdf* (heruntergeladen am *12.01.2018*)

Benson, V. & McAlaney, J. (2019). *Cyber Influence and Cognitive Threats*. London: Academic Press

Berg, A. & Niemeier, M. (2019). Wirtschaftsschutz in der digitalen Welt. Veröffentlicht unter: *https://www.bitkom.org/sites/default/files/2019-11/bitkom_wirtschaftsschutz_2019.pdf* (heruntergeladen am 20.04.2019)

Berking, M. & Rief, W. (2012). *Klinische Psychologie und Psychotherapie für Bachelor* (Band II: Therapieverfahren. Lesen, Hören, Lernen im Web). Berlin: Springer

Berry, W.D. (1993). *Understanding Regression Assumptions*. Newbury Park: Sage

Betsch, T., Funke, J. & Plessner, H. (2011). *Denken – Urteilen, Entscheiden, Problemlösen*: Allgemeine Psychologie für Bachelor. Berlin: Springer

Bhardwaj, A. & Goundar, S. (2020). Keyloggers: silent cyber security weapons. *Network Security*, 2, 14-19

Biermann, K. & Polke-Majewski, K. (2020). Datenklau: Ein Schüler hackt das politische System. Veröffentlicht unter: *https://www.zeit.de/digital/datenschutz/2019-01/datenklau-hacker-schueler-angriff-daten-politiker-datendiebstahl-datenleak* (heruntergeladen am 10.07.2020)

Billett, S. (2018). Accessing and Securing Conceptual and Symbolic Knowledge Required for Digital Era Work. In: Harteis, C (Hrsg). *Professional and Practice-based Learning.* Wiesbaden: Springer. S. 197-212

Bitkom (2017). Spionage, Sabotage, Datendiebstahl: Schaden von 55 Milliarden Euro. Veröffentlicht unter: *https://www.it-daily.net/analysen/16170-spionage-sabotage-datendiebstahl-schaden-von-55-milliarden-euro* (heruntergeladen am 20.04.2019)

BKA-SO51 (2016). Bundeslagebild Cybercrime 2016. Veröffentlicht unter: *https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2016.pdf* (heruntergeladen am 20.05.2019)

BKA (2016). Internet-Kriminalität/Cybercrime. Veröffentlicht unter: *https://www.bka.de/DE/UnsereAufgaben/Deliktsber* (heruntergeladen am 20.04.2019)

BKA (2017). *Cybercrime Bundeslagebild 2017*. Wiesbaden: Bundeskriminalamt

Blass, B. (2019). Passwortklau verhindern. *best practice onkologie*, 14(1), 50-52

Blickhäuser, A. & Bargen, H. (2008). Fit for Gender Mainstreaming. Veröffentlicht unter: *http://www.fit-for-gender.org/toolbox/toolbox/index.html* (heruntergeladen am 23.06.2020)

Blom, P. (2017). *Was auf dem Spiel steht*. München: Carl Hanser

Bloom, B. S. (1976). *Taxonomie von Lernzielen im kognitiven Bereich*. Weinheim: Beltz

Boddy, M. (2019). Exposed: Cyberattacks on Cloud Honeypots. Veröffentlicht unter: *https://www.sophos.com/en-us/medialibrary/PDFs/Whitepaper/sophos-exposed-cyberattacks-on-cloud-honeypots-wp.pdf* (heruntergeladen am 20.06.2019)

Bonfadelli, H. & Friemel, T. N. (2017). *Medienwirkungsforschung* (6. Aufl.). Konstanz: UVK

Borković, V. (2010). *Evaluation kommunaler Sportprojekte zur sozialen Integration von Heranwachsenden*. Potsdam: Universitätsverlag Potsdam

Bortz, J., & Doering, N. (2006). *Forschungsmethoden und Evaluation für Human- und Sozialwissenschaftler* (4. Aufl.). Heidelberg: Springer

Bortz, J., Lienert, G. A. & Boehnke, K (2008). *Verteilungsfreie Methoden in der Biostatistik* (3. Aufl.). Heidelberg: Springer

Bradley, P. (2013). *Expert Internet Searching* (4. Aufl.). London: Facet Publishing

Brand, D. (2004). Wirkungen situativer Kriminalprävention. Eine Evaluationsstudie zur Videoüberwachung in der Bundesrepublik Deutschland. Veröffentlicht unter: *https://pub.uni-bielefeld.de/download/2306207/2306210* (heruntergeladen am 20.04.2019)

Braun, K. H., Stübig, F. & Stübig, H. (2018). *Erziehungswissenschaftliche Reflexion und pädagogischpolitisches Engagement.* Wolfgang Klafki weiterdenken. Wiesbaden: Springer

Brenner, S. (2010). *Cybercrime*: Criminal Threats from Cyberspace. Santa Barbara: Praeger

Brien, J. (2018). 1,35 Terabit pro Sekunde: Bisher größte DDoS-Attacke trifft Github. Veröffentlicht unter: *https://t3n.de/news/groesster-ddos-attacke-github-971277/* (heruntergeladen am 12.01.2018)

Brighton, C. (2010). A simple Keylogger Program. Veröffentlicht unter: *http://www.cplusplus.com/forum/lounge/27569/* (heruntergeladen am 20.04.2019)

Brönimann, C. (1970). *Aufbau und Beurteilung des Kommunikationssystems von Unternehmungen.* Schriftenreihe: Führung und Organisation der Unternehmung (Band 8). Stuttgart: Paul Haupt

Brown, F. & Ragan, R. (2019). SearchDiggity. Veröffentlicht unter: *https://resources.bishopfox.com/resources/tools/google-hacking-diggity/attack-tools/* (heruntergeladen am 12.01.2020)

BSI (2012). Cyber-Bedrohungen. Ein Einstieg. Veröffentlicht unter: *https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/BSI-ACS_012.pdf?__blob=publicationFile&v=1* (heruntergeladen am 20.04.2018)

BSI (2019). Sensibilisierung der Mitarbeiter für Informationssicherheit. Veröffentlicht unter: *https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutz Kompendium/bausteine/ORP/ORP_3_Sensibilisierung_und_Schulung.html* (heruntergeladen am 20.06.2019)

Bubolz-Lutz, E. (2017). Selbstbestimmtes Lernen im Alter am Beispiel des Denk-Raum 50 plus. *DAS MAGAZIN*, 30-32. IV

Budde, J. & Venth, A. (2010). Genderkompetenz für lebenslanges Lernen. Bildungsprozesse geschlechterorientiert gestalten. Veröffentlicht unter: *https://www.die-bonn.de/doks/2009-geschlechterforschung-01.pdf* (heruntergeladen am 19.07.2019)

Bühner, M. (2006). *Einführung in die Test- und Fragebogenkonstruktion* (2. Aufl.). München: Pearson

Bühner, M. (2011). *Einführung in die Test- und Fragebogenkonstruktion* (3. Aufl.). München: Pearson

Bühner, M. & Ziegler, M. (2009). *Statistik für Psychologen und Sozialwissenschaftler*. München: Pearson

Bulgurcu, B., Cavusoglu, H. & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 34(3). 523-548

Bundeszentrale für politische Bildung. (2015). Medienkompetenz-Datenbank: Zielsetzung und Auswahlkriterien. Veröffentlicht unter: *http://www.bpb.de/lernen/digitale-bildung/medienpaedagogik/206271/ueber-die-datenbank* (heruntergeladen am 21.03.2019)

Bunker, G. (2020). Targeted cyber attacks: how to mitigate the increasing risk. *Network Security*, 1. 17-19

Büring, H. (2019). Ist das Tracken von Nutzern übers Smartphone legal? Veröffentlicht unter: *https://www.golem.de/news/wlan-tracking-und-datenschutz-ist-das-tracken-von-nutzern-uebers-smartphone-legal-1901-138464.html* (heruntergeladen am 23.02.2019)

Burkhardt, W. (2001). *Förderung kindlicher Medienkompetenz durch die Eltern.* Grundlagen, Konzepte und Zukunftsmodelle. Opladen: Leske + Budrich

Burzan, N. (2008). *Quantitative Forschung in der Sozialstrukturanalyse.* Anwendungsbeispiele aus methodischer Perspektive. Wiesbaden: VS Verlag

BVDW (2018). *EU-Datenschutzgrundverordnung 2018: BVDW-Praxisleitfaden*. Berlin: Bundesverband Digitale Wirtschaft

Cattell, R. B. (1966). The Scree Test For The Number Of Factors. *Multivariate Behavioral Research*, 1(2). 245-276

Cekerevac, Z., Dvorak, Z., Prigoda, L. & Cekerevac, P. (2018). Hacking, protection and the consequences of hacking. Veröffentlicht unter: *http://komunikacie.uniza.sk/index.php/communications/article/download/92/73/* (heruntergeladen am 20.04.2019)

Chantler, N. (1996). *Profil eines Computer-Hacker*. Florida: Infowar

Chapple, M. & Seidl, D. (2017). *CompTIA CySA+ Study Guide: Exam CS0-001*. Indianapolis: Wiley Publishing

Chiesa, R., Ducci, S. & Ciappi, S. (2009). *Profiling Hackers.* The Science of Criminal Profiling as Applied to the World of Hacking. Boca Raton: Auerbach Publication

Cialdini, R. B. (2017). *Die Psychologie des Überzeugens.* Wie Sie sich selbst und Ihren Mitmenschen auf die Schliche kommen. Bern: Hogrefe

Ciampa, M. (2011). *Security+ Guide to Network Security Fundamentals*. Boston: Cengage Learning

Clark, D. A., Beck, A. T. & Campisi, C. (2014). *Ängste bewältigen - ein Übungsbuch.* Lösungen aus der Kognitiven Verhaltenstherapie. Paderborn: Junfermann

Clough, J. (2010). *Principles of Cybercrime*. New York: Cambridge University Press

Coffer Group (2018). MAC Address Lookup and Search. Veröffentlicht unter: *http://www.coffer.com/mac_find/* (heruntergeladen am 12.01.2018)

Cohen, J. (1988). *Statistical power analysis for the behavioral sciences* (2. Aufl.). New York: Lawrence Erlbaum Associates

Comenius, J. A. (1891). *Die Klassiker der Pädagogik*. Langensalza: Greßler

Computerhilfen.de (2012). Der Schrottplatz hat was zu bieten! Aber Festplatte vernünftig? Veröffentlicht unter: *https://www.computerhilfen.de/hilfen-4-398560-0.html* (heruntergeladen am 20.12.2018)

Cornish, D. B. & Clarke, R. V. (2003). Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention. In Clarke, R. V. (Hrsg). *Theory for Situational Crime Prevention.* Crime Prevention Studies (vol. 16). Devon: Willan Publishing. S. 41-96

Cox, J. (2019). Jackpotting: So lassen Cyberkriminelle Geldautomaten Scheine spucken. Veröffentlicht unter: *https://www.vice.com/de/article/7x5ddg/malware-leert-geldautomaten-cyberkriminalitaet-hacking-geld* (heruntergeladen am 20.05.2020)

Cronbach, L. J. (1990). *Essentials of Psychological Testing* (5. Aufl.). New York: Harper & Row

Czernik, A. (2016). Definition und Unterscheidung der Begriffe Daten, Informationen & Wissen. Veröffentlicht unter: *https://www.dr-datenschutz.de/definition-und-unterscheidung-der-begriffe-daten-informationen-wissen/* (heruntergeladen am 07.07.2020)

D'Arcy, J., Hovav, A. & Galletta, D. (2009). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research*, 20(1). 79-98

Darlington, R. B. & Hayes, A. F. (2017). *Regression Analysis and Linear Models, Concepts, Applications, and Implementation*. New York: Guilford Press

Darms, M., Haßfeld, S. & Fedtke, S. (2019). *IT-Sicherheit und Datenschutz im Gesundheitswesen*. Wiesbaden: Springer

David, L. (2014). Qualiform. Kompetenzen von ErwachsenenbildnerInnen: Theoretische Themeneinführung und Darstellung der empirischen Ergebnisse (2. Fassung). Veröffentlicht unter: *https://www.researchgate.net/profile/Lisa_David/publication/265865680_Qualiform_Kompetenzen_von_ErwachsenenbildnerInnen/links/54200d130cf241a65a1afbda/Qualiform-Kompetenzen-von-ErwachsenenbildnerInnen.pdf* (heruntergeladen am 27.07.2019)

Day, M., Turner, G. & Drozdiak, N. (2019). Amazon Workers Are Listening to What You Tell Alexa. Veröffentlicht unter: *https://www.bloomberg.com/news/articles/2019-04-10/is-anyone-listening-to-you-on-alexa-a-global-team-reviews-audio* (heruntergeladen am 11.04.2019)

Debo, C. & Earley, S. (2015). Responding to Cybersecurity and Social Engineering Threats 2015 OTA Winter Conference and Trade Show. Veröffentlicht unter: *https://ohiotownships.org/sites/default/files/Responding to Cybersecurity and Social Engineering Threats.pdf* (heruntergeladen am 20.04.2018)

Deibert, R. & Rohozinski, R. (2009). *Tracking GhostNet:* Investigating a Cyber Espionage Network. Toronto, Ottawa: University of Toronto,The SecDev Group

Dellori, C. (2016). *Die absolute Metapher ‚lebenslanges Lernen'.* Eine Argumentationsanalyse (1. Aufl.). Wiesbaden: Springer

Detken, K. & Eren, E. (2006). *WLAN-Sicherheit – von WEP bis CCMP.* Bremen: DECOIT

Devine, C. & de Bouvette, O., T. (2018). Airdump-ng.

Dewe, B. (2004). Wissen, Können und die Frage der Refexivität. In: Bender, W(Hrsg.)., Groß, M. & Heglmeier, H. *Lernen und Handeln:* Eine Grundfrage der Erwachsenenbildung. Schwalbach: Wochenschauverlag. S. 321-331

Dickey, C. (2015). Hacking Made Easy Assessing the Vulnerability of Wireless Networks. Veröffentlicht unter: *https://www.morgan.edu/Documents/ACADEMICS/DEPTS/ElectricEng/Senior Design Final Report-1.pdf* (heruntergeladen am 02.04.2019)

Dittmar, N. & Lörch, T. (2018). Security-Aspekte: Security-Aspekte beim Einsatz von COTS- und Open SourceSoftwarekomponenten für kritische Systeme. Veröffentlicht unter: *https://www.certitudo-gmbh.de/files/content/Downloads/Certitudo-Security-Aspekte.pdf* (heruntergeladen am 20.12.2019)

Doering, N. & Bortz, J. (2016). *Forschungsmethoden und Evaluation in den Sozial- und Humanwissenschaften* (5. Aufl.). Berlin: Springer

Dolch, J. (1965). *Grundbegriffe der pädagogischen Fachsprache*. München: Ehrenwirth

Dombach, R. & Schmitz, P. (2016). Lohnt sich Sicherheits-Training? Security Awareness ist Zeitverschwendung! Veröffentlicht unter: *https://www.security-insider.de/security-awareness-ist-zeitverschwendung-a-567723/* (heruntergeladen am 20.11.2019)

Dornfest, R., Rausch, P. & Calishain, T. (2003). *Google Hacks:* Tips & Tools for Finding and Using the World's Information. Köln: O'Reilly

Dpa (2014). Bertelsmann beteiligt sich an E-Learning-Anbieter Udacity. Veröffentlicht unter: *https://www.nw.de/lokal/kreis_guetersloh/guetersloh/11256752_Bertelsmann-beteiligt-sich-an-E-Learning-Anbieter-Udacity.html* (heruntergeladen am 20.07.2019)

Dreißigacker, A. & Riesner, L. (2018). *Private Internetnutzung und Erfahrung mit computerbezogener Kriminalität.* Ergebnisse der Dunkelfeldstudien des Landeskriminalamtes Schleswig-Holstein 2015 und 2017. Hannover: kriminologisches Forschungsinstitut Niedersachsen e.V.

Dreyer, S. (2018). Sorgen, Einstellungen, Wissen, Handeln: Die Ergebnisse des Jugendmedienschutz-Index aus medienpolitischer Sicht. *JMS-Report*, 1. 1-3

Dreyfus, S. E. (2004). The Five-Stage Model of Adult Skill Acquisition. Veröffentlicht unter: *https://www.bumc.bu.edu/facdev-medicine/files/2012/03/Dreyfus-skill-level.pdf* (heruntergeladen am 26.10.2019)

Drössler, S., Steputat, A., Schubert, M., Günther, N., Staudte, R., Kofahl, M. & Seidler, A. (2018). Informationsüberflutung durch digitale Medien am Arbeitsplatz. *Zentralblatt für Arbeitsmedizin, Arbeitsschutz und Ergonomie*, 68(2). 77-88

DSV-Gruppe (2006). *Entsicherung am Arbeitsplatz:* Die geheime Logik der IT-Security in Unternehmen. Köln: known_sense

Dudenredaktion (2019).cyber. Veröffentlicht unter: *https://www.duden.de/rechtschreibung/cyber_* (heruntergeladen am 20.11.2019)

Durumeric, Z., Adrian, D., Mirian, A. & Bailey, M. (2019). Censys. Veröffentlicht unter: https://censys.io/ (heruntergeladen am 12.01.2020)

Dziuban, C. & Shirkey, E. (1974). When is a Correlation Matrix Appropriate for Factor Analysis? *Psychological Bulletin*, 18(6). 358-361

Eagly, A. H. & Chaiken, S. (1993). *Psychology of Attitudes*. San Diego: Cengage Learning

EC-Council (2010). *Investigating Network Intrusions and Cybercrime*. New York: EC-Council

Eckert, T. (2009). Bildungsstatistik. In: Tippelt, R. & Schmidt, B. (Hrsg). *Handbuch Bildungsforschung*. Wiebaden: VS Verlag für Sozialwissenschaften. S. 589-606

Edelmann, G. & Möller, C. (1977). *Grundkurs Lernplanung*. Weinheim: Beltz

Edwards, G. (2020). Cybercrime Investigators Handbook. Veröffentlicht unter: *https://books.google.de/books?id=548hygEACAAJ* (heruntergeladen am 20.04.2020)

Egloff, F. J. & Wenger, A. (2019). *Public Attribution of Cyber Incidents* (Security Policy No. 244). Zürich: ETH

Ellis, P. D. (2010). *The Essential Guide to Effect Sizes, Statistical Power, Meta-Analysis, and the Interpretation of Research Results*. New York: Cambridge University Press

Erbschloe, M. (2019). *Social Engineering: Hacking Systems, Nations, and Societies*. Boca Raton: CRC Press

Ernst, S. (2015). *GOTCHA!: Your Little Black Book to a Safer Experience*. Sydney: Goko Publishing

Euler, D. & Hahn, A. (2014). *Wirtschaftsdidaktik*. Bern: UTB

EZFF (2018). *Jahrbuch des Föderalismus 2018.* Föderalismus, Subsidiarität und Regionen in Europa. Tübingen: Europäischen Zentrum für Föderalismus-Forschung

Fahl, S., Marian, H., Acar, Y. & Smith, M. (2013). On The Ecological Validity of a Password Study. Veröffentlicht unter: *http://mattsmith.de/pdfs/Eco-Password.pdf* (heruntergeladen am 20.07.2019)

Fahrenberg, J. (2002). *Psychologische Interpretation:* Biographien – Texte – Tests. Bern: Hans Huber

Feld, T. C., Kraft, S., May, S. & Seitter, W. (2013). *Engagierte Beweglichkeit:* Weiterbildung in öffentlicher Verantwortung. Wiesbaden: Springer

Felser, G. (2015). *Werbe- und Konsumentenpsychologie* (4. Aufl.). Berlin: Springer

FFG (2016). Abschlussbericht zur Vorstudie „Weiterbildung zur Stärkung digitaler Kompetenz älterer Menschen“. Veröffentlicht unter: *http://www.ffg.tu-dortmund.de/cms/de/Projekte/Abgeschlossene_Projekte/2016/Weiterbildung-zur-Staerkung-digitaler-Kompetenz-aelterer-Menschen/FfG_Weiterbildung-zur-Staerkung-digitaler-Kompetenz-aelterer-Menschen.pdf* (heruntergeladen am 23.08.2019)

Cybercrime 2017 in Facts and Figures. (2017). Veröffentlicht unter: *https://www.fidelissecurity.com/sites/default/files/Fidelis_Cybercrime_2017.pdf* (heruntergeladen am 12.01.2018)

Field, A. (2018). *Discovering Statistics Using IBM SPSS* (5. Aufl.). Thousand Oaks: Sage

Fileccia, M. (2008). *Knowhow für junge User.* Mehr Sicherheit im Umgang mit dem World Wide Web. Materialien für den Unterricht. Düsseldorf: Landesanstalt für Medien Nordrhein-Westfalen

Fischer, M. (2001). Produktlebenszyklus und Wettbewerbsdynamik. Grundlagen für die ökonomische Bewertung von Markteintrittsstrategien. Veröffentlicht unter: *https://madoc.bib.uni-mannheim.de/10064/* (heruntergeladen am 20.06.2018)

Fischer, M. S. (1988). *Mensch und Technik: Literarische Phantasie und Textmaschine.* Symposium in Aachen vom 15.-16. April 1988, veranstaltet vom Literaturbüro in der Euregio Maas-Rhein e.V. und dem Kulturamt der Stadt Aachen. Aachen: Alano

Fishbein, M. (1963). An investigation of the relationships between beliefs about an object and the attitude toward that object. *Human Relations*, 16

Fishbeln, M., Ajzen, I. & Landy, E. S. (1970). Attitudinal Variables and Behavior: Three Empirical Studies and a Theoretical Reanalysis. Veröffentlicht unter: *https://apps.dtic.mil/dtic/tr/fulltext/u2/715369.pdf* (heruntergeladen am 20.04.2019)

Flechsig, K.-H. (1996). *Kleines Handbuch didaktischer Modelle.* Eichenzell: Neuland

Flenov, M. (2005). *Hacker Linux Uncovered*. Wayne: Alist LLC

Floyd, D. L., Prentice-Dunn, S. & Rogers, R. W. (2000). A Meta-Analysis of Research on Protection Motivation Theory. *Journal of Applied Social Psychology*, 30(2). 407-429

Forlin, C. & Chambers, D. (2011). Teacher preparation for inclusive education, increasing knowledge but raising concerns. *Asia-Pacific Journal of Teacher Education*, 39(1). 17-32

Förtsch, O. (2012). *Handbuch zur Geldemission für jedermann:* Ideen, Strukturen, Verfahren und ein Aufruf zum Mitmachen. Oberhaching: Tintenfaß

Frei, B. (2003). *Pädagogische Autorität:* Eine empirische Untersuchung bei Schülerinnen, Schülern und Lehrpersonen der 5., 6. und 8. Schulklasse. Münster: Waxmann

Fromm, S. & Baur, N. (2008). *Datenanalyse mit SPSS für Fortgeschrittene* (2. Aufl.). Wiesbaden: VS Verlag für Sozialwissenschaften

Frumento, E. (2017). *Victim Communication Stack*. A exible model to select the Human Attack Vector. Milan: Cefriel

Füllgraf, W. (2015). *Hacktivisten.* Abschlussbericht zum Projektteil der Hellfeldbeforschung. Wiesbaden: Bundeskriminalamt

Funken, M. (2020). Außenanbindung. Veröffentlicht unter: *https://www.rz.uni-wuerzburg.de/dienste/kommunikation/datennetz/aufbau/* (heruntergeladen am 06.05.2020)

Fussan, C. (2010). *Managementmaßnahmen gegen Produktpiraterie und Industriespionage*. Wiesbaden: Gabler

Gaigl, A. (2014). Weiterbildungen kompetenzorientiert gestalten – Anforderungen an Weiterbildnerinnen und Weiterbildner. In: Weiterbildungsinitiative Frühpädagogische Fachkräfte (Hrsg.). *Kompetenzorientierte Gestaltung von Weiterbildungen.* Grundlagen für die Frühpädagogik. München: WiFFWegweiser. S. 34-53

Gandolfi, A. (2001). *Von Menschen und Ameisen:* Denken in komplexen Zusammenhängen. Zürich: Orell Füssli

Gardner, B. (2014). *Most Attacks Are Targeted in Building:* An Information Security Awareness Program. Amsterdam: Elsevier

Gardner, B. & Thomas, V. (2014). *Building an Information Security Awareness Program, Defending Against Social Engineering and Technical Threats*. Waltham: Elsevier

Gassmann, C. (2013). *Erlebte Aufgabenschwierigkeit bei der Unterrichtsplanung:* Eine qualitativ-inhaltsanalytische Studie zu den Praktikums-phasen der universitären Lehrerbildung. Wiesbaden: Springer

Gehrke, M. (2019). *Angewandte empirische Methoden in Finance & Accounting: Umsetzung mit R (De Gruyter Studium)*. Berlin: De Gruyter Oldenbourg

George, D. & Mallery, P. (2019). *IBM SPSS Statistics 25 Step by Step. A Simple Guide and Reference* (15. Aufl.). New York: Routledge

Geuß, A. (2018). *Qualität im Journalismus:* Eine Synopse zum aktuellen Forschungsstand. Bamberg: University of Bamberg Press

Gindl, M. & Hefler, G. (2006). Gendersensible Didaktik in universitärer Lehre und Weiterbildung für Erwachsene. Veröffentlicht unter: *https://www.ph-freiburg.de/fileadmin/dateien/sonstige/gleichstellung/Leitfaden_gendersensible_Didaktik_unigraz.pdf* (heruntergeladen am 20.09.2019)

Glas, P, Pieler, D. & Rosenstiel, L. V. (2004). *Strategisches Kompetenzmanagement*. Wiesbaden: Gabler

Glaser, C. (2009). Käufer- und Nutzergruppen von Sicherheitsprodukten. Veröffentlicht unter: *https://depositonce.tu-berlin.de/bitstream/11303/2361/3/Dokument_19.pdf* (heruntergeladen am 05.04.2019)

Glos, R. G. & Seemann, M. (2013). *Heimnetzwerke.* DSL/WLAN/PC/Handy/Drucker & Co. Haar: Franzis

GMT (2018). Check out our 2017 annual report. Veröffentlicht unter: *https://www.khanacademy.org/about/blog/post/175353939990/check-out-our-2017-annual-report* (heruntergeladen am 20.10.2019)

Gorges, J. (2018). *Eine adaptierte Erwartungs-Wert-Skala zur Erfassung von Fort- und Weiterbildungsmotivation.* Unveröffentlichte Skalendokumentation. Universität Bielefeld

Gorges, J., Neumann, P., Lütje-Klose, B. & Wild, E. (2017). Dimensionen inklusionsbezogener Fortbildungsmotivation von Sonderpädagoginnen und Sonderpädagogen und Lehrkräften allgemeiner Schulen. *Empirische Sonderpädagogik*, 3. 199-214

Gouldner, A. W. (1960). The Norm of Reciprocity: A Preliminary Statement. *American Sociological Review*, 25(2). 161-178

Goyal, P. (2017). Cracking Into Computers. An Attempt To Hack The Infinity. Veröffentlicht unter: https://books.google.com.ua/books?id=WwslDwAAQBAJ (heruntergeladen am 20.03.2019)

Grant, H. (2015). *Social Crime Prevention in the Developing World Exploring the Role of Police in Crime Prevention*. New York: Springer

Graves, K. (2010). *CEH Certified Ethical Hacker Study Guide*. Hoboken, New Jersey: Wiley Publishing

Grillenberger, B. (2017). Password Strength Meter. Veröffentlicht unter: *https://docplayer.org/40429389-Password-strength-meter.html* (heruntergeladen am 28.07.2019)

Grimes, R. A. (2017). *Hacking the Hacker.* Learn from the Experts Who Take Down Hackers. Crosspoint Boulevard: John Wiley & Sons

Grotlüschen, A. (2010). *Erneuerung der Interessetheorie:* Die Genese von Interesse an Erwachsenen- und Weiterbildung. Wiesbaden: VS Verlag für Sozialwissenschaften

Gruenwald, H. (2017). J. VIZIO to Pay $2.2 Million to FTC, State of New Jersey to Settle Charges It Collected Viewing Histories on 11 Million Smart Televisions without Users' Consent. Veröffentlicht unter: *https://www.ftc.gov/news-%0Aevents/press-releases/2017/02/%0Avizio-pay-22-million-ftc-state-new-%0Ajersey-settle-charges-it%0A* (heruntergeladen am 07.05.2019)

Guggenberger, J. M. (2010). *Aufbau und Ablauf einer IT-Integration:* Phasenmodell und Vorgehenskonzept unter Berücksichtigung rechtlicher Aspekte. Wiesbaden: Gabler

Gul, S. A. (2016). Keylogger Application Program in C# with Source Code & Download. Veröffentlicht unter: *https://www.csharpens.com/projects/keylogger-application-program-in-c-sharp-with-source-code-download-43/* (heruntergeladen am 18.04.2019)

Günther, W. (1966). S*piel, Kampf und Arbeit als Formen der Selbstbildung im Frühwerk Ernst Jüngers*. Kiel: Christian-Albrechts-Universität

Gut, M. & Kammermann, M. (2016). *CompTia Security+: It-Sicherheit Verständlich Erklärt - Vorbereitung Auf Die Prüfung Syo-401*. Frechen: mitp

Habedank, S. (2011). Didaktik und Methodik. Worin liegt der Unterschied? *Direkt!*, *1*, 1

Haesen, V. (2014). *Der Schutz gegen den unlauteren Wettbewerb in Deutschland und England vor dem Hintergrund fortschreitender europäischer Harmonisierung*. München: Herbert Utz

Hagendorff, T. (2019). Post-Privacy oder der Verlust der Informationskontrolle. In: Behrendt, H., Loh, W., Matzner, T. & Misselhorn, C. (Hrsg.). *Privatsphäre 4.0: Eine Neuverortung des Privaten im Zeitalter der Digitalisierung.* Berlin: Metzler. S. 91-106

Hallahan, J. (2007). Countering Insider Threats - Handling Insider Threats Using Dynamic, Run-Time Forensics. Veröffentlicht unter: *https://apps.dtic.mil/dtic/tr/fulltext/u2/a473440.pdf* (heruntergeladen am 20.08.2019)

Hallet, W. (2006). *Didaktische Kompetenzen:* Lehr- und Lernprozesse erfolgreich gestalten. Stuttgart: Klett

Hamburg, I. & Lütgen, G. (2019). Digital Divide, Digital Inclusion and Inclusive Education. *Advances in Social Sciences Research Journal*, 6(4). 193-206

Hammel, M. (2005). *Naturwissenschaftliches Wissen mit Neuen Medien vermitteln.* Fragen und Analysen zur geschlechtsgerechten Partizipation. Schiften zur Kommunikation Wissenschaft-Offentlichkeit *2*. Koblenz: Forschungsstelle Wissenstransfer

Handwerk, H. (2020). *Inklusion als Ausdrucksgestalt:* Rekonstruktive Inklusionsforschung an Freien Waldorfschulen. Wiesbaden: Springer

Hannig, U. (2002). *Knowledge Management und Business Intelligence*. Heidelberg: Springer

Hansen, S. (2008). *Lernen durch freiwilliges Engagement:* Eine empirische Studie zu Lernprozessen in Vereinen. Wiesbaden: VS Verlag

Harenski, C. L., Harenski, K. A., Shane, M. S. & Kiehl, K. A. (2011). Neural development of mentalizing in moral judgment from adolescence to adulthood. Veröffentlicht unter: *https://ac.els-cdn.com/S1878929311001009/1-s2.0-S1878929311001009-main.pdf?_tid=af664552-885e-4ee1-923a-50b445e60c6d&download=true&acdnat=1552121517_389c8e2b0695d729c9dda7cff6a860a7%0A%0A* (heruntergeladen am 20.04.2019)

Harnisch, S. & Zettl, K. (2020). Am Anfang war die Attribution… Cyber-Angriffe und deren Beantwortung als Herausforderung demokratischen Regierens. Veröffentlicht unter: *https://www.uni-heidelberg.de/md/politik/harnisch/person/publikationen/am_anfang_war_die_attribution_harnisch_zettl.pdf* (heruntergeladen am 20.08.2020)

Hartig, C. (2009). Berufliche Selbstbeschreibung als berufskulturelle Selbstaufklärung. In: Seitter, W. (Hrsg.). *Professionalitätsentwicklung in der Weiterbildung*. Wiesbaden: Springer. S. 205-232

Hartig, J., Jude, N. & Wagner, W. (2008). Methodische Grundlagen der Messung und Erklärung sprachlicher Kompetenzen. In: Klieme, E. (Hrsg.). *Unterricht und Kompetenzerwerb in Deutsch und Englisch.* Ergebnisse der DESI-Studie. Weinheim: Beltz. S. 34-54

Haschke, C., Westrick, M. G. & Schwenk, U. (2018). Gesundheitsinfos: Wer suchet, der fndet – Patienten mit Dr. Google zufrieden. Veröffentlicht unter: *https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/VV_SpotGes_Gesundheitsinfos_final.pdf* (heruntergeladen am 20.12.2018)

Hayden, J. (2019). *Introduction to Health Behavior Theory*. Burlington: Jones & Bartlett Learning

Hayes, A. F. (2007). Using heteroskedasticity-consistent standard error estimators in OLS regression: An introduction and software implementation. *Behavior Research Methods*, 39(4). 709-722

Hayes, A. F. (2018). *Introduction to Mediation, Moderation, and Conditional Process Analysis* (2. Aufl.). New York: Guilford Press

Heimann, P., Otto, G. & Schulz, W. (1965). *Unterricht: Analyse und Planung*. Hannover: Schroedel

Helisch, M. & Pokoyski, D. (2009). Awareness aus der Perspektive des Marketings. In: Pokoyski, D. (Hrsg.). *Security Awareness: Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung.* Wiesbaden: Springer Vieweg+Teubner

Helmke, A. (2010). *Unterrichtsqualität und Lehrerprofessionalität:* Diagnose, Evaluation und Verbesserung des Unterrichts.Hannover: Seelze-Velber

Hemmerich, W. A. (2019). Effektstärke. Veröffentlicht unter: *https://matheguru.com/stochastik/effektstarke.html* (heruntergeladen am 05.09.2019)

Hermann, D. (2016). Kriminalprävention und Ethik. Veröffentlicht unter: *http://www.praeventionstag.de/dokumentation/download.cms?id=2502&datei=DPT_2016_Hermann_final-2502.pdf* (heruntergeladen am 17.04.2019)

Hermann, D. & Bubenitschek, G. (2015). Kosten und Nutzen Kommunaler Kriminalprävention. Veröffentlicht unter: *http://www.praeventionstag.de/dokumentation/download.cms?id=2358&datei=0900-Guenther-Bubenitschek_F3147-2358.pdf* (heruntergeladen am 20.05.2019)

Herzig, B., Meister, D. M., Moser, H. & Niesyto, H. (Hrsg.) (2010). *Jahrbuch Medienpädagogik 8.* Medienkompetenz und Web 2.0. Wiesbaden: Springer VS

Hiemisch, A. (2017). *Fragekomplex zum geplanten Verhalten im Kontext von IT-Sicherheit*. Greifswald: Universität Greifswald

Hillenbrand, C., Melzer, C. & Hagen, T. (2013). Bildung schulischer Fachkräfte für inklusive Bildungssysteme. In: Döbert, H. & Weishaupt, H. (Hrsg.). *Inklusive Bildung professionell gestalten.* Situationsanalyse und Handlungsempfehlungen. Münster: Waxmann.

Hobbensiefken, G. (1980). *Berufsforschung.* Einführung in traditionelle und moderne Theorien. Wiesbaden: Springer

Höfer, R. & Kraus, W. (2005). Die Konstruktion von Zugehörigkeit. Individuelle Strategien, organisatorische Antworten. Ergebnisse der bisherigen Forschungsarbeit. Veröffentlicht unter: *http://www.ipp-muenchen.de/texte/kraus_kochel.pdf* (heruntergeladen am 27.07.2019)

Hofielen, G. (2018). Corporate Responsibility als Veränderungsstrategie und CR Manager*innen als Veränderungsmanager*innen. Veröffentlicht unter: *https://www.hm-practices.org/wp-content/uploads/2018/11/3_CR-als-Veränderungsmanagement.pdf* (heruntergeladen am 04.06.2020)

Hollinger, R. (1988). Computer hackers follow a guttman-like progression. *Social Sciences Review*, Florida: University Of Florida

Holt, T. J. (2013). *Examining the forces shaping cybercrime markets online*. Science Computer Review, 31. 165-177

Holtz, R. & Miller, N. (1985). Assumed similarity and opinion certainty. *Journal of Abnormal and Social Psychology*, 55. 244-252

Hönigswald, R. (1918). *Über die Grundlagen der Pädagogik*. München: Reinhardt

Hooß, K. (2014). *Wissenschaftliche Weiterbildung für IT-Wissensarbeiter.* Bedingungen und Motive der Teilnahme und Nichtteilnahme. Wiesbaden: Springer

Hopf, W. (2010). *Freiheit - Leistung - Ungleicheit.* Bildung und soziale Herkunft in Deutschland. Weinheim: Beltz Juventa

Hornsteiner, G. (2012). *Daten und Statistik:* Eine praktische Einführung für den Bachelor in Psychologie und Sozialwissenschaften. Berlin: Springer

Hosmer, C. (2014). *Python Forensics.* A Workbench for Inventing and Sharing Digital Forensic Technology. Waltham: Syngress

Howaldt, J. (2004). *Neue Formen sozialwissenschaftlicher Wissensproduktion in der Wissensgesellschaft:* Forschung und Beratung in betrieblichen und regionalen Innovationsprozessen. Münster: Lit

Huber, E. (2012). *Cyberstalking und Cybercrime.* Kriminalsoziologische Untersuchung zum Cyberstalking-Verhalten der Österreicher (1. Aufl.). Wiesbaden: Springer

Humbert, L. (2005). *Didaktik der Informatik mit praxiserprobtem Unterrichtsmaterial*. Wiesbaden: Teubner

Humbert, L. (2006). *Didaktik der Informatik mit praxiserprobtem Unterrichtsmaterial* (2. Aufl.). Wiesbaden: Teubner

Husák, M., Neshenko, N., Pour, M. S., Bou-Harb, E. & Čeleda, P. (2018). *Assessing Internet-wide Cyber Situational Awareness of Critical Sectors*. Boca: Florida Atlantic University, Raton: Masaryk University

IBM (2018a). IBM X-Force Threat Intelligence Index. Veröffentlicht unter: *https://crowdresearchpartners.com/wp-content/uploads/2017/07/Insider-Threat-Report-2018.pdf* (heruntergeladen am 25.05.2020)

IBM (2018b). IBM X-Force Threat Intelligence Index 2017. Veröffentlicht unter: *https://www.leadersinsecurity.org/component/phocadownload/category/11-2017-cybersecurity-publications.html?download=185:2017-cybersecurity-publications* (heruntergeladen am 20.05.2019)

Ifinedo, P. (2012). Effects of organization insiders' self-control and relevant knowledge on participation in information systems security deviant behavior. *Computers & Security*, 31. 6-95

Ifinedo, P. (2013). *Information systems security policy compliance.* An empirical study of the effects of socialization, influence, and cognition. Amsterdam: Elsevier

Immler, C. (2007). *Das PC-Handbuch*. München: Markt und Technik

Infosec (2014). Security Awareness Training Whitepaper The Power Of Interactivity And Repetition. Veröffentlicht unter: *https://resources.infosecinstitute.com/wp-content/uploads/Security-Awareness-Training-Best-Practices.pdf* (heruntergeladen am 20.05.2019)

Ioannou, N. (2019). *Internet Security Fundamentals.* A Modern Day Digital Survival Guide. London: Boolean Logical Ltd

Ipsos (2017). Jeder zweite hat Angst, Opfer von Cyberkriminalität zu werden. Veröffentlicht unter: *https://de.statista.com/infografik/9344/jeder-zweite-deutsche-hat-angst-vor-cybercrime/* (heruntergeladen am 12.01.2018)

iso.org (2005). ISO 27001. Veröffentlicht unter: *http://bcc.portal.gov.bd/sites/default/files/files/bcc.portal.gov.bd/page/adeaf3e5_cc55_4222_8767_f26bcaec3f70/ISO_IEC_27001.pdf* (heruntergeladen am 20.07.2018)

IT-Sicherheitsgesetz (2017). Veröffentlicht unter: *https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&start=//*%255B@attr_id=%27bgbl115s1324.pdf%27%255D#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl115s1324.pdf%27%5D__1526585932794* (heruntergeladen am 20.01.2019)

Jank, W. & Meyer, H. (2002). *Didaktische Modelle*. Berlin: Cornelsen

Janssen, J. & Laatz, W. (2017). *Statistische Datenanalyse mit SPSS.* Eine anwendungsorientierte Einführung in das Basissystem und das Modul Exakte Tests (9. Aufl.). Berlin: Springer

Jonas, K., Stroebe, W. & Hewstone, M. (2014). *Sozialpsychologie* (6. Aufl.). Berlin: Springer

Jüngst, K. L. & Dörr, G. (1998). *Lernen mit Medien*. Weinheim: Juventa

Kähler, W. M. (2004). *Statistische Datenanalyse.* Verfahren verstehen und mit SPSS gekonnt einsetzen (3. Aufl.). Wiesbaden: Springer

Kahlert, H. & Mischau, A. (2000). *Neue Bildungswege für Frauen.* Frauenhochschulen und Frauenstudiengänge im Überblick. Frankfurt am Main: Campus

Kaiser, H. F. & Rice, J. (1974). Little Jiffy, Mark IV. *Educational and Psychological Measurement*, 34(1). 112

Kapfer, P. (2014). *Internal Hacking y contramedidas en entorno Windows Pirateo interno, medidas de protección, desarrollo de herramientas*. Cornellà de Llobregat: Ediciones Eni

Karl, D. (2009). *Arbeitsfähigkeit, ein ganzheitlicher, integrativer Ansatz* (Arbeitswissenschaft in der betrieblichen Praxis, Band 31). Frankfurt am Main: Peter Lang

Kaschek, B. & Schumacher, I. (2015). *Führungspersönlichkeiten und ihre Erfolgsgeheimnisse.* Management und Leadership im 21. Jahrhundert. Springer

Top Ten Most Notorious (Infamous) (2018). Hackers of All Time. Veröffentlicht unter: *https://usa.kaspersky.com/resource-center/threats/top-ten-greatest-hackers* (heruntergeladen am 28.04.2019)

Kaspersky Security Bulletin. Overall Statistics for 2017. (2017) Veröffentlicht unter: *https://media.kaspersky.com/jp/pdf/pr/Kaspersky_KSB2017_ Statistics-PR-1045.pdf* (heruntergeladen am 20.07.2019)

Kaufmann, K. & Windany, S. (2013). Berufliche Weiterbildung. Gelegenheits- und Teilnahmestrukturen. *Zeitschrift für Erziehungswissenschaft*, 16(1). 45

Keegan, W. J., Schlegelmilch, B. & Stöttinger, B. (2002). *Globales Marketing-Management*: Eine europäische Perspektive. München: Oldenbourg

Kelley, P., Komanduri, S., Mazurek, M. & Shay, R. (2012). Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms. Veröffentlicht unter: *https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber= 6234434* (heruntergeladen am 20.09.2019)

Kershaw, M. (2016). Kismet. Veröffentlicht unter: *https://www.kismetwireless.net/* (heruntergeladen am 18.08.2019)

Kersten-Frisch, P. (2015). *Englisch lernen in Betrieben*. Tübingen: Narr Francke Attempto

Khan, B., Alghathbar, K. S., Nabi, S. I. & Khan, M. K. (2011). Effectiveness of information security awareness methods based on psychological theories. Veröffentlicht unter: *https://pdfs.semanticscholar.org/a5ab/bcadc980486d19bdcab 247f68feded7f09c9.pdf* (heruntergeladen am 20.07.2018)

Khanal, S., Lynton, C. & Dean, R. (2013). *Packet Simulation of Distributed Denial of Service (DDoS) Attack and Recovery.* Baltimore,: Morgan State University

Khrais, H. (2018). *Python for Offensive PenTest.* A practical guide to ethical hacking and penetration testing using Python (English Edition). Birmingham: Packt Publishing

Kilger, M., Arkin, O. & Stutzman, J. (2004). *Profiling in The Honeynet Projekt. Know Your Enemy. Learning abaut Security Threats*. Boston: Addison

Kirchhof, R. (2003). *Ganzheitliches Komplexitätsmanagement*. Wiesbaden: Deutscher Universitäts-Verlag

Klafki, W. (1964). Didaktische Analyse als Kern der Unterrichtsvorbereitung. In: Roth, H. & Blumenthal, A. (Hrsg.). *Didaktische Analyse* (Auswahl Reihe A, Bd. 1). Hannover: Schroedel. S. 5-34

Klau, P. (2002). *Hacker, Cracker, Datenräuber*. Wiesbaden: Vieweg

Klein, R. H. & Luciano, M. E. (2016). What influences information security behavior? A study with Brazilian users. Veröffentlicht unter: *http://www.jistem.fea.usp.br/index. php/jistem/article/download/10.4301%25S1807-17752016000300007/619* (heruntergeladen am 17.06.2019)

Kleist, P. (2009). Das Intention-to-Treat-Prinzip. *Schweiz Med Forum*, 9(25). 451

Kline, P. (1994). *An easy guide to factor analysis*. London: Routledge

Köhntopp, A., Pfitzmann, M. & Fox, D. (2001). *Verlässliche IT-Systeme 2001.* Sicherheit in komplexen IT-Infrastrukturen. Wiebaden: Springer

Koldner, L. (2014). Der Faktor Mensch in der Datensicherheit – Kann man Sicherheitsbewusstsein messen? Veröffentlicht unter: *http://www.aow.ruhr-uni-bochum.de/mam/content/newsletter030.pdf* (heruntergeladen am 12.01.2018)

Kolland, F., Wanka, A. & Gallistl, V. (2019). Technik und Alter – Digitalisierung und die Ko-Konstitution von Alter(n) und Technologien. In: Schroete, K. R., Vogel, C. & Künemund, H. (Hrsg.). *Handbuch Soziologie des Alter(n)s*. Wiesbaden: Springer. S. 15

König, S. (2018). *Analyse von Längsschnittdaten.* Workshop bei der Winterakademie der Graduiertenakademie Pädagogische Hochschulen BW am 27./28.2.2018 in Bad Herrenalb. Veröffentlicht unter: *http://sportwissenschaft.ph-weingarten.de/fileadmin/redaktuere/Subdomains/Sportwissenschaft/Praesentation_BadH_final_.pdf* (heruntergeladen am 20.08.2019)

Kosfeld, R. (o.J.). Lösungen zu den Aufgaben zur Multivariaten Statistik. Teil 2: Aufgaben zur Faktorenanalyse. Veröffentlicht unter: *https://www.uni-kassel.de/fb07/fileadmin/datas/fb07/5-Institute/IVWL/Kosfeld/lehre/multivariate/Multivariate_Aufgaben_mit_Loes2.pdf* (heruntergeladen am 20.05.2019)

Köster, D. (2009). Entwicklungschancen in alternden Gesellschaften durch Bildung. Trends und Perspektiven. In: Dehmel, A., Kremer, H., Schaper, N., Sloane, P.F.E. (Hrsg.). *Bildungsperspektiven in alternden Gesellschaften*. Frankfurt am Main: Peter Lang. S. 101

Kovaleva, A., Beierlein, C., Kemper, C. & Rammstedt, B. (2012). Eine Kurzskala zur Messung von Kontrollüberzeugung: Die Skala Internale-Externale-Kontrollüberzeugung-4 (IE-4). Veröffentlicht unter: *https://www.gesis.org/fileadmin/kurzskalen/working_papers/IE4_Workingpaper.pdf* (heruntergeladen am 20.05.2018)

Krah, E. S. (2017). Finanzsektor ist Top-Angriffsziel für Hacker. Veröffentlicht unter: *https://www.springerprofessional.de/bank-it/it-sicherheit/finanzsektor-ist-top-angriffsziel-fuer-hacker/12260790* (heruntergeladen am 12.03.2019)

Krämer, W., Schoffer, O., Gerß, J. & Tschiersch, L. (2018). *Datenanalyse mit SAS.* Statistische Verfahren und ihre grafischen Aspekte. Berlin: Springer

Krampen, G. & Zayer, H. (2006). *Didaktik und Evaluation in der Psychologie*. Göttingen: Hogrefe

Krauth, J. (1973). Nichtparametrische Ansätze zur Auswertung von Verlaufskurven. *Biometrische Zeitschrift*, 15. 557-566

Krauthausen, G. (2012). *Digitale Medien im Mathematikunterricht der Grundschule*. Heidelberg: Springer

Krebs, M. (1998). *Organisation von Wissen in Unternehmungen und Netzwerken*. Wiesbaden: Springer

Kreß, J. (2016). *Onlinecommunities für Senioren:* Wie virtuelle Netzwerke als Unterstützung im Alltag dienen. Wiesbaden: Springer

Krombholz, K., Hobel, H., Huber, M. & Weippl, E. (2014). Advanced Social Engineering Attacks. Veröffentlicht unter: *https://www.sba-research.org/wp-content/uploads/publications/jisa_revised.pdf* (heruntergeladen am 18.07.2018)

Kron, F. W. (1993). *Grundwissen Didaktik*. München, Basel: Reinhardt

Kronauer, M. (2010). *Inklusion und Weiterbildung:* Reflexionen zur gesellschaftlichen Teilhabe in der Gegenwart. Bielefeld: Bertelsmann

Kronthaler, F. (2016). *Statistik angewandt:* Datenanalyse ist (k)eine Kunst mit dem R Commander. Berlin: Springer

Kühl, E. (2017). My Friend Cayla: Vernichten Sie diese Puppe. Veröffentlicht unter: *http://www.zeit.de/digital/datenschutz/2017-02/my-friend-cayla-puppe-spion-%0Abundesnetzagentur%0A* (heruntergeladen am 17.07.2019)

Kuhl, J. (2001). *Motivation und Persönlichkeit:* Interaktionen psychischer Systeme. Göttingen: Hogrefe

Kuhlmei, E. (2018). *Lerne mit uns Statistik!* Drei Studis erklären statistische Verfahren und ihre SPSS-Anwendungen. Berlin: Springer

Kuketz, M. (2018). Shodan: Suchmaschine für das »Internet of Shit«. Veröffentlicht unter: *https://www.kuketz-blog.de/shodan-suchmaschine-fuer-das-internet-of-shit/* (heruntergeladen am 12.01.2018)

Kul, G., Upadhyaya, S. & Hughes, A. (2016). Complexity of Insider Attacks to Databases. Veröffentlicht unter: *https://cse.buffalo.edu/~gokhanku/ComplexityOfInsiderAttacks.pdf* (heruntergeladen am 20.12.2018)

Kuß, A. & Eisend, M. (2010). *Marktforschung.* Grundlagen der Datenerhebung und Datenanalyse (3. Aufl.). Wiesbaden: Gabler

Kwon, H., Shakarian, J., Priniski, H., Sarkar, S. & Shakarian, P. (2017). Crisis and collective problem solving in dark web: An exploration of a black hat forum. Veröffentlicht unter: *https://www.researchgate.net/profile/Kyounghee_Kwon/publication/318477668_Crisis_and_Collective_Problem_Solving_in_Dark_Web_An_Exploration_of_a_Black_Hat_Forum/links/59e78e74a6fdccfe7f8ae1a0/Crisis-and-Collective-Problem-Solving-in-Dark-Web-An-Exploration-of-a-Black-Hat-Forum.pdf* (heruntergeladen am 19.06.2019)

Lampert, T. R. (2017). Keylogger in Java. Veröffentlicht unter: *https://www.programcreek.com/java-api-examples/?code=tiagorlampert/sAINT/sAINT-master/src_template/main/java/saint/keylogger/Keylogger.java* (heruntergeladen am 20.01.2020)

Lang, F. R. & Lüdtke, O. (2005). Der Big Five-Ansatz der Persönlichkeitsforschung. Instrumente und Vorgehen. In: Schumann, S. (Hrsg.). *Persönlichkeit: Eine vergessene Größe der empirischen Sozialforschung*. Wiesbaden: VS Verlag. S. 29-39

Langbehn, A. (2010). *Praxishandbuch Produktentwicklung:* Grundlagen, Instrumente und Beispiele. Frankfurt am Main: Campus

Lange, H. J. & Bötticher, A. (2015). *Cyber-Sicherheit*. Wiesbaden: Springer

Langner, A. (2019). Weitergedacht. In: Langner, A., Ritter, M., Steffens, J. & Jugel, D. (Hrsg.). *Inklusive Bildung forschend entdecken*. Wiebaden: Springer. S. 231-259

LaPiere, R. T. (1934). Attitudes vesus action. *Social Forces*, 13

Laufer, D. & Meineck, S. (2020). Eine polnische Firma schafft gerade unsere Anonymität ab. Veröffentlicht unter: *https://netzpolitik.org/2020/gesichter-suchmaschine-pimeyes-schafft-anonymitaet-ab/* (heruntergeladen am 15.07.2020)

Lazarus, R. S. & Folkman, S. (1984). *Stress, Appraisal, and Coping*. New York: Springer

Lazarus, R. S. & Lazarus, B. N. (2006). *Coping with Aging*. Oxford: Oxford University Press

Lempert, P. (2018). Spektakuläre Cybercrime-Fälle. Veröffentlicht unter: *https://magazin-forum.de/de/node/7548* (heruntergeladen am 02.04.2020)

Leukfeldt, R., Veenstra, S. & Stol, W. (2013). *High Volume Cyber Crime and the Organization of the Police.* The results of two empirical studies in the Netherlands. Netherlands: University of Applied Sciences

LfK (2019). Richtline zur Förderung von Präventionsprojekten. Veröffentlicht unter: *http://www.service.m-v.de/serviceassistent/download?id=1586188* (heruntergeladen am 20.07.2019)

Lin, H. (2016). Attribution of Malicious Cyber Incidents. Veröffentlicht unter: *https://www.hoover.org/sites/default/files/research/docs/lin_webready.pdf* (heruntergeladen am 20.03.2019)

Linden, M. & Hautzinger, M. (1981). *Psychotherapie-Manual.* Sammlung psychotherapeutischer Techniken und Einzelverfahren. Heidelberg: Springer

Lindner, D. (2002). *Einflussfaktoren des erfolgreichen Auslandseinsatzes.* Konzeptionelle Grundlagen - Bestimmungsgrößen - Ansatzpunkte zur Verbesserung. Wiesbaden: Gabler

Lipski, M. (2009). *Social Engineering.* Der Mensch als Sicherheitsrisiko in der IT. Hamburg: Diplomica

Lloret-Segura, S., Ferreres-Traver, A., Hernández-Baeza, A. & Tomás-Marco, I. (2014). Exploratory Item Factor Analysis. A practical guide revised and up-dated. *Anales de Psicología / Annals of Psychology*, 30(3). 1151-1169

Long, J., Pinzon, S., Wiles, J. & Mitnick, K. D. (2008a). Social Engineering: Here's How I Broke Into Their Buildings. Burlington: Syngress

Long, J. S. & Ervin, L. H. (2000). Using heteroskedasticity consistent standard errors in the linear regression model. *American Statistician*, 54(3). 217-224

Long, J., Wiles, S. P. & Mitnick, K. D. (2008). *No Tech Hacking: A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing*. Burlington: Syngress

Lorenz, J. H. (1992). Größen und Maße in der Grundschule. *Die Grundschule*, *4*(11). 12-14

Loviscach, J. (2015). Hypothesentest, p-Wert und weshalb man damit vorsichtig sein muss. Veröffentlicht unter: *https://www.youtube.com/watch?v=xk3qlX37mvA* (heruntergeladen am 20.04.2019)

Luber, S. & Schmitz, P. (2018). Definition Honeypot und Honeynet. Was ist ein Honeypot? Veröffentlicht unter: *https://www.security-insider.de/was-ist-ein-honeypot-a-703883/* (heruntergeladen am 03.11.2019)

Lumsden, D. B. & Sherron, R. (1978). *Introduction to Educational Gerontology*. Washington: Hemisphere Publ. Corp

MacCallum, R. C., Widaman, K. F., Zhang, S. & Hong, S. (1999). Sample size in factor analysis. *Psychological Methods*, *4*. 87-89

Majlinda, Z. (2018). Cybersecurity Awareness and Beyond. Veröffentlicht unter: *https://www.osce.org/chairmanship/367571?download=true* (heruntergeladen am 18.06.2019)

Malik, M. & Singh, Y. (2015). A Review: DoS and DDoS Attacks. Veröffentlicht unter: *https://www.ijcsmc.com/docs/papers/June2015/V4I6201515.pdf* (heruntergeladen am 12.01.2018)

Markuson, D. (2019). Tipps zur Risikominderung. Smarte Spielzeuge mit Schwachstellen. Veröffentlicht unter: *https://www.datensicherheit.de/aktuelles/tipps-zur-risikominderung-smarte-spielzeuge-mit-schwachstellen-35234* (heruntergeladen am 20.11.2019)

Marlinspike, M. (2016). New Tricks For Defeating SSL In Practice. Veröffentlicht unter: *http://www.blackhat.com/presentations/bh-dc-09/Marlinspike/BlackHat-DC-09-Marlinspike-Defeating-SSL.pdf* (heruntergeladen am 20.04.2019)

Matherly, J. (2019). The search engine for the Internet of Things. Veröffentlicht unter: *https://www.shodan.io/* (heruntergeladen am 12.09.2019)

Matrosov, A., Rodionov, E. & Bratus, S. (2019). *Rootkits and Bootkits.* Reversing Modern Malware and Next Generation Threats. San Francisco: William Pollock

McDowell, M. (2018). US-CERT is part of the Department of Homeland Security. Veröffentlicht unter: *https://www.us-cert.gov/ncas/tips* (heruntergeladen am 07.09.2019)

McGuire, M. & Dowling, S. (2013). Cyber crime: A review of the evidence. Veröffentlicht unter: *https://assets.publishing.service.gov.uk/government/uploads/system/* uploads/attachment_data/file/246751/horr75-chap1.pdf (heruntergeladen am 12.04.2019)

McLaughlin, E. & Muncie, J. (2006). *The SAGE Dictionary of Criminology*. London: Sage

McLuhan, M., Fiore, Q. & Agel, J. (1967). *The Medium is the Message.* An Inventory of Effects. New York: Bantam Books

Meder, N. (2006). *Web-Didaktik*. Duisburg: Bertelsmann

Meier, L. H. (2008). *Koordination interdependenter Planungssysteme in der Logistik.* Einsatz multiagentenbasierter Simulation im Planungsprozess von Container-Terminals im Hafen. Wiesbaden: Gabler

Memorandum über Lebenslanges Lernen (2000), pttps://www.hrk.de/uploads/ tx_szconvention/memode.pdf, (heruntergeladen am 03.04.2019)

Mengering, F. (2011). Probleme der Hypothesenprüfung mittels Signifikanztests. In: Akremi, L., Baur, N. & Fromm, S. (Hrsg). *Datenanalyse mit SPSS für Fortgeschrittene 1.* Datenaufbereitung und uni- und bivariate Statistik (3. Aufl.). Wiesbaden: VS Verlag. S. 293

Mennicken, S., Sack, O. & Ziefle, M. (2011). People and a virtual doctor's visit: learning about multiple facets of acceptance in a telemedical scenario. In: *Workshop User-Centered-Design of Pervasive Health Applications (UCD-PH)*. Aachen: Human Technology Centre RWTH Aachen. S. 57-58

Merten, R. (2008). *Darstellung der Bedrohung durch Social Engineering und Analyse der als Gegenmaßnahme vorhandenen IT-Sicherheitsprozesse am Beispiel eines großen Unternehmens*. Hamburg: Diplomica

Merton, R. K. (1968). The Matthew Effect in Science. The reward and communication systems of science are considered. *Science*, 159(3810). 56-63

Messner, M. (2009). Metasploit. Exploiting Framework – the basics. *HAKIN9*, *6*. 20-25

Metzger, M. (2011). *Erwachsenenbildung in der Sozialen Arbeit*. Heidelberg: VS Verlag

Meyer, B. (2009). *Wie muss die Wirtschaft umgebaut werden?* Perspektiven einer nachhaltigeren Entwicklung. Frankfurt am Main: Fischer

Milne, S., Sheeran, P. & Orbell, S. (2000). Prediction and Intervention in Health-Related Behavior: A Meta-Analytic of Protection Motivation Theory. *Journal of Applied Social Psychology*, 30/1

Mitnick, K. D. & Simon, W. (2003). *Die Kunst der Täuschung*. Frechen: mitp.

Moallem, A. (2019). *Cybersecurity Awareness Among Students and Faculty*. Broken Sound Parkway Northwest: CRC Press

Mocker, M. (2009). What Is Complex About 273 Applications? Untangling Application Architecture Complexity in a Case of European Investment Banking. In: *2009 42nd Hawaii International Conference on System Sciences*. S. 1-14

Mohr, H. (2008). *Einführung in (natur-)wissenschaftliches Denken*. Heidelberg: Springer

Moosbrugger, H. & Kelava, A. (2012). *Testtheorie und Fragebogenkonstruktion* (2. Aufl.). Heidelberg: Springer

Morgan, S. (2019). Global Cybersecurity Spending Predicted To Exceed $1 Trillion. Veröffentlicht unter: *https://cybersecurityventures.com/cybersecurity-market-report/* (heruntergeladen am 08.07.2020)

Moser, K. (2017). *Wirtschaftspsychologie* (2. Aufl.). Wiesbaden: Springer

Müller, W. (2016). Reihe Studienmanuskript (Band 9). Veröffentlicht unter: *https://www.fh-dortmund.de/de/fb/9/personen/lehr/mueller/medien/* (heruntergeladen am 20.05.2019)

Mummendey, H. D. (1988). *Verhalten und Einstellung:* Untersuchung der Einstellungs- und Selbstkonzeptänderung nach Änderung des alltäglichen Verhaltens. Berlin :Springer

Mundfrom, D. J., Shaw, D. G. & Ke, T. L.(2009). Minimum Sample Size Recommendations for Conducting Factor Analyses. *International Journal of Testing*, 5(2). 166

Mutzeck, W. (2007). Pädagogisches Training als Möglichkeit der Vermittlung von Handlungskompetenzen. In: Mutzeck, W. & Popp, K. (Hrsg.). *Professionalisierung von Sonderpädagogen: Standards, Kompetenzen und Methoden*. Weinheim: Beltz. S. 405-419

Narahari, A. C. & Shah, V. (2016). Cyber Crime and Security. A Study on Awareness among Young Netizens of Anand. Veröffentlicht unter: *http://www.ijariie.com/AdminUploadPdf/Cyber_Crime_and_Security_–_A_Study_on_Awareness_among_Young_Netizens_of_Anand__Gujarat_State__India__ijariie3502.pdf* (heruntergeladen am 12.06.2019)

Neigel, A. R., Claypoole, V. L., Waldfogle, G. E., Acharya, S. & Hancock, G. M. (2020). Holistic cyber hygiene education: Accounting for the human factors. *Computers & Security*, *92*

Nerdinger, F. W., Blickle, G. & Schaper, N. (2011). *Arbeits- und Organisations-psychologie* (2. Aufl.). Berlin: Springer

Newman, R. C. (2009). *Computer Security: Protecting Digital Resources.* Massachusetts: Jones and Bartlett

Niemand, T. (2014). *Produktpiraterie:* Eine integrative Analyse der Einflussgrößen, Moderatoren und Mediatoren des Erwerbs von Fälschungen und Raubkopien. Wiesbaden: Springer

North, K. (2016). *Wissensorientierte Unternehmensführung: Wissensmanagement gestalten* (6. Aufl.). Wiesbaden: Springer

NortonLifeLock (2017). Was ist Cyberkriminalität? Veröffentlicht unter: *https://de.norton.com/%0Acybercrime-definition%0A* (heruntergeladen am 03.02.2018)

Novelli, S. (2019). *Hacklog.* Volume 1: Anonymity, IT Security & Ethical Hacking. Handbook. Rom: Independently

O'Connor, B. P. (2000a). SPSS, SAS, MATLAB, and R Programs for Determining the Number of Components and Factors Using Parallel Analysis and Velicer's MAP Test. Veröffentlicht unter: *https://people.ok.ubc.ca/brioconn/nfactors/parallel.sps* (heruntergeladen am 07.07.2019)

O'Connor, B. P. (2000b). SPSS and SAS programs for determining the number of components using parallel analysis and Velicer's MAP test. *Behavior Research Methods*, 32. 396-402

O'Leary, M. (2019). *Cyber Operations.* Building, Defending, and Attacking Modern Computer Networks (2. Aufl.). Towson: Apress

Obrecht, W. (1996). Das Theorie-Praxis-Problem als Problem der Ausbildung. In: SASSA (Hrsg.): *Das Theorie-Praxis-Problem als Problem der Ausbildung in Sozialer Arbeit*. Luzern: Sassa. S. 31-70

Oliver, A. (2018). Student stellt DDoS-Tool X4U Doser bereit. Veröffentlicht unter: *https://www.link11.com/de/blog/student-stellt-ddos-tool-x4u-doser-bereit/* (heruntergeladen am 20.01.2019)

Oppliger, R. (2016). *SSL and TLS: Theory and Practice* (Second Edition). London: Artech House

Ortner, G. E. (2016). Den Umgang mit den Massenmedien muss man erst lernen. *L.A. multimedia, Netucation*, 03. 16

Ozkaya, E. (2018). *Learn Social Engineering, Learn the art of human hacking with an internationally renowned expert*. Birmingham: Packt Publishing

Pahnila, S., Siponen, M. & Mahmood, A. (2007). Employees' Behavior towards IS Security Policy Compliance. Veröffentlicht unter: *https://www.computer.org/csdl/proceedings/hicss/2007/2755/00/27550156b.pdf* (heruntergeladen am 03.04.2019)

Park, C.-Y. (1999). *The Illusion of Knowing.* The Role of Perceived Self-knowledge in News Media Impact During an Election Campaign. Michigan: Michigan State University

Pätzold, G. (2006). Vermittlung von Fachkompetenz in der Berufsbildung. In: Arnold, R., Lipsmeier, A. (Hrsg.). *Handbuch der Berufsbildung* (2. Aufl.). Wiesbaden: Springer

Paul, G. L. (1967). Strategy of Outcome Research in Psychotherapy. *Journal of Consulting Psychology*, 31(2), 111

Peterßen, W. H. (1982). *Handbuch der Unterrichtsplanung.* Grundfragen, Modelle, Stufen, Dimensionen. München: Ehrenwirth

Peterßen, W. H. (2001). *Lehrbuch Allgemeine Didaktik*. München: Oldenbourg

Petty, R. & Cacioppo, J. (1986). *Communication and Persuasion.* Central and Peripheral Routes to Attitude Change. New York: Springer

Petty, R. E., Cacioppo, J. T. & Goldman, R. (1981). Personal involvement as a determinant of argument-based persuasion. *Journal of Personality and Social Psychology*, 41. 847-855

Pfadenhauer, M. & Kurtz, T. (2010). *Soziologie der Kompetenz*. Wiesbaden: VS Verlag

Pfajfar, M. (2019). Tor. Cambridge: Electronic Frontier Foundation. Veröffentlicht unter: *https://www.torproject.org/about/history/* (heruntergeladen am 08.07.2019)

Pierce, W., Cheney, C. (2013). *Behavior Analysis and Learning* (5. Aufl.). New York: Psychology Press

Piotrowski, M. (2005). Dangerous Google – Searching for Secrets. *hakin9*, 4. 2-12

Pogue, C. (2018). Welcome to The Black Report 2018. Veröffentlicht unter: *https://www.nuix.com/sites/default/files/report_nuix_black_report_2018_web_us.pdf* (heruntergeladen am 13.04.2019)

Pokoyski, D. & Pütz, S. (2014). *Corporate Audiobooks.* Hörspiele, Features & Co. in der Unternehmenskommunikation. Wiesbaden: Springer

Pollino, D., Pennington, B., Bradley, T. & Dwivedi, H. (2006). *Hacker's Challenge 3: 20 Brand New Forensic Scenarios & Solutions*. New York: McGraw-Hill

Porschen, H. (2020). So tickt und klickt Deutschland. Gesellschaft im Wandel – Wie digitaler Konsum und soziale Medien den Alltag der Deutschen prägen. Veröffentlicht unter: *https://docs.zoho.com/file/7lcp747cc095693f34f03adff5aa9d9c72f8f* (heruntergeladen am 25.06.2020)

Portnoff, R., Lee, L., Egelman, S., Mishra, P., Leung, D. & Wagner, D. (2015). Somebody's Watching Me? Assessing the Effectiveness of Webcam Indicator Lights. Veröffentlicht unter: *https://www.guanotronic.com/%7B~%7Dserge/papers/chi15-webcam.pdf* (heruntergeladen am 11.07.2019)

Prexl, L. (2016). *Mit digitalen Quellen arbeiten*. Richtig zitieren aus Datenbanken, E-Books, YouTube und Co. (2. Aufl.). Paderborn: Schöningh

Prochaska, J. O. & Diclemente, C. C. (1983). Stages and Processes of Self-Change of Smoking - toward an Integrative Model of Change. *Journal of Consulting and Clinical Psychology,* 51(3). 390-395

Prochaska, J. O. & Prochaska, J. M. (2016). *CHANGING TO THRIVE: Using the Stages of Change to Overcome the Top Threats to Your Health and Happiness*. Minnesota: Hazelden Publishing

Purpura, P. (2018). *Security and Loss Prevention* (7. Aufl.). Waltham: Elsevier

PwC (2016). Turnaround and transformation in cybersecurity: Key findings from The Global State of Information Security Survey 2016. Veröffentlicht unter: *https://www.pwc.com/sg/en/publications/assets/pwc-global-state-of-information-security-survey-2016.pdf* (heruntergeladen am 21.10.2019)

PWC (2018). Digitisation A Quantitative and Qualitative Market Research Elicitation. Veröffentlicht unter: *https://www.pwc.de/de/digitale-transformation/pwc-digitisation-market-research-update.pdf* (heruntergeladen am 25.06.2020)

Quilling, E. & Nicolini, H. J. (2007). *Erfolgreiche Seminargestaltung.* Strategien und Methoden in der Erwachsenenbildung. Wiesbaden: VS Verlag für Sozialwissenschaften

Rabe, L. (2019). Anteil der Internetnutzer nach Geschlecht in Deutschland in den Jahren 2001 bis 2018. Veröffentlicht unter: *https://de.statista.com/statistik/daten/studie/3100/umfrage/internetnutzung-in-deutschland-nach-geschlecht-seit-2001/* (heruntergeladen am 03.02.2020)

Rabenstein, K. (2003). *In der gymnasialen Oberstufe fächerübergreifend lehren und lernen:* Eine Fallstudie über die Verlaufslogik fächerübergreifenden Projektunterrichts und die Erfahrungen der Schüler. Wiesbaden: Springer

Raithel, J. (2008). *Quantitative Forschung: Ein Praxiskurs*. Wiesbaden: Springer

Rasch, B., Friese, M., Hofmann, W. & Naumann, E. (2010). *Quantitative Methoden 1.* Einführung in die Statistik für Psychologen und Sozialwissenschaftler (3. Aufl.). Berlin: Springer

Rasch, B., Friese, M., Hofmann, W. & Naumann, E. (2014). *Quantitative Methoden 2.* Einführung in die Statistik für Psychologen und Sozialwissenschaftler (4. Aufl.). Berlin: Springer

Raulff, U. & Lepper, M. (2016). *Handbuch Archiv: Geschichte, Aufgaben, Perspektiven*. Stuttgart: J. B. Metzler

Rech, S. (2006). Wie eine andere Welt. Eine Grounded Theory-Studie zur Frage der Teilhabe von Eltern an schulischer Kommunikation am Beispiel von RealschülerInnen. Veröffentlicht unter: *https://d-nb.info/981499953/34* (heruntergeladen am 22.05.2019)

Redmiles, E., Malone, A. & Mazurek, M. (2016). *I Think They're Trying to Tell Me Something.* Advice Sources and Selection for Digital Security. Maryland: University of Maryland

Refsdal, A., Solhaug, B. & Stølen, K. (2015). *Cyber-Risk Management*. Heidelberg: Springer

Reiber, L. (2019). *Mobile Forensic Investigations: A Guide to Evidence Collection, Analysis, and Presentation* (2. Aufl.). New York: McGraw-Hill Professional Publishing

Reibold, H. (2015). *WLAN Security kompakt: Praxiseinstieg in das Penetration Testing von drahtlosen Netzwerken*. Saarbrücken: Brain-Media

Reich-Claassen, J. (2010). *Warum Erwachsene (nicht) an Weiterbildungsveranstaltungen partizipieren:* Einstellungen und prägende Bildungserfahrungen als Regulative des Weiterbildungsverhaltens. Eine qualitativ-explorative Untersuchung erwartungswidriger Teilnahme und Nichtteilnahme. München: Lit

Reich, K. (1977). *Theorien der Allgemeinen Didaktik:* Zu den Grundlinien didaktischer Wissenschaftsentwicklung in der Bundesrepublik Deutschland und in der Deutschen Demokratischen Republik. Stuttgart: Klett

Reich, K. (1998). *Die Ordnung der Blicke:* Perspektiven des interaktionistischen Konstruktivismus. Berlin: Luchterhand

Reich, K. (2005). Konstruktivistische Didaktik - Kontexte und handlungsbezogene Perspektiven. Veröffentlicht unter: *http://konstruktivismus.uni-koeln.de/reich_works/aufsatze/reich_68.pdf* (heruntergeladen am 24.05.2019)

Reichardt, J. (2011). *Lehrbuch Digitaltechnik:* Eine Einführung mit VHDL (2. Aufl.). München: Oldenbourg

Reimann, G. (2018). *Betrieblicher Datenschutz Schritt für Schritt - gemäß EU-Datenschutz-Grundverordnung:* Lösungen zur praktischen Umsetzung. Textbeispiele, Musterformulare, Checklisten. Berlin: Beuth

Reimann, J. (2015). Die Website = Ihre Internetpräsenz. Veröffentlicht unter: *https://www.textschoepfung.de/warum-eine-homepage-keine-website-ist-und-eine-website-keine-webseite/* (heruntergeladen am 21.04.2020)

Reinmann-Rothmeier, G. & Mandl, H. (2001). Unterrichten und Lernumgebungen gestalten. In: Krapp, A. & Weidenmann, B. (Hrsg.). *Pädagogische Psychologie. Ein Lehrbuch* (4., vollst. überarb. Aufl.). Weinheim: Beltz. S. 601-646

Reiss, M. & Reiss, G. (2009). *Praxisbuch IT-Dokumentation*. München: Addison-Wesley

Renneberg, B. & Hammelstein, P. (2006). *Gesundheitspsychologie*. Heidelberg: Springer

Ribolits, E. (2006). Was hat das mit Bildung zu tun? Lernen statt revoltieren? In: Ribolits, E., Sertl, M. & Zuber, J. (Hrsg.). *Verlierer im Überfluss.* Bildungssystem und Ungleichheit – Aspekte eines diffusen Zusammenhangs. Innsbruck: StudienVerlag.

Rid, T. & Buchanan, B. (2015). Attributing Cyber Attacks. *The Journal of Strategic Studies*, 38. 4-37

Riedl, A. (2004). *Grundlagen der Didaktik*. Wiesbaden: Franz Steiner

Riedl, R. (2000). *Strukturen der Komplexität.* Eine Morphologie des Erkennens und Erklärens. Berlin, Heidelberg: Springer

Rist, L., Vestergaard, J., Haslinger, D. & Pasquale, A. (2018). Conpot ICS/SCADA Honeypo. Veröffentlicht unter: *http://conpot.org* (heruntergeladen am 14.05.2019)

Ristic, I. (2014). *Understanding and deploying SSL/TLS and PKI to secure servers and web applications*. London: Feisty Duck

Röbe, E. (2019). *Lehrer werden - Lehrer sein - Lehrer bleiben:* Ein Praxisbuch zur Professionalisierung. Stuttgart: UTB

Rocha, Á. & Guarda, T. (2018). *Proceedings of the International Conference on Information Technology & Systems (ICITS 2018)*. Cham: Springer

Rodgers, M. (2000). A new hacker taxonomy. Veröffentlicht unter: *http://homes.cerias.purdue.edu/%7B~%7Dmkr/hacker.doc* (heruntergeladen am 03.12.2020)

Roeske, T. (2018). WLAN-Tracking: Vorteile und Datenschutz-Risiken. Veröffentlicht unter: *https://www.datenschutzbeauftragter-info.de/wlan-tracking-vorteile-und-datenschutz-risiken/* (heruntergeladen am 20.05.2020)

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology*, 91. 93-114

Rohlfes, J. (1997). Exemplarischer Geschichtsunterricht. In: Bergmann, K. (Hrsg.). *Handbuch der Geschichtsdidaktik* (5., überarb. Aufl.). Seelze: Velber. S. 280

Roper, C., Grau, J. & Fischer, L. (2006). *Security Education, Awareness, And Training, From Theory to Practice*. Amsterdam: Elsevier

Rosenstock, R., Schweiger, A. & Schubert, C. (2016). *Studie: Der Medienkompass Mecklenburg-Vorpommern (II)*. Schwerin: Medienanstalt Mecklenburg-Vorpommern Rosenthal, R. (1976). *Experimenter effects in behavioral research*. New York: Wiley Publishing

Rothgangel, S. (2010). *Medizinische Psychologie und Soziologie*. Stuttgart: Thieme

Rotter, J. B. (1975). Some problems and misconceptions related to the construct of internal versus external control of reinforcement. *Journal of Consulting and Clinical Psychology*, 43(1). 56-67

Rouse, M. (2016). Watering-Hole-Angriff - Auflauern an der Wasserstelle. Veröffentlicht unter: *https://www.computerweekly.com/de/definition/Watering-Hole-Angriff-Auflauern-an-der-Wasserstelle* (heruntergeladen am 21.04.2020)

Rouse, M. (2018). *Social Engineering*. München: TechTarget

Ruprecht, H. (1977). *Medienwahl und Medienverwendung*. Bonn/Frankfurt am Main: Deutsches Institut für Erwachsenenbildung

Saalbach, K. (2017). Attribution of Cyber Attacks Methods and Practice. Veröffentlicht unter: *https://repositorium.ub.uni-osnabrueck.de/bitstream/urn:nbn:de:gbv:700-2017022015577/2/Attribution_of_Cyber_Attacks_Saalbach.pdf* (heruntergeladen am 27.07.2019)

Sackmann, R. & Winkler, O. (2013). Technology generations revisited: The internet generation. *Gerontechnology*, 3. 497

Salkind, N. J. (2007). *Encyclopedia of Measurement and Statistics*. Teller Road: Sage

Samuel, A. (2004). *Hacktivism and the Future of Political Participation*. Cambridge: Harvard University

SanNicolas-Rocca, T., Schooley, B. & Spears, J. L. (2014). *Designing Effective Knowledge Transfer Practices to Improve IS Security Awareness and Compliance. Hawaii: San Jose State University, University of South Carolina, DePaul University*

Sauldie, S. (2014). *Digital Leadership für Führungskräfte von morgen.* Die iROI-Strategie für Leader: digital führen - digilog leben. Norderstadt: Books on Demand

Sauter, R., Sauter, W. & Wolfig, R. (2018). *Agile Werte- und Kompetenzentwicklung:* Wege in eine neue Arbeitswelt. Berlin: Springer

Scarbath, H. & Beyer-Stiepani, T. (2012). *Handbuch Trainingskompetenz.* Multiplikatorenkonzept für die betriebliche Weiterbildung. Birmingham: Bertelsmann

Schäfer, E. (2017). *Lebenslanges Lernen.* Erkenntnisse und Mythen über das Lernen im Erwachsenenalter. Berlin: Springer

Schäfer, T. (2016). *Methodenlehre und Statistik:* Einführung in Datenerhebung, deskriptive Statistik und Inferenzstatistik. Wiesbaden: Springer

Scheer, A. W. (2000). *E-Business* - Wer geht? Wer bleibt? Wer kommt? Heidelberg: Physica

Schicke, H., Felden, H. & Schäffter, O. (2014). *Denken in Übergängen: Weiterbildung in transitorischen Lebenslagen*. Wiesbaden: Springer

Schiersmann, C. (1987). *Computerkultur und weiblicher Lebenszusammenhang.* Zugangsweisen von Frauen und Mädchen zu neuen Technologien. Bad Honnef: Bock

Schillerhof, T. (2018). *Amazon Echo - Das ultimative Handbuch: Anleitung, Alexa-App, Skills, Smart Home, Sprachbefehle, IFTTT*. München: BookRix

Schmidt-Lauff, S (2018). Zeittheoretische Implikationen in der Erwachsenenbildung. In: Tippelt, R. & Hippel, A. (Hrsg.). *Handbuch Erwachsenenbildung/Weiterbildung* (6. Aufl.). Wiesbaden: Springer. S. 323

Schmitz, P. (2020). Phishing setzt auf den Leichtsinn der Opfer. Veröffentlicht unter: *https://www.security-insider.de/phishing-setzt-auf-den-leichtsinn-der-opfer-a-942904/?xing_share=news* (heruntergeladen am 14.06.2020)

Schneider, K. (2019). Onlinebanking: Hacker finden immer neue Sicherheitslücken. Veröffentlicht unter: *https://www.handelsblatt.com/finanzen/banken-versicherungen/angriffe-mit-schadsoftware-wie-sich-bankkunden-vor-hacker-angriffen-auf-das-smartphone-schuetzen-koennen/24860678.html* (heruntergeladen am 21.11.2019)

Scholl, M. (2017a). Informationssicherheitsbewusstsein für den Berufseinstieg. Veröffentlicht unter: *https://secaware4job.wildau.biz/#lernszenarien* (heruntergeladen am 21.11.2019)

Scholl, M. (2017b). Stärkefaktor Mensch: Digitalisierung nicht ohne Informationssicherheit, Informationssicherheit nicht ohne Awareness. Veröffentlicht unter: *https://www.th-wildau.de/files/Beschaeftigte/Margit_Scholl/20171207_Dialog_IT-Sicherheit_Frankfurt-Oder_ms-final-Druckversion.pdf* (heruntergeladen am 04.08.2019)

Scholl, M., Fuhrmann, F. & Pokoyski, D. (2016). *Information security awareness training 3.0 for young professionals*. Wildau: Technischen Hochschule Wildau

Schorb, B. (2009). Gebildet und kompetent. Medienbildung statt Medienkompetenz? *Medien und Erziehung. Zeitschrift für Medienpädagogik*, 53(5). 50-56

Schorb, B. (2020). Medienkompetenz als Ergebnis gelungener Medienaneignung. Veröffentlicht unter: http://www.nuernberg.de/imperia/md/buendnis_fuer_familie/dokumente/bernd_schorb_vortrag.pdf (heruntergeladen am 04.09.2020)

Schrittwieser, S. & Katzenbeisser, S. (2011). *Information Hiding 13th International Conference*. Wiesbaden: Springer

Schröder, H. (2002). *Lernen – Lehren – Unterricht*. München: Oldenbourg

Schuler, H., Brandstätter, H., Bungard, W., Greif, S., Ulich, E. & Wilpert, B. (1995). *Lehrbuch Organisationspsychologie* (2. Aufl.). Bern: Hans Huber

Schumacher, M. & Barczok, A. (2017). Keygrabber Wi-Fi Premium: Mini-Adapter schneidet alles mit (im Video). Veröffentlicht unter: *https://www.heise.de/ct/artikel/Keygrabber-Wi-Fi-Premium-Mini-Adapter-schneidet-alles-mit-im-Video-3814161.html* (heruntergeladen am 06.05.2020)

Schumacher, M., Roedig, U. & Moschgath, M.-L. (2003). *Hacker Contest: Sicherheitsprobleme, Lösungen, Beispiele*. Berlin: Springer

Schwarz, J. (2012). *Modul: Statistik Itemanalyse / Skalenanalyse / Faktoranalyse*. Bern: Berner Fachhochschule

Schwarz, J. & Enzler, H. B. (2019). Methodenberatung. Veröffentlicht unter: *https://www.methodenberatung.uzh.ch/de/datenanalyse_spss/unterschiede/zentral/mvarianz.html* (heruntergeladen am 24.09.2019)

Schwarz, J. & Kohler, F. (2019). Empiricial Methods. Ressourcen für empirische Methoden. Veröffentlicht unter: *https://www.empirical-methods.hslu.ch/entscheidbaum/interdependenzanalyse/reduktion-der-variablen/faktoranalyse/#1* (heruntergeladen am 03.07.2019)

Global Human Capital Trends 2016 (2016). Veröffentlicht unter: *https://www2.deloitte.com/content/dam/Deloitte/global/Documents/* (heruntergeladen am 20.04.2019)

Schwarzer, R. & Jerusalem, M. (1999). *Skalen zur Erfassung von Lehrer- und Schülermerkmalen.* Dokumentation der psychometrischen Verfahren im Rahmen der Wissenschaftlichen Begleitung des Modellversuchs Selbstwirksame Schulen. Berlin: Freie Universität Berlin

Schwarzer, R. & Jerusalem, M. (2002). Das Konzept der Selbstwirksamkeit. *Zeitschrift für Pädagogik,* 44. 28-53

Sedlmeier, P. & Renkewitz, F. (2013). *Forschungsmethoden und Statistik: Ein Lehrbuch für Psychologen und Sozialwissenschaftler* (2. Aufl.). München: Pearson Education

Seligman, M. E. P. (1979). *Erlernte Hilflosigkeit*. München: Urban & Schwarzenberg

Selinger, M. (2013). Adobe & Java Make Windows Insecure. *AV-TEST*. Veröffentlicht unter: *https://www.av-test.org/en/news/adobe-java-make-windows-insecure/* (heruntergeladen am 03.02.2019)

Shackleford, D. (2019). Penetrationstests mit Social Engineering: Vier effektive Techniken. Veröffentlicht unter: *https://www.searchsecurity.de/tipp /Penetrationstests-mit-Social-Engineering-Vier-effektive-Techniken* (heruntergeladen am 04.01.2020)

Shamsi, J. & Flowers, A. (2016). Attribution in cyberspace: techniques and legal implications: SCN-SI-088. *Security and Communication Networks*, 10. 13

Shay, R., Bauer, L., Christin, N. & Cranor, L. (2015). *A Spoonful of Sugar? The Impact of Guidance and Feedback on Password-Creation Behavior*. Pittsburgh: Carnegie Mellon University.

Shay, R., Ion, I., Reeder, R. & Consolvo, S. (2014). My religious aunt asked why I was trying to sell her viagra: Experiences with account hijacking. Veröffentlicht unter: *https://storage.googleapis.com/pub-tools-public-publication-data/pdf/41941.pdf* (heruntergeladen am 19.05.2019)

Shepherd, L. A. & Archibald, J. (2017). *Security Awareness and Affective Feedback:* Categorical Behaviour vs. Reported Behaviour. Dundee: Abertay University.

Siebert, H. (1977). Thesen und Materialien zur Didaktik und Methodik. In: Siebert, H., Gerl, H., Recktenwald, H., Schaffner, L., Schlutz, E., Tietgens, H. & Weinberg, J. (Hrsg.). *Praxis und Forschung in der Erwachsenenbildung*. Opladen: Westdeutscher Verlag. S. 132

Siebert, H. (2012). *Didaktisches Handeln in der Erwachsenenbildung:* Didaktik aus konstruktivistischer Sicht. Augsburg: Ziel

Singer, T. (2019). *Dehumanisierung der Kriegführung:* Herausforderungen für das Völkerrecht und die Frage nach der Notwendigkeit menschlicher Kontrolle. Berlin: Springer

Singh, A., Adeyemi, I. & Venter, H. (2019). Digital Forensic Readiness Framework for Ransomware Investigation: 10th International EAI Conference, ICDF2C 2018, New Orleans, LA, USA, September 10-12, 2018, Proceedings. In: Breitinger, F., Baggili, I. (Hrsg). *Digital Forensics and Cyber Crime 10th International EAI Conference, ICDF2C 2018 New Orleans, LA, USA, September 10-12, 2018 Proceedings*. Wiesbaden: Springer. S. 91-105

SINUS-Institut (2017). Wenn es um vertrauliche Informationen geht - Brief oder E-Mail? DIVSI Studie über die Kommunikation im privat-geschäftlichen Bereich. Veröffentlicht unter: *https://www.divsi.de/wp-content/uploads/2018/01/brief-mail.pdf* (heruntergeladen am 03.02.2019)

Smigierski, J. (2019). Mauchly Test & Sphärizität in SPSS. Veröffentlicht unter: *https://www.beratung-statistik.de/statistik-beratung-infos/spss-tips/mauchly-test-sphaerizitaet-spss/* (heruntergeladen am 03.07.2019)

Solms, S. H. & Solms, R. (2009). *Information Security Governance*. New York: Springer Science & Business Media

Song, M., Seo, J. & Lee, K. (2015). *Study on the effectiveness of the security countermeasures against spear phishing.* In: Information Security Applications - 15th International Workshop, WISA 2014, Revised Selected Papers. Vol. 8909. pp. 394-404

Sorge, C., Lo Iacono, L. & Gruschka, N. (2013). *Sicherheit in Kommunikationsnetzen*. München: Oldenbourg

Sowa, A. (2017). *IT-Prüfung, Sicherheitsaudit und Datenschutzmodell:* Neue Ansätze für die IT-Revision. Wiesbaden: Springer

Spanhel, D. (1999). *Integrative Medienerziehung in der Hauptschule.* Ein Entwicklungsprojekt auf der Grundlage responsiver Evaluation. München: KoPäd

Spitzer, M. (2012). *Digitale Demenz:* Wie wir uns und unsere Kinder um den Verstand bringen. München: Droemer

Spitzer, M. (2015). *Cyberkrank! Wie das digitalisierte Leben unsere Gesundheit ruiniert*. Ulm: Droemer

Spring, T. (2005). Web of Crime: Who's Catching the Cybercrooks? Veröffentlicht unter: *https://www.pcworld.com/article/122245/article.html* (heruntergeladen am 18.09.2019)

Stanjek, K. (2020). *Altenpflege konkret Sozialwissenschaften* (7. Aufl.). München: Elsevier

Statista (2017). Welche Dinge im Leben sind Ihnen außerordentlich wichtig und erstrebenswert? Veröffentlicht unter: *https://de.statista.com/statistik/daten/studie/321901/umfrage/umfrage-unter-jungen-erwachsenen-zu-den-wichtigsten-dingen-im-leben/* (heruntergeladen am 04.08.2019)

Steffen, A. (2019). *Impulse zur eigenen Veränderung:* Selbstcoaching mit dem Prinzip von Weniger und Mehr (1. Aufl.). Berlin: Springer

Steffens, T. (2018). *Auf der Spur der Hacker:* Wie man die Täter hinter der Computer-Spionage enttarnt. Berlin: Springer

Steinhaus, I. (2018). Software-Schwachstellen als Handelsware. Veröffentlicht unter: *https://www.it-zoom.de/it-director/e/software-schwachstellen-als-handelsware-19661/* (heruntergeladen am 18.09.2019)

Stern, S. (2002). *Organisationsentstehung in innovativen Neugründungen:* Kommunikation und Organisation in jungen Multimediaunternehmen. Wiesbaden: Deutscher Universitäts-Verlag

Stevens, J. P. (2002). *Applied Multivariate Statistics for the Social Science* (4. Aufl.). London: Routledge

Stimmer, F. (2000). *Grundlagen des methodischen Handelns in der Sozialen Arbeit*. Stuttgart: Kohlhammer

Stoetzer, M. W. (2017). *Regressionsanalyse in der empirischen Wirtschafts- und Sozialforschung* (Band 1). Eine nichtmathematische Einführung mit SPSS und Stata. Berlin: Springer

Stone, G. P. & Hagoel, L. (1978). Über den Umgang mit Motiven. In: Hammerich, K & Klein, M (Hrsg.) . *Materialien zur Soziologie des Alltags.* Wiesbaden: Springer VS. S. 47

Symantec Corporation (2009). Cyberkriminalität. Veröffentlicht unter: https://de.norton.com/cybercrime-definition (heruntergeladen am 20.06.2018)

Symantec Corporation (2018). Norton Cyber Security Insights Report 2017. Tempe: Symantec Corporation

Technische Universität Dresden (2009). Kompetenzpass für Weiterbildner/innen. Erwachsenenpädagogische Kompetenzen bilanzieren. Veröffentlicht unter: *http://tu-dresden.de/die_tu_dresden/%0Afakultaeten/erzw/erzwibp/eb/forschung/%0AGesamt_Handreichung.pdf* (heruntergeladen am 20.06.2020)

Technologies Wombat Security (2017). User Risk Report Results of an international cybersecurity awareness survey. Veröffentlicht unter: *https://cdn2.hubspot.net/hubfs/372792/2017/*User Risk Report/Wombat 2017 Report.pdf (heruntergeladen am 04.05.2018)

Ternès, A. & Hagemes, H.-P. (2018). *Die Digitalisierung frisst ihre User:* Der digitale Wahnsinn und wie Sie ihn beherrschen. Wiesbaden: Springer

Teymourlouei, H. (2015). Quick Reference: Cyber Attacks Awareness and Prevention Method for Home Users. World Academy of Science, Engineering and Technology. *International Journal of Computer, Electrical, Automation, Control and Information Engineering*, 9. 678-684

Thomas, V. (2014). *Social Engineering in Most Attacks Are Targeted in Building an Information Security Awareness Program.* Amsterdam: Elsevier

Thorndike, E. L. (1920). A constant error in psychological ratings. *Journal of Applied Psychology*, 4(1). 25-29

Tietgens, H. (1992). *Refexionen zur Erwachsenenbildungsdidaktik*. Bad Heilbrunn: Klinkhardt

Tiongson, R. (2015). Using MK5 Karma wifi pineapple Mark V. Veröffentlicht unter: *https://www.youtube.com/watch?v=h234luDi6D8* (heruntergeladen am 20.06.2020)

Tischer, M., Durumeri, Z., Foster, S., Duan, S., Mori, A., Bursztein, E. & Bailey, M. (2013). Users Really Do Plug in USB Drives They Find. Veröffentlicht unter: *https://zakird.com/papers/usb.pdf%0A* (heruntergeladen am 14.06.2019)

TMG (2007). Telemediengesetz. Veröffentlicht unter: https://www.gesetze-im-internet.de/tmg/BJNR017910007.html (heruntergeladen am 14.06.2019)

Tonry, M. & Farrington, D. P. (1995). Strategic Approaches to Crime Prevention: Crime & Just. Veröffentlicht unter: *https://pdfs.semanticscholar.org/82c3/00f77c242a1dd77af552e647ae233679054d.pdf* (heruntergeladen am 14.06.2019)

Tsolkas, A. & Schmidt, K. (2017). *Rollen und Berechtigungskonzepte:* Identity- und Access-Management im Unternehmen (2. Aufl.). Wiesbaden: Springer

Tufin Survey Finds One in Six New York Teenagers Hack - And Rarely Get Caught(2010). Veröffentlicht unter: *https://www.tufin.com/pr/tufin-survey-finds-one-in-six-new-york-teenagers-hack-and-rarely-get-caught* (heruntergeladen am 24.05.2019)

Tulodziecki, G. (2010). Standards für die Medienbildung als eine Grundlage für die empirische Erfassung von Medienkompetenz-Niveaus. In: Niesyto, H., Meister, D. M. & Mosrer, H. (Hrsg.). *Jahrbuch Medienpädagogik 8: Medienkompetenz und Web 2.0*. Wiesbaden: VS Verlag. S. 85

UBM (2018). Black Hat. Veröffentlicht unter: *https://www.blackhat.com/about.html* (heruntergeladen am 03.02.2019)

UNESCO (2005). Global Monitoring Report. Education for All. Literacy for life. Veröffentlicht unter: *http://unesdoc.unesco.org/images/0014/001416/141639e.pdf* (heruntergeladen am 04.05.2020)

Urban, D. & Mayerl, J. (2011). *Regressionsanalyse: Theorie, Technik und Anwendung*. Wiesbaden: VS Verlag

Urban, D. & Mayerl, J. (2018). *Angewandte Regressionsanalyse: Theorie, Technik und Praxis* (5. Aufl.). Wiesbaden: Springer

Urton, K. (2017). Selbstwirksamkeitserwartung – Was bedingt sie und wie kann sie gefördert werden? Veröffentlicht unter: *https://www.uni-potsdam.de/fileadmin01/projects/inklusion/PDFs/ZEIF-Blog/Urton_2017_Selbstwirksamkeitserwartung.pdf* (heruntergeladen am 04.08.2019)

van Elsbergen, G. (2005). *Chancen und Risiken kommunaler Kriminalprävention:* Eine qualitativ-empirische Analyse. Osnabrück: VS Verlag

Vick, J. & Roters, F. (2003). Account-Missbrauch im Internet. Ein Sammelverfahren mit anschließender kriminologischer Auswertung. Veröffentlicht unter: *https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/Publikationsreihen/Forschungsergebnisse/2003AccountMissbrauchImInternet.pdf* (heruntergeladen am 14.09.2019)

Vierbuchen, M. C. (2015). *Förderung sozial-kognitiver Informationsverarbeitung im Jugendalter:* Konzeption und Evaluation eines Förderprogramms unter besonderer Berücksichtigung spezifischer Risikofaktoren für schulischen Dropout. Oldenburg: Universität Oldenburg

Viertl, R. K. W. (1990). *Einführung in die Stochastik mit Elementen der Bayes-Statistik und Ansätzen für die Analyse unscharfer Daten*. Wien: Springer

Vieweg, W. (2015). *Management in Komplexität und Unsicherheit: Für agile Manager*. Wiesbaden: Springer

Vitalwerks Internet Solutions (2018). Offensive Security's Exploit Database Archive. Veröffentlicht unter: *https://www.exploit-db.com/about-exploit-db/* (heruntergeladen am 28.05.2019)

Vladimirovich, S. N. (2018). *Аудит безопасности информационных систем*. Saint Petersburg: Piter Publishing

Vogel, M. (2016). Der „Mere-Exposure-Effekt" in der Mensch-Technik-Interaktion und seine Auswirkungen auf das Nutzererleben. Veröffentlicht unter: *https://depositonce.tu-berlin.de/bitstream/11303/6024/6/vogel_marlene.pdf* (heruntergeladen am 14.07.2019)

Vogelgesang, W., Wetzstein, T. A. & Winter, R. (2017). *Auf digitalen Pfaden:* Die Kulturen von Hackern, Programmierern, Crackern und Spielern. Wiesbaden: Springer

von Alemann, H. (1977). *Der Forschungsprozeß:* Eine Einführung in die Praxis der empirischen Sozialforschung. Stuttgart: Teubner

von Bothmer, C. (2017). *Studie: Digitale Inklusion von Senioren durch gezielte Unterstützung*. München: Telefónica Deutschland Holding AG

von Roehl, S. (2005). Modelle der Informationsverarbeitung. Veröffentlicht unter: *https://www.phil-fak.uni-duesseldorf.de/sozwiss/mewi1/reader/ss05/vonroehl/ModellederInformationsverarbeitung_Zsf.pdf* (heruntergeladen am 04.05.2020)

Warren, T. (2017). Microsoft confirms some Windows 10 source code has leaked. Veröffentlicht unter: *https://www.theverge.com/2017/6/24/15867350/microsoft-windows-10-source-code-leak* (heruntergeladen am 20.03.2018)

Watson, G., Mason, A. & Ackroyd, R. (2014). *Social Engineering Penetration Testing:* Executing Social Engineering Pen Tests, Assessments and Defense (1 Aufl.). Rockland: Syngress Publishing

Weinberg, G. M. (2004). *Die Psychologie des Programmierers:* Seine Persönlichkeit, sein Team, sein Projekt. Frechen: mitp.

Weis, E. (2017). Diese Arten von Cyberkriminalität sollten Unternehmen kennen: Was ist Cyberkriminalität? Veröffentlicht unter: *https://www.brandmauer.de/blog/it-security/diese-arten-von-cyberkriminalitaet-sollten-unternehmen-kennen-teil-1* (heruntergeladen am 20.03.2018)

Weissinger, L. (2017). Modelling Trust and Trust-Building Among IT-Security Professionals. Veröffentlicht unter: *https://doi.org/10.1007/978-3-319-58460-7_39* (heruntergeladen am 03.08.2018)

Welp, K. & Kaufmann, N. (2018). Hinweise für IT-Administratoren. Veröffentlicht unter: *https://www.dfn.de/fileadmin/3Beratung/Recht/Wissensbasis/Hinweise_fuer_IT-Administratoren.pdf* (heruntergeladen am 03.02.2019)

Wendekamm, M. & Frevel, B. (2017). *Sicherheitsproduktion zwischen Staat, Markt und Zivilgesellschaft*. Wiesbaden: Springer

Weyer, J. (2009). Dimensionen der Komplexität und Perspektiven des Komplexitätsmanagements. In: Weyer, J. & Schulz-Schaeffer, I. (Hrsg.). *Management komplexer Systeme*. München: Oldenbourg.

Whitman, M. E. & Mattord, H. J. (2008). *Principles of information security* (3. Aufl.). Stanford: Course Technology

Whitman, M. E. & Mattord, H. J. (2017). *Principles of Information Security* (6. Aufl.). Boston: Cengage Learning

Wicker, A. W. (1971). An examination of the "other variables" explanation of attitude-behavior inconsistency. *Journal of Personality and Social Psychology*, 19. 18-30

Wickert, C. (2020). Kriminalitätsfurcht. Veröffentlicht unter: *https://soztheo.de/kriminologie/kriminalitaetsfurcht/* (heruntergeladen am 16.04.2020)

Wilkens, I. & Leber, U. (2003). Partizipation an beruflicher Weiterbildung: Empirische Ergebnisse auf Basis des Sozio-Ökonomischen Panels. In: *Mitteilungen aus der Arbeitsmarkt- und Berufsforschung*. Nürnberg: Institut für Arbeitsmarkt- und Berufsforschung der Bundesagentur für Arbeit. S. 329-343

Willems, E. (2015). *Cybergefahr: Wie wir uns gegen Cyber-Crime und Online-Terror wehren können*. Wiesbaden: Springer

Wilson, M. & Hash, J. (2003). Building an Information Technology Security Awareness and Training Program. Veröffentlicht unter: *https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf* (heruntergeladen am 04.07.2018)

Wind, M. & Breiter, A. (2011). *Informationstechnik und ihre Organisationslücken:* Soziale, politische und rechtliche Dimensionen aus der Sicht von Wissenschaft und Praxis. Berlin: Lit

Winkelmann, C. (2011). Ressourcenstärkendes Training für angehende und berufstätige Lehrkräfte an berufsbildenden Schulen: *Prävention und Gesundheitsförderung*, 6(1). 48-57

Winter, H. (2001). Mensch und Maß?: ein kurzes Kapitel leiblicher Mathematik. *Die Grundschule*, 15(141). 46-49

Winter, K. (2013). *Soziale und sozialpsychische Determinanten des Gesundheitsverhaltens:* Eine theoriegeleitete Analyse am Beispiel von Überernährung und Tabakkonsum. Berlin: Freie Universität

Wirsing, L. (2017). Vorsicht vor Konferenz-WLAN. Welche Gefahren von Fake-Hotspots ausgehen. Veröffentlicht unter: *https://blog.converia.de/de/kostenfreies-konferenz-wlan-fake-hotspots/* (heruntergeladen am 08.06.2020)

Witte, K. & Allen, M. (2000). A Meta-Analysis of Fear Appeals: Implications for Effective Public Health Campaigns. *Health Education and Behavior*, 27. 606

Witteck, C. (2011). *Bestimmungsgründe dysfunktionalen Verhaltens in Organisationen:* Eine Analyse der Forschungsschwerpunkte im Zeitablauf. München: Rainer Hampp

Witzke, S. (2016). *Carsharing und die Gesellschaft von Morgen:* Ein umweltbewusster Umgang mit Automobilität? Berlin: Springer

Wolter, A. (2009). Die Öffnung der Hochschule für Berufstätige – Nationale und internationale Perspektiven. In: *Hanft, A. & Knust, M. (2009) Weiterbildung und lebenslanges Lernen in Hochschulen: Eine internationale Vergleichsstudie zu Strukturen, Organisation und Angebotsformen, Münster: Waxmann, S*. 10-11

Wright, J. & Cache, J. (2015). *Hacking Exposed Wireless: Wireless Security Secrets & Solution* (4. Aufl.). New York: McGraw-Hill Education

Yar, M. (2006). *Cybercrime and Society*. New Delhi: Sage

Young, S. & Aitel, D. (2004). *The Hacker's Handbook:* The Strategy behind Breaking into and Defending Networks. Boca Raton: CRC Press LLC

Yu, S. (2014). *Distributed Denial of Service Attack and Defense*. Heidelberg: Springer

Zajonc, R. & Moreland, R. L. (1982). Exposure effects in person perception: Familiarity, similarity, and attraction. *Journal of Experimental Social Psychology*, 18. 395-415

Zeuner, C. (2011). Didaktik und Methodik in der Erwachsenenbildung: Grundlagen der Vermittlung oder theoretische Spielerei? In: Holzer, D. & Kloyber, C. (Hrsg.). *The dark side of LLL* (Vol. 3: Kritik als Methode).

Zimbardo, P. G. & Gerrig, R. J. (2008). *Psychologie* (18. Aufl.). München: Pearson Studium

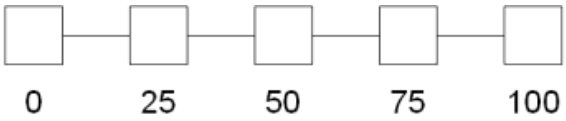
Zöfel, P. (2000). *Statistik verstehen:* Ein Begleitbuch zur computerunterstützten Anwendung. München: Addison-Wesley

Anhang

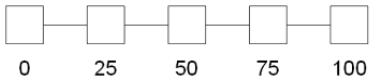
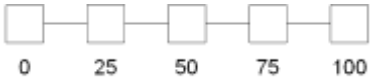
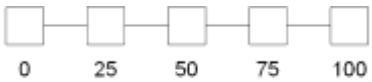
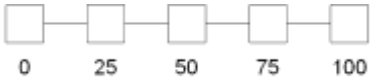
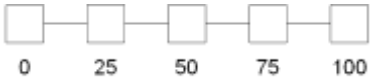
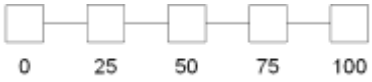
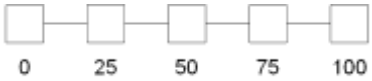
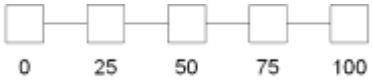
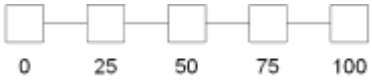
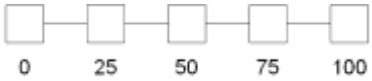
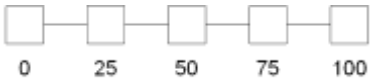
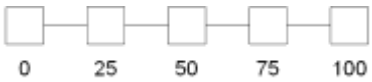
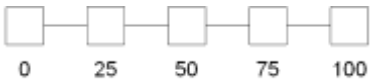
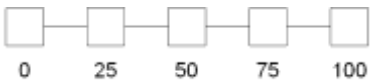
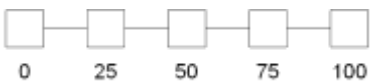
Anhang 1: Fragebogen ‚geplantes Verhalten im Kontext IT-Sicherheit'

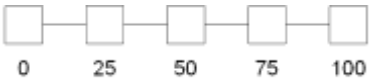
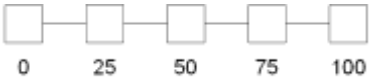
Im Folgenden finden Sie eine Reihe von Aussagen zum Umgang mit Tricks und Betrügereien im Internet sowie zur Datensicherheit, denen Sie mehr oder weniger zustimmen können. Es geht dabei um Ihre persönliche Meinung zu dem Thema. Um Ihre Zustimmung/Ablehnung auszudrücken, steht Ihnen eine Skala von 0 bis 100 zur Verfügung. Dabei bedeutet 0 = *trifft nicht zu* und 100 = *trifft voll zu*. Die Zahlen dazwischen dienen der Abstufung Ihrer Zustimmung/Ablehnung.

trifft nicht zu trifft voll zu



Ich finde es wichtig, darüber Bescheid zu wissen, wie man im Internet betrogen werden kann.	0 25 50 75 100
Nur wenn ich mich regelmäßig informiere, kann ich verhindern, Betrügern im Netz zum Opfer zu fallen.	0 25 50 75 100
Mir ist es wichtig, über Betrugs- und Manipulationsmöglichkeiten im Netz auf dem Laufenden zu bleiben.	0 25 50 75 100
Ich versuche, mich regelmäßig über Möglichkeiten der Datensicherheit auf den neuesten Stand zu bringen.	0 25 50 75 100
Um mich wirksam gegen Betrug im Netz zu schützen, muss ich wissen, wie ich sicher mit meinen Daten umgehe.	0 25 50 75 100
Datensicherheit ist keine einmalige Angelegenheit, sondern ein laufender Prozess, und muss immer wieder aktualisiert werden.	0 25 50 75 100
Ich versuche meine Kenntnisse zu erweitern, wie ich mich vor Betrug mit dem Internet schützen kann.	0 25 50 75 100
Von Zeit zu Zeit erkundige ich mich über neue Formen des Internetbetrugs, um nicht selbst Opfer zu werden.	0 25 50 75 100
In der Regel sagt einem der gesunde Menschenverstand, wie man sich vor Betrug im Netz schützen kann.	0 25 50 75 100

Es ist nicht schwer, über den Stand von Betrugs- und Manipulationsmöglichkeiten im Netz auf dem Laufenden zu bleiben.	
Ich kann mich gut gegen Betrug im Netz schützen.	
Mir fällt es leicht, mich regelmäßig über die Entwicklungen bei der Internetkriminalität zu informieren.	
Im Alltag ist es mir zu aufwendig, auf dem neusten Stand zu bleiben, was Betrugsmöglichkeiten im Netz angeht.	
Ich weiß, wie ich mich informieren muss, um vor Betrügereien im Netz sicher zu sein.	
Im Umgang mit meinen Daten bin ich leichtsinnig.	
Ich traue mir zu, mich effektiv vor Betrug im Netz zu schützen.	
Ich weiß, wie ich mich verhalten muss, um vor Tricksereien im Netz sicher zu sein.	
Mir ist es zu umständlich, sicher mit meinen Daten umzugehen, auch wenn ich eigentlich wüsste, wie.	
Mich regelmäßig darüber zu informieren, wie ich mich gegen Betrug im Netz schützen kann, fällt mir leicht.	
Ich weiß, was ich tun muss, um meine Daten vor Missbrauch zu schützen.	
Die Sicherheit meiner Daten ist mir sehr wichtig.	
Ich versuche, bezüglich der Möglichkeiten, meine Daten zu schützen, auf dem Laufenden zu bleiben.	
In der Hektik des Alltags kommt die Datensicherheit bei mir zu kurz.	
Um mich wirksam gegen Betrug im Netz zu schützen, muss ich mich mit Maßnahmen der Datensicherheit auskennen.	

Ich bin hinreichend informiert, um Internetbetrügern nicht auf den Leim zu gehen.	
Ich weiß genug, um nicht auf Tricks von Internetbetrügern hereinzufallen.	

(Hiemisch 2017)

Anhang 2: Fragebogen ‚Weiterbildungsmotivation'

Item	Bilanzwert	Erfolgserwartung
Ich bin den Anforderungen der Fortbildung voll und ganz gewachsen.		x
Die Fortbildung hat bei mir eine sehr hohe Priorität.	x	
Die Fortbildung bringt mir nichts.	x	
Ich werde die Fortbildung sehr wahrscheinlich erfolgreich besuchen.	x	
Mit den Anforderungen in der Fortbildung werde ich besser zurechtkommen als andere.		x
Meine Fähigkeiten für die Fortbildungsinhalte sind niedrig.		x
Ich habe bessere Dinge zu tun, als diese Fortbildung zu besuchen.	x	
Alles in allem lohnt es sich, die Fortbildung zu besuchen.	x	
Ich werde meine Kenntnisse und Kompetenzen durch die Fortbildung wesentlich weiterentwickeln.		x
Unterm Strich ist die Fortbildung den Aufwand nicht wert.	x	
Für die Fortbildung lohnt es sich bestimmt, den erforderlichen Aufwand zu investieren.	x	
Ich denke, dass sich der Aufwand für die Fortbildung am Ende nicht lohnt.		x
Ich halte meine Begabung für die Fortbildungsinhalte für hoch.		x
Ich denke nicht, dass mir der Besuch der Fortbildung etwas bringen wird.	x	

(Gorges 2018)

Anhang 3: Fragen zu den Beweggründen der Teilnahme (BWG)

Item	Frage
dabei1	Ich bereits einen Sicherheitsvorfall hatte.
dabei2	Mich das Thema interessiert.
dabei3	Die Kenntnisse die ich erwerbe mir im Alltag helfen.
dabei4	Weil es mir Spaß macht, sich für neue Dinge zu interessieren.
dabei5	Es mir beruflich nützt.
dabei6	Da ich mich kreativ betätigen möchte.
dabei7	Da ich Menschen kennenlerne.

Anhang 4: Fragen zur Selbstwirksamkeitserwartung (SWE)

Item	Frage
swk1	1. Wenn sich Widerstände auftun, finde ich Mittel und Wege, mich durchzusetzen.
swk2	2. Die Lösung schwieriger Probleme gelingt mir immer, wenn ich mich darum bemühe.
swk3	3. Es bereitet mir keine Schwierigkeiten, meine Absichten und Ziele zu verwirklichen.
swk4	4. In unerwarteten Situationen weiß ich immer, wie ich mich verhalten soll.
swk5	5. Auch bei überraschenden Ereignissen glaube ich, dass ich gut mit ihnen zurechtkommen kann.
swk6	6. Schwierigkeiten sehe ich gelassen entgegen, weil ich meinen Fähigkeiten immer vertrauen kann.
swk7	7. Was auch immer passiert, ich werde schon klarkommen.
swk8	8. Für jedes Problem kann ich eine Lösung finden.
swk9	9. Wenn eine neue Sache auf mich zukommt, weiß ich, wie ich damit umgehen kann.
swk10	10. Wenn ein Problem auftaucht, kann ich es aus eigener Kraft meistern.

(Schwarzer & Jerusalem 1999)

Anhang 5: Fragen zur Evaluation

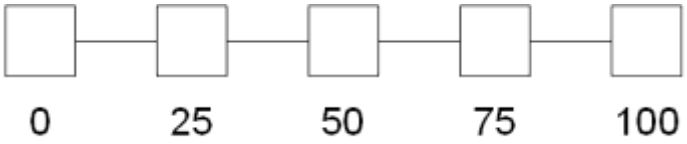
Veranstaltungsorganisation	
1	Die Veranstaltungsräume waren funktionsgerecht.
2	Die Anzahl der Teilnehmenden gestattete ein effektives Arbeiten.
3	Die Zeitstruktur hat den Lernprozess unterstützt.
Medien	
1	Die Medien und Materialien haben den Lernprozess unterstützt.
2	Die Medien und Materialien waren strukturiert.
3	Die Medien und Materialien regten zur konkreten Umsetzung der Inhalte im schulischen Alltag an.
Referentinnen und Referenten	
1	Die Referentinnen und Referenten bezogen theoretische Ansätze auf die Praxis der Teilnehmenden.
2	Die Referentinnen und Referenten waren professionell (z.B. im Umgang mit Störungen).
3	Die Referentinnen und Referenten gingen auf die Wünsche der Teilnehmenden ein.
4	Die Referentinnen und Referenten erlebte ich als kompetent.
5	Die Referentinnen und Referenten vermittelten den Inhalt verständlich.
Allgemein	
1	Die gesamte Qualifizierung entspricht meinem Bedarf.
2	Ich sehe die didaktisch-methodische Umsetzung dieser Veranstaltung als gelungen an.
3	Die Veranstaltung entsprach meinen Erwartungen.
4	Es herrschte eine gute Arbeitsatmosphäre.
5	Ich profitiere persönlich von der Veranstaltung.
6	Ich schätze meinen eigenen Lernerfolg als hoch ein.

Anhang 6: Fragebogen zu t1

Veranstaltung Der zweite Blick“

Im Folgenden finden Sie eine Reihe von Aussagen zum Umgang mit Tricks und Betrügereien im Internet sowie zur Datensicherheit, denen Sie mehr oder weniger zustimmen können. Es geht dabei um Ihre persönliche Meinung zu dem Thema. Um Ihre Zustimmung/Ablehnung auszudrücken, steht Ihnen eine Skala von 0 bis 100 zur Verfügung. Dabei bedeutet 0 = *trifft nicht zu* und 100 = *trifft voll zu*. Die Zahlen dazwischen dienen der Abstufung Ihrer Zustimmung/Ablehnung.

trifft nicht zu trifft nicht zu



Zweiter Buchstabe des Vornamens der Mutter, Vater, Oma und Opa

Pseudonym: ☐☐☐☐

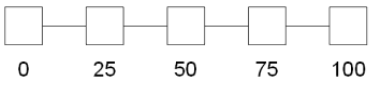
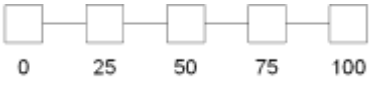
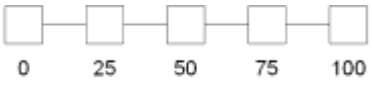
Alter:	

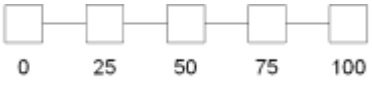
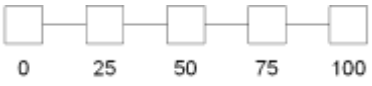
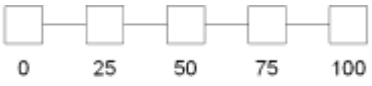
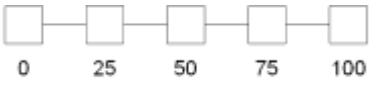
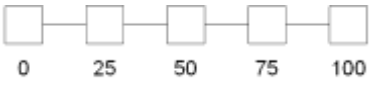
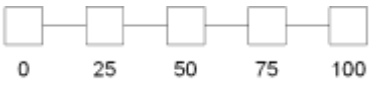
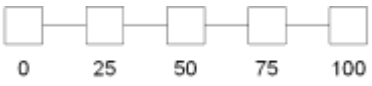
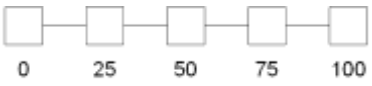
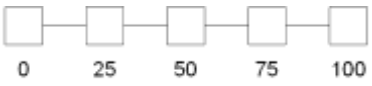
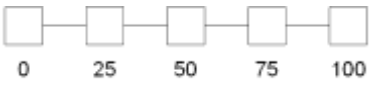
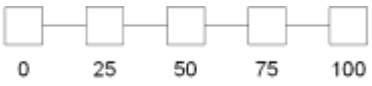
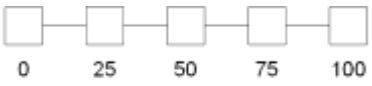
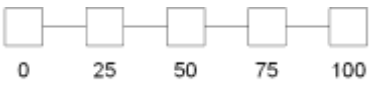
	männlich	weiblich
Geschlecht:	☐	☐

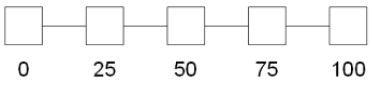
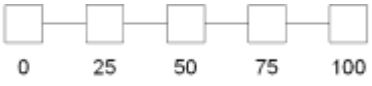
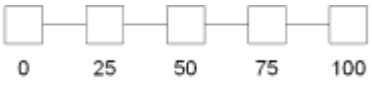
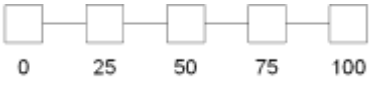
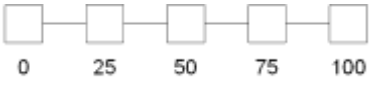
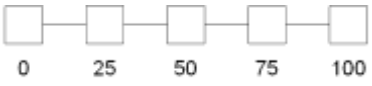
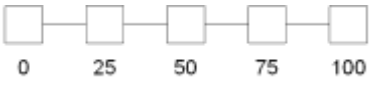
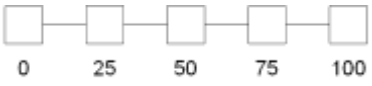
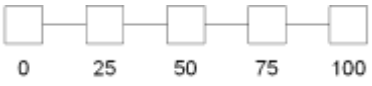
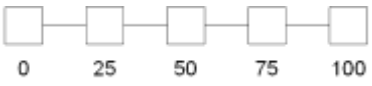
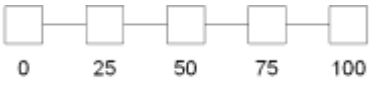
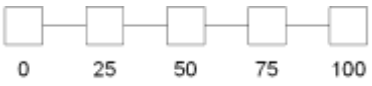
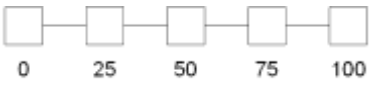
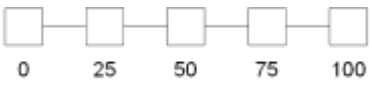
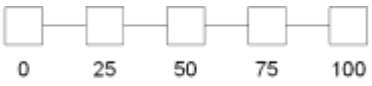
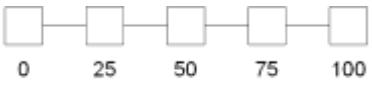
	Berufsausbildung	Fachhochschule	Hochschule	*Andere*
Qualifikation:				

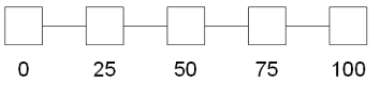
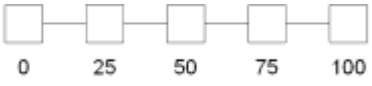
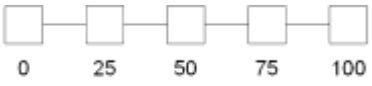
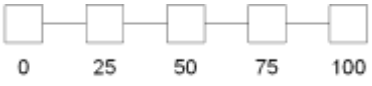
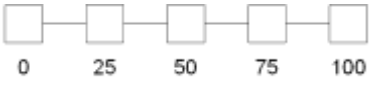
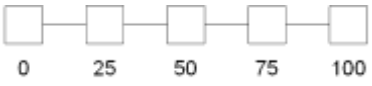
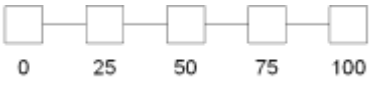
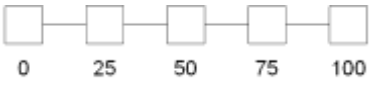
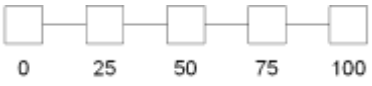
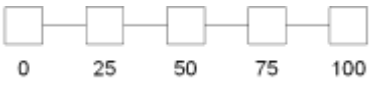
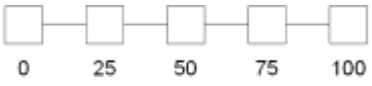
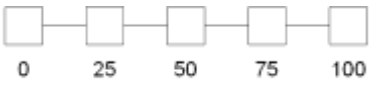
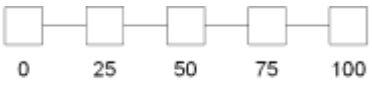
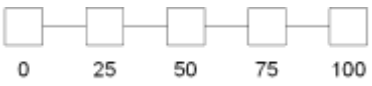
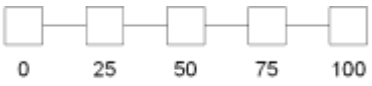
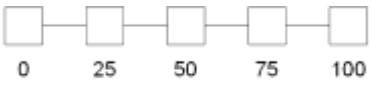
Ich bin heute dabei, weil…

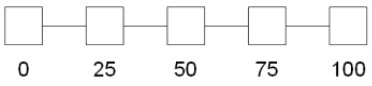
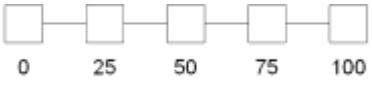
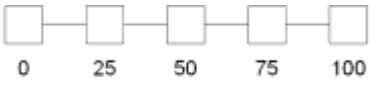
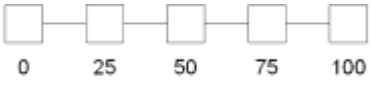
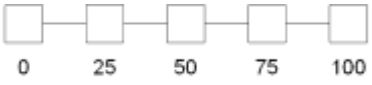
…ich bereits einen Sicherheitsvorfall hatte.	0 25 50 75 100
…mich das Thema interessiert.	0 25 50 75 100
…die Kenntnisse, die ich erwerbe, mir im Alltag helfen.	0 25 50 75 100
… es mir Spaß macht, mich für neue Dinge zu interessieren.	0 25 50 75 100

…es mir beruflich nützt.	
…ich mich kreativ betätigen möchte.	
…ich Menschen kennenlerne.	

Ich finde es wichtig, darüber Bescheid zu wissen, wie man im Internet betrogen werden kann.	
Nur wenn ich mich regelmäßig informiere, kann ich verhindern, Betrügern im Netz zum Opfer zu fallen.	
Mir ist es wichtig, über Betrugs- und Manipulationsmöglichkeiten im Netz auf dem Laufenden zu bleiben.	
Ich versuche, mich regelmäßig über Möglichkeiten der Datensicherheit auf den neusten Stand zu bringen.	
Um mich wirksam gegen Betrug im Netz zu schützen, muss ich wissen, wie ich sicher mit meinen Daten umgehe.	
Datensicherheit ist keine einmalige Angelegenheit, sondern ein laufender Prozess, und muss immer wieder aktualisiert werden.	
Ich versuche, meine Kenntnisse zu erweitern, wie ich mich vor Betrug mit dem Internet schützen kann.	
Von Zeit zu Zeit erkundige ich mich über neue Formen des Internetbetrugs, um nicht selbst Opfer zu werden.	
In der Regel sagt einem der gesunde Menschenverstand, wie man sich vor Betrug im Netz schützen kann.	
Es ist nicht schwer, über den Stand von Betrugs- und Manipulationsmöglichkeiten im Netz auf dem Laufenden zu bleiben.	
Ich kann mich gut gegen Betrug im Netz schützen.	
Mir fällt es leicht, mich regelmäßig über die Entwicklungen bei der Internetkriminalität zu informieren.	
Im Alltag ist es mir zu aufwendig, auf dem neusten Stand zu bleiben, was Betrugsmöglichkeiten im Netz angeht.	

Ich weiß, wie ich mich informieren muss, um vor Betrügereien im Netz sicher zu sein.	
Im Umgang mit meinen Daten bin ich leichtsinnig.	
Ich traue mir zu, mich effektiv vor Betrug im Netz zu schützen.	
Ich weiß, wie ich mich verhalten muss, um vor Tricksereien im Netz sicher zu sein.	
Mir ist es zu umständlich, sicher mit meinen Daten umzugehen, auch wenn ich eigentlich wüsste, wie.	
Mich regelmäßig darüber zu informieren, wie ich mich gegen Betrug im Netz schützen kann, fällt mir leicht.	
Ich weiß, was ich tun muss, um meine Daten vor Missbrauch zu schützen.	
Die Sicherheit meiner Daten ist mir sehr wichtig.	
Ich versuche, bezüglich der Möglichkeiten, meine Daten zu schützen, auf dem Laufenden zu bleiben.	
In der Hektik des Alltags kommt die Datensicherheit bei mir zu kurz.	
Um mich wirksam gegen Betrug im Netz zu schützen, muss ich mich mit Maßnahmen der Datensicherheit auskennen.	
Ich bin hinreichend informiert, um Internetbetrügern nicht auf den Leim zu gehen.	
Ich weiß genug, um nicht auf Tricks von Internetbetrügern hereinzufallen.	
Wenn sich Widerstände auftun, finde ich Mittel und Wege, mich durchzusetzen.	
Die Lösung schwieriger Probleme gelingt mir immer, wenn ich mich darum bemühe.	
Es bereitet mir keine Schwierigkeiten, meine Absichten und Ziele zu verwirklichen.	

In unerwarteten Situationen weiß ich immer, wie ich mich verhalten soll.	
Auch bei überraschenden Ereignissen glaube ich, dass ich gut mit ihnen zurechtkommen kann.	
Schwierigkeiten sehe ich gelassen entgegen, weil ich meinen Fähigkeiten immer vertrauen kann.	
Was auch immer passiert, ich werde schon klarkommen.	
Für jedes Problem kann ich eine Lösung finden.	
Wenn eine neue Sache auf mich zukommt, weiß ich, wie ich damit umgehen kann.	
Wenn ein Problem auftaucht, kann ich es aus eigener Kraft meistern.	
Ich bin den Anforderungen der Fortbildung voll und ganz gewachsen.	
Die Fortbildung hat bei mir eine sehr hohe Priorität.	
Die Fortbildung bringt mir nichts.	
Ich werde die Fortbildung sehr wahrscheinlich erfolgreich besuchen.	
Mit den Anforderungen in der Fortbildung werde ich besser zurechtkommen als andere.	
Meine Fähigkeiten für die Fortbildungsinhalte sind niedrig.	
Ich habe bessere Dinge zu tun, als diese Fortbildung zu besuchen.	
Alles in allem lohnt es sich, die Fortbildung zu besuchen.	
Ich werde meine Kenntnisse und Kompetenzen durch die Fortbildung wesentlich weiterentwickeln.	

Unterm Strich ist die Fortbildung den Aufwand nicht wert.	
Für die Fortbildung lohnt es sich bestimmt, den Aufwand zu investieren.	
Ich denke, dass sich der Aufwand für die Fortbildung am Ende nicht lohnt.	
Ich halte meine Begabung für die Fortbildungsinhalte für hoch.	
Ich denke nicht, dass mir der Besuch der Fortbildung etwas bringen wird.	

Anhang 7: Fragebogen zu t2

Veranstaltung „Der zweite Blick“

Im Folgenden finden Sie eine Reihe von Aussagen zum Umgang mit Tricks und Betrügereien im Internet sowie zur Datensicherheit, denen Sie mehr oder weniger zustimmen können. Es geht dabei um Ihre persönliche Meinung zu dem Thema. Um Ihre Zustimmung/Ablehnung auszudrücken, steht Ihnen eine Skala von 0 bis 100 zur Verfügung. Dabei bedeutet 0 = *trifft nicht zu* und 100 = *trifft voll zu*. Die Zahlen dazwischen dienen der Abstufung Ihrer Zustimmung/Ablehnung.

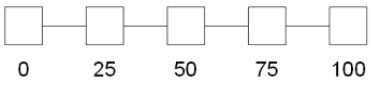
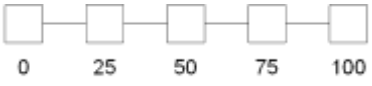
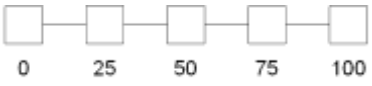
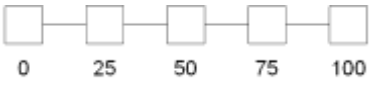
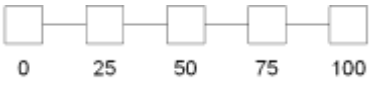
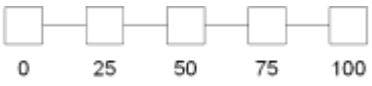
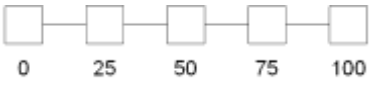
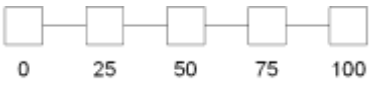
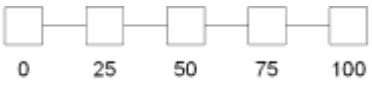
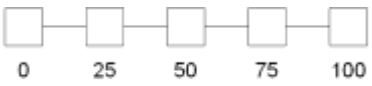
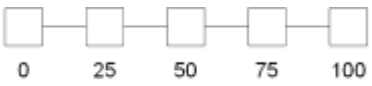
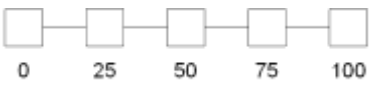
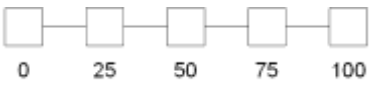
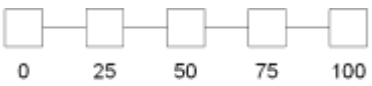
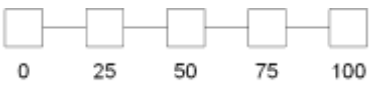
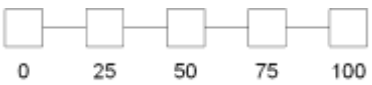
trifft nicht zu — trifft voll zu

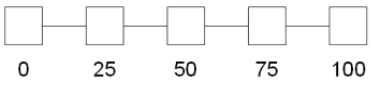
0 25 50 75 100

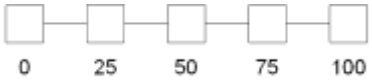
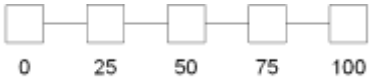
Zweiter Buchstabe des Vornamens der Mutter, Vater, Oma und Opa

Pseudonym: ☐☐☐☐

Ich finde es wichtig, darüber Bescheid zu wissen, wie man im Internet betrogen werden kann.	0 25 50 75 100
Nur wenn ich mich regelmäßig informiere, kann ich verhindern, Betrügern im Netz zum Opfer zu fallen.	0 25 50 75 100
Mir ist es wichtig, über Betrugs- und Manipulationsmöglichkeiten im Netz auf dem Laufenden zu bleiben.	0 25 50 75 100
Ich versuche, mich regelmäßig über Möglichkeiten der Datensicherheit auf den neusten Stand zu bringen.	0 25 50 75 100
Um mich wirksam gegen Betrug im Netz zu schützen, muss ich wissen, wie ich sicher mit meinen Daten umgehe.	0 25 50 75 100
Datensicherheit ist keine einmalige Angelegenheit, sondern ein laufender Prozess, und muss immer wieder aktualisiert werden.	0 25 50 75 100
Ich versuche, meine Kenntnisse zu erweitern, wie ich mich vor Betrug mit dem Internet schützen kann.	0 25 50 75 100
Von Zeit zu Zeit erkundige ich mich über neue Formen des Internetbetrugs, um nicht selbst Opfer zu werden.	0 25 50 75 100
In der Regel sagt einem der gesunde Menschenverstand, wie man sich vor Betrug im Netz schützen kann.	0 25 50 75 100

Es ist nicht schwer, über den Stand von Betrugs- und Manipulationsmöglichkeiten im Netz auf dem Laufenden zu bleiben.	
Ich kann mich gut gegen Betrug im Netz schützen.	
Mir fällt es leicht, mich regelmäßig über die Entwicklungen bei der Internetkriminalität zu informieren.	
Im Alltag ist es mir zu aufwendig, auf dem neusten Stand zu bleiben, was Betrugsmöglichkeiten im Netz angeht.	
Ich weiß, wie ich mich informieren muss, um vor Betrügereien im Netz sicher zu sein.	
Im Umgang mit meinen Daten bin ich leichtsinnig.	
Ich traue mir zu, mich effektiv vor Betrug im Netz zu schützen.	
Ich weiß, wie ich mich verhalten muss, um vor Tricksereien im Netz sicher zu sein.	
Mir ist es zu umständlich, sicher mit meinen Daten umzugehen, auch wenn ich eigentlich wüsste, wie.	
Mich regelmäßig darüber zu informieren, wie ich mich gegen Betrug im Netz schützen kann, fällt mir leicht.	
Ich weiß, was ich tun muss, um meine Daten vor Missbrauch zu schützen.	
Die Sicherheit meiner Daten ist mir sehr wichtig.	
Ich versuche, bezüglich der Möglichkeiten, meine Daten zu schützen, auf dem Laufenden zu bleiben.	
In der Hektik des Alltags kommt die Datensicherheit bei mir zu kurz.	
Um mich wirksam gegen Betrug im Netz zu schützen, muss ich mich mit Maßnahmen der Datensicherheit auskennen.	
Ich bin hinreichend informiert, um Internetbetrügern nicht auf den Leim zu gehen.	

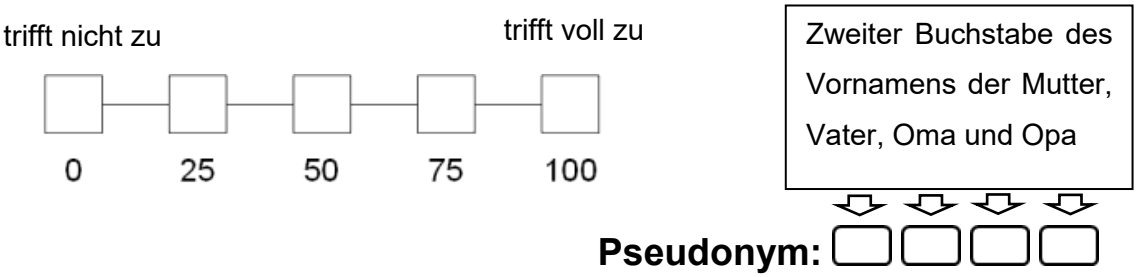
Ich weiß genug, um nicht auf Tricks von Internetbetrügern hereinzufallen.	
Die Veranstaltungsräume waren funktionsgerecht.	
Die Anzahl der Teilnehmenden gestattete ein effektives Arbeiten.	
Die Zeitstruktur hat den Lernprozess unterstützt.	
Die Medien und Materialien haben den Lernprozess unterstützt.	
Die Medien und Materialien waren strukturiert.	
Die Medien und Materialien regten zur konkreten Umsetzung der Inhalte im beruflichen Alltag an.	
Die Referentinnen und Referenten bezogen theoretische Ansätze auf die Praxis der Teilnehmenden.	
Die Referentinnen und Referenten waren professionell (z.B. im Umgang mit Störungen).	
Die Referentinnen und Referenten gingen auf die Wünsche der Teilnehmenden ein.	
Die Referentinnen und Referenten erlebte ich als kompetent.	
Die Referentinnen und Referenten vermittelten den Inhalt verständlich.	
Die gesamte Qualifizierung entspricht meinem Bedarf.	
Ich sehe die didaktisch-methodische Umsetzung dieser Veranstaltung als gelungen an.	
Die Veranstaltung entsprach meinen Erwartungen.	
Es herrschte eine gute Arbeitsatmosphäre.	

Ich profitiere persönlich von der Veranstaltung.	
Ich schätze meinen eigenen Lernerfolg als hoch ein.	

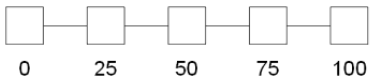
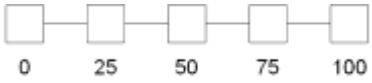
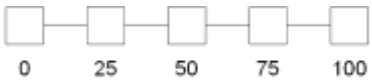
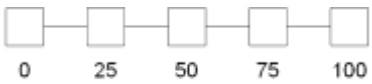
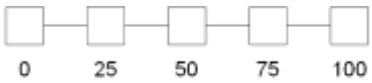
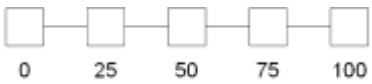
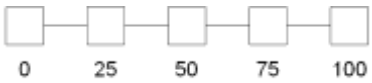
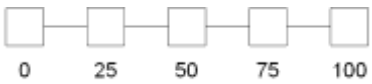
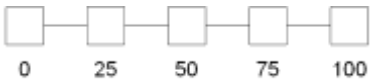
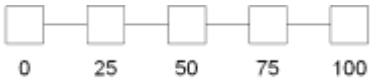
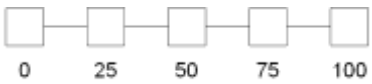
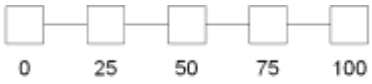
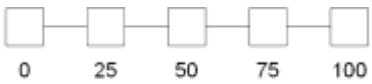
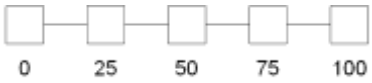
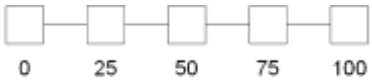
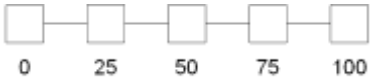
Anhang 8: Fragebogen zu t3

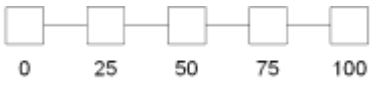
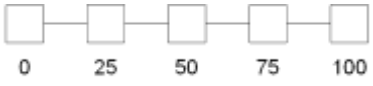
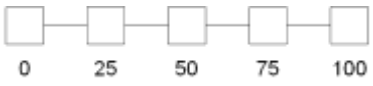
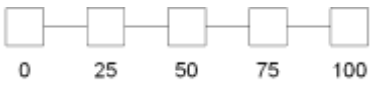
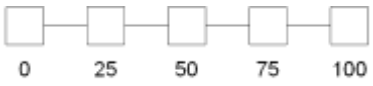
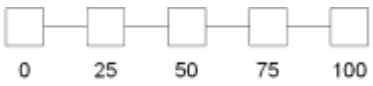
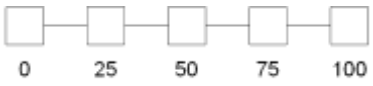
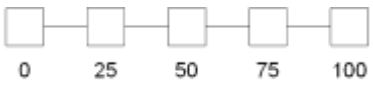
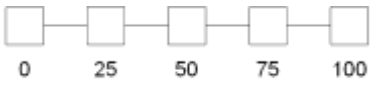
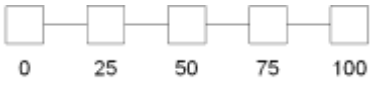
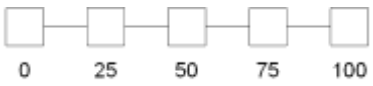
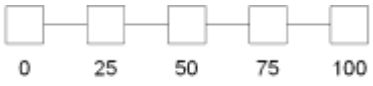
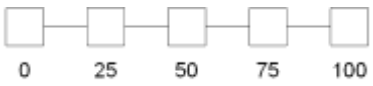
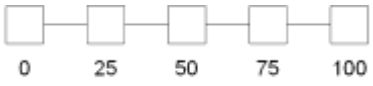
Veranstaltung „Der zweite Blick“

Mit dem Blick auf die Veranstaltung heute: Wie würden Sie heute urteilen, wenn Sie diese Veranstaltung nochmal besuchen würden? Es geht dabei um Ihre persönliche Meinung zu dem Thema. Um Ihre Zustimmung/Ablehnung auszudrücken, steht Ihnen eine Skala von 0 bis 100 zur Verfügung. Dabei bedeutet 0 = *trifft nicht zu* und 100 = *trifft voll zu*. Die Zahlen dazwischen dienen der Abstufung Ihrer Zustimmung/Ablehnung.



Ich finde es wichtig, darüber Bescheid zu wissen, wie man im Internet betrogen werden kann.	0 25 50 75 100
Nur wenn ich mich regelmäßig informiere, kann ich verhindern, Betrügern im Netz zum Opfer zu fallen.	0 25 50 75 100
Mir ist es wichtig, über Betrugs- und Manipulationsmöglichkeiten im Netz auf dem Laufenden zu bleiben.	0 25 50 75 100
Ich versuche, mich regelmäßig über Möglichkeiten der Datensicherheit auf den neusten Stand zu bringen.	0 25 50 75 100
Um mich wirksam gegen Betrug im Netz zu schützen, muss ich wissen, wie ich sicher mit meinen Daten umgehe.	0 25 50 75 100
Datensicherheit ist keine einmalige Angelegenheit, sondern ein laufender Prozess, und muss immer wieder aktualisiert werden.	0 25 50 75 100
Ich versuche, meine Kenntnisse zu erweitern, wie ich mich vor Betrug mit dem Internet schützen kann.	0 25 50 75 100
Von Zeit zu Zeit erkundige ich mich über neue Formen des Internetbetrugs, um nicht selbst Opfer zu werden.	0 25 50 75 100
In der Regel sagt einem der gesunde Menschenverstand, wie man sich vor Betrug im Netz schützen kann.	0 25 50 75 100
Es ist nicht schwer, über den Stand von Betrugs- und Manipulationsmöglichkeiten im Netz auf dem Laufenden zu bleiben.	0 25 50 75 100

Ich kann mich gut gegen Betrug im Netz schützen.	
Mir fällt es leicht, mich regelmäßig über die Entwicklungen bei der Internetkriminalität zu informieren.	
Im Alltag ist es mir zu aufwendig, auf dem neusten Stand zu bleiben, was Betrugsmöglichkeiten im Netz angeht.	
Ich weiß, wie ich mich informieren muss, um vor Betrügereien im Netz sicher zu sein.	
Im Umgang mit meinen Daten bin ich leichtsinnig.	
Ich traue mir zu, mich effektiv vor Betrug im Netz zu schützen.	
Ich weiß, wie ich mich verhalten muss, um vor Tricksereien im Netz sicher zu sein.	
Mir ist es zu umständlich, sicher mit meinen Daten umzugehen, auch wenn ich eigentlich wüsste, wie.	
Mich regelmäßig darüber zu informieren, wie ich mich gegen Betrug im Netz schützen kann, fällt mir leicht.	
Ich weiß, was ich tun muss, um meine Daten vor Missbrauch zu schützen.	
Die Sicherheit meiner Daten ist mir sehr wichtig.	
Ich versuche, bezüglich der Möglichkeiten, meine Daten zu schützen, auf dem Laufenden zu bleiben.	
In der Hektik des Alltags kommt die Datensicherheit bei mir zu kurz.	
Um mich wirksam gegen Betrug im Netz zu schützen, muss ich mich mit Maßnahmen der Datensicherheit auskennen.	
Ich bin hinreichend informiert, um Internetbetrügern nicht auf den Leim zu gehen.	
Ich weiß genug, um nicht auf Tricks von Internetbetrügern hereinzufallen.	

Ich bin den Anforderungen der Fortbildung voll und ganz gewachsen.	
Die Fortbildung hat bei mir eine sehr hohe Priorität.	
Die Fortbildung bringt mir nichts.	
Ich werde die Fortbildung sehr wahrscheinlich erfolgreich besuchen.	
Mit den Anforderungen in der Fortbildung werde ich besser zurechtkommen als andere.	
Meine Fähigkeiten für die Fortbildungsinhalte sind niedrig.	
Ich habe bessere Dinge zu tun, als diese Fortbildung zu besuchen.	
Alles in allem lohnt es sich, die Fortbildung zu besuchen.	
Ich werde meine Kenntnisse und Kompetenzen durch die Fortbildung wesentlich weiterentwickeln.	
Unterm Strich ist die Fortbildung den Aufwand nicht wert.	
Für die Fortbildung lohnt es sich bestimmt, den Aufwand zu investieren.	
Ich denke, dass sich der Aufwand für die Fortbildung am Ende nicht lohnt.	
Ich halte meine Begabung für die Fortbildungsinhalte für hoch.	
Ich denke nicht, dass mir der Besuch der Fortbildung etwas bringen wird.	

Anhang 9: Bekanntmachung der Maßnahme im Stadtreporter

Kunst:Offen - Flyer für Vorpommern ist da

(TVV) Der diesjährige Kunst:Offen Flyer liegt ab sofort in allen Tourist-Informationen in Vorpommern, auf Usedom, Fischland-Darß-Zingst und Rügen aus. Ebenso kann der Flyer auf www.kunst-offen.net oder telefonisch unter 03834/891189 beim Tourismusverband Vorpommern e.V. bestellt werden. „Mit 281 Künstlern an 160 Standorten wird auch in diesem Jahr zu Kunst:Offen in Vorpommern wieder Einiges geboten. Neben der eigentlichen Werkschau gibt es vielerorts zahlreiche Zusatzangebote und Rahmenprogramme, die die Veranstaltung bereichern. Für Jeden, Groß und Klein, ist etwas dabei." so Sven Köppert, der die Veranstaltung beim Tourismusverband Vorpommern e.V. organisiert und betreut.

Bereits zum 24. Mal öffnen Kunstschaffende in Vorpommern zu **Pfingsten vom 19. bis 21. Mai** ihre Türen. Die **Eröffnungsveranstaltung** findet in diesem Jahr am **18. Mai ab 17:00 Uhr im KULTurSPEICHER** im Seebad Ueckermünde statt. Unterstützt wird Kunst:Offen 2018 in Vorpommern durch die Hauptsponsoren Stadtwerke Greifswald und die Sparkasse Vorpommern sowie die Tourismusverbände Fischland-Darß-Zingst und Insel Rügen. Mehr Informationen unter **www.kunst-offen.net**

Modern & kreativ!

Das Freizeitzentrum stellt sich vor!

Freitag, 20. April, von 10:00 bis 16:00 Uhr

Alle interessierten Kinder, Jugendlichen und Erwachsenen sind herzlich zu einem Tag der offenen Tür in das Freizeitzentrum eingeladen.

Bastelstraße + Schminkstation + Fahrzeuge im Außenbereich + Computer + PS-Konsolen + Eye-Toy-Spiele + Billard + Tischkicker

13:00 und 15:00 Uhr Führungen durch das Haus

Der Eintritt an diesem Tag ist frei!

FZ am Haffring 20
Telefon 039771/27209
www.fz-uem.de

STADTBIBLIOTHEK
UECKERMÜNDE · UECKERSTRASSE 96

Öffnungszeiten:
Dienstag
09:00 - 12:00 und 13:00 - 19:00 Uhr
Mittwoch
09:00 - 12:00 Uhr
Donnerstag
09:00 - 12:00 und 13:00 - 18:00 Uhr

Sie wollen die Ausleihe eines Buches verlängern? Einfach eine E-Mail an **stadtbibliothek@ueckermuende.de**

TELEFON: 039771-28480

KINDERBIBLIOTHEK HAFF-GRUNDSCHULE

Öffnungszeiten:
Montag
09:00 - 12:00 Uhr
13:00 - 16:00 Uhr

www.ueckermuende.de/bibliothek.html

Cybersicherheit: Vortrag in der Jugendherberge

Das digitale Zeitalter hat bereits in allen Lebensbereichen begonnen. Wer hier nicht mitmacht, ist ausgeschlossen von der Kommunikation der Freunde, der Bekannten und auch der Familie.

Gelingt trotz aller Schwierigkeiten der kommunikative Anschluss durch Kauf und Nutzung neuer Medien zeigt sich für Cyber-Security-Experten ein bedenkenswertes Bild. Ohne zu wissen werden Geräte in Betrieb genommen, deren technische Möglichkeiten nicht mal mehr erahnt werden können. Das mangelnde Interesse an Cybersicherheit wird dann im schlimmsten Fall durch unumkehrbare Konsequenzen sichtbar, wenn persönliche Daten in fremde Hände gelangen oder verbotene Inhalte auf persönlichen Medien „abgelegt" werden.

Der studierte Cyber-Security-Experte und Mediendidaktiker Heiko Franke zeigt Ihnen hautnah, wie Hacker IT- und Kommunikationssysteme aufbrechen können. Die Unachtsame Nutzung digitaler Medien auf Grund fehlender Medienkompetenz wird an praktischen Beispielen aus Mecklenburg-Vorpommern gezeigt und es werden mögliche Gegenmaßnahmen dargestellt.

Der einstündige Vortrag ist eine geförderte Maßnahme des Landesrates für Kriminalitätsvorbeugung und deshalb für Sie **kostenfrei**. Die Veranstaltung findet am **Freitag, dem 04. Mai, von 16:00 bis ca. 17:00 Uhr in der Jugendherberge Bellin,** Herbergstraße 1, statt. Im Anschluss an die Veranstaltung können Sie gern beim Grillen mit Herrn Franke ins Gespräch kommen. Auch Dirk Scheer, zuständiger Dezernent beim Landkreis und Vorsitzender des Präventionsrates, sowie Hartmut Braun, Leiter des Polizeireviers Ueckermünde, beantworten gern Ihre Fragen in gemütlicher Atmosphäre.

Da nur eine begrenzte Platzanzahl besteht wird um Voranmeldung gebeten (auch für das Grillen). Information und Anmeldung bitte in der Jugendherberge, Telefon 039771/22411, E-Mail: detlef.rabethge@jugendherberge.de.

CariMobil Beratung auf Rädern

caritas

Wir kommen zu Ihnen, sprechen mit Ihnen und unterstützen Sie bei Fragen

- zu Anträgen, amtlichen Schreiben und Behördenangelegenheiten,
- zu Miete, Wohnen und Wohngeld,
- des Auskommens und des Lebensunterhalts,
- zu Arbeit, Arbeitslosigkeit, ALG I und ALG II (Hartz IV),
- zur Erziehung, Schule und zu den Berufswegen Ihrer Kinder,
- zu Krankheiten, Krankheitsfolgen, Rehabilitation und Pflege,
- zu Einschränkungen und Behinderungen,
- zu Renten, Beiträgen oder zur Sicherung im Alter,
- zu Schulden, Ratenzahlung und Entschuldung.

Das Beratungsmobil ist am **Mittwoch, dem 21.04., von 10:30 bis 11:30 Uhr in Ueckermünde-West, Parkplatz Penny-Markt** und am **Donnerstag, dem , von 09:00 bis 10:00 Uhr auf dem Parkplatz Haffcenter in Ueckermünde-Ost** anzutreffen. Wir stellen Kontakte her und beraten Sie kostenlos und unbürokratisch.

CariMobil Pasewalk, Caritasverband für das Erzbistum Berlin e.V., Bahnhofstraße 29, 17309 Pasewalk, Mobil: 0172/5356776, E-Mail: carimobil.pasewalk@caritas-vorpommern.de

VITALSTADT Ueckermünde

Besuchen Sie die Netzwerkpartner unter www.vitalstadt-ueckermuende.de!

Anhang 10: Reportage über die präventive Maßnahme

Nordkurier - Haff-Zeitung vom
08.05.2018

So schützen Sie sich vor Cyberkriminalität

Wie einfach es für Einbrecher ist, eine WLAN-Kamera außer Gefecht zu setzen, oder wie Kaufhäuser das Konsumverhalten ihrer Kunden ausspionieren, erläuterte Sicherheitsexperte Heiko Franke in einem Vortrag.

Bellin. Kennen Sie das auch? Sie besuchen ab und an dasselbe Einkaufszentrum und wundern sich, dass Ihr Handy irgendwann weiß, was Sie vielleicht als nächstes kaufen möchten? Ihnen wird vorgeschlagen, noch das eine oder andere Geschäft zu besuchen, so wie beim letzten Besuch. Klingt fast ein bisschen gruselig und dennoch ist diese Spionage nicht illegal.

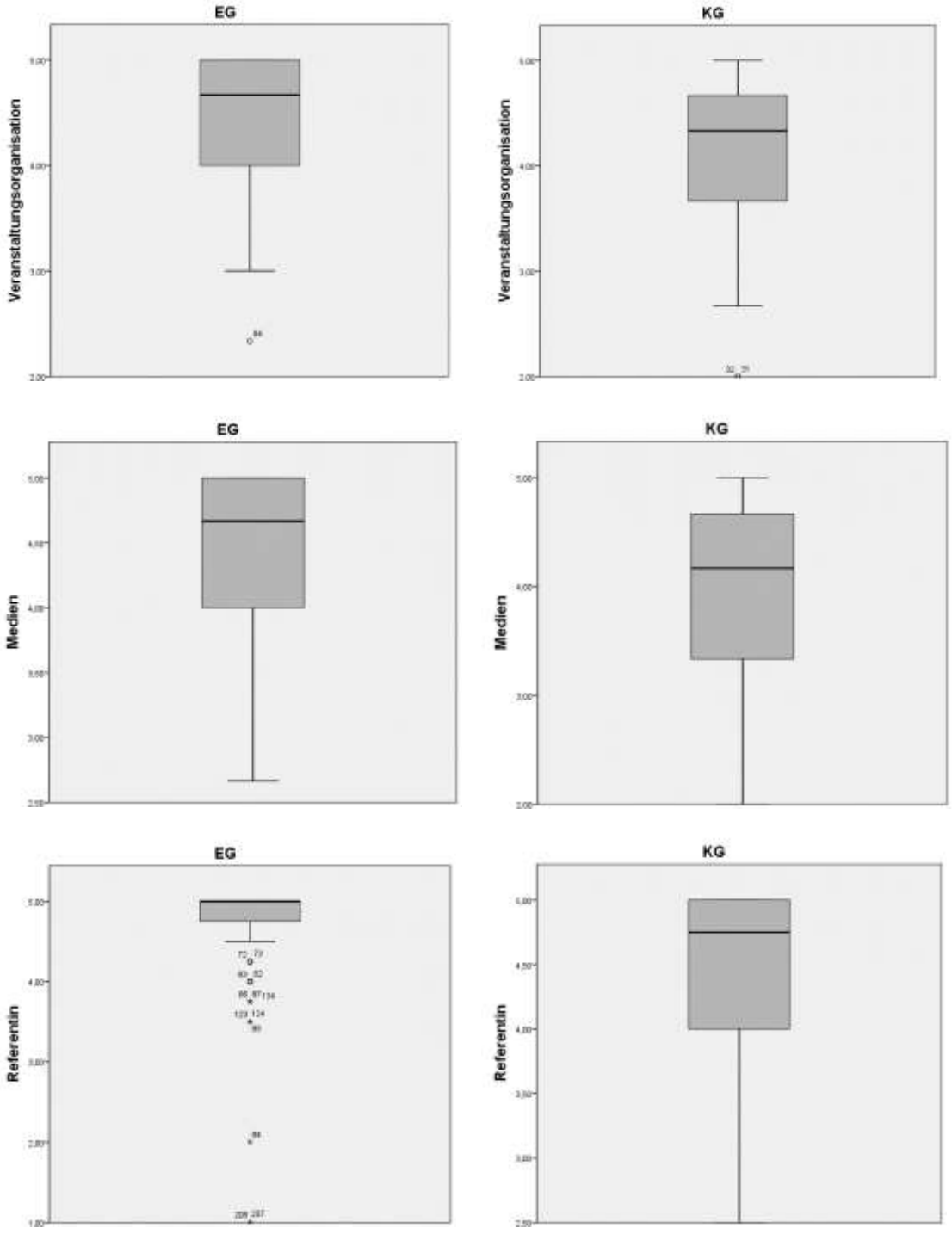
„Um so etwas zu vermeiden, sollte beim Handy unbedingt das WLAN ausgeschaltet sein", erklärt Heiko Franke, Cyber-Security-Experte und IT Sicherheitskoordinator beim Landkreis Vorpommern-Greifswald. „Sonst wählt sich das Handy an jeder Station mit seiner MAC-Adresse (das ist die Geräteadresse, mit der Ihr Gerät in jedem einzelnen Netzwerk identifiziert werden kann) im Einkaufszentrum ein. Damit hinterlässt der Nutzer eine eindeutige Spur und offenbart beispielsweise sein Konsumverhalten. Beim nächsten Besuch erinnert sich das System an die MAC-Adresse und Ihnen werden entsprechende Dinge vorgeschlagen. Auch der Standort sollte immer ausgeschaltet sein", empfiehlt Heiko Franke.

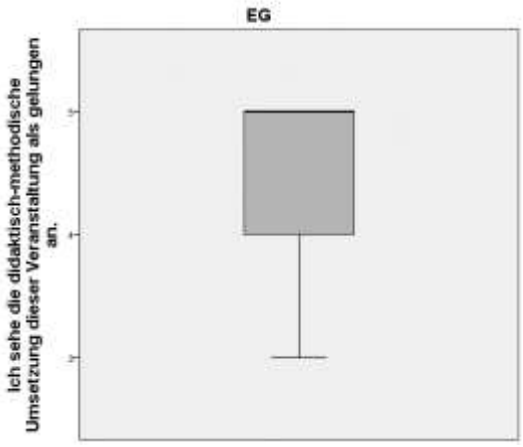
„Wenn wir von Cyberkriminalität nicht unbedingt betroffen sind, denken wir oft nicht darüber nach, was mit unseren Daten passiert und gehen leichtsinnig mit ihnen um", weiß der Experte. Franke hatte für die interessierten Zuhörer etliche Beispiele parat, wie einfach es für Hacker ist, IT- und Kommunikationssysteme aufzubrechen, und gab gleichzeitig Denkan-

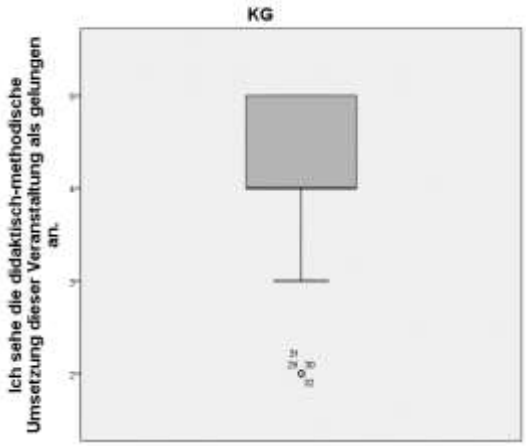
stöße zum Schutz.
Den Vortrag über Cybersicherheit nutzte auch Hartmut Braun, Leiter des Ueckermünder Polizeireviers, um sich zu informieren. „Es ist schon erstaunlich, wie einfach es beispielsweise ist, eine WLAN-Kamera, so wie sie viele jetzt zum Schutz vor Einbrechern nutzen, außer Gefecht zu setzen. Die Täter müssen nicht einmal in der unmittelbaren Nähe sein“, so der Polizist nach dem Vortrag. Wie das funktioniert, hatte der Sicherheitsexperte vor Ort demonstriert. Mit einem alten Rechner und einer speziellen Software konnte die Live-Kamera im Saal mit den Bildern der Gäste eingefroren werden. So hätten Einbrecher freie Bahn und könnten mühelos das Haus leerräumen. Hier können entsprechende Passwörter helfen. Den sichersten Schutz allerdings bieten Kameras mit Netzwerkanschluss, denn alle WLAN-Kameras bergen erhebliche Sicherheitsrisiken.
„Zum eigenen Schutz sollten wir wirklich alle ein zweites Mal hinschauen, was wir machen und uns entsprechend informieren und beraten lassen“, mahnte der Experte. Sein Vortrag „Der zweite Blick“ kann unter der Telefonnummer: 038348 7603335 gebucht werden und ist kostenfrei. Das Projekt wird vom Landesrat für Kriminalitätsvorbeugung gefördert und vom Präventionsrat des Landkreises unterstützt.

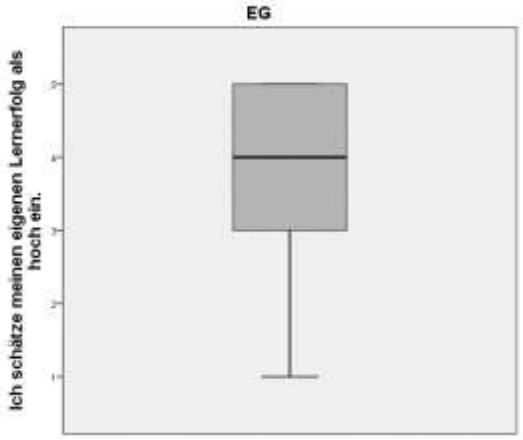
Die interessierten Zuhörer konnten einige Dinge vor Ort gleich auf ihren Handys überprüfen.

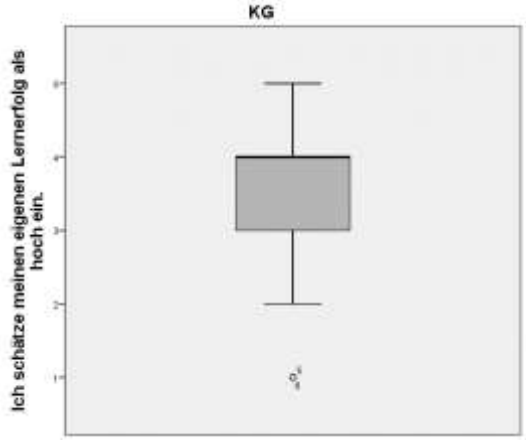
Anhang 11: Evaluation der präventiven Maßnahme KG vs. EG




EG
Ich sehe die didaktisch-methodische Umsetzung dieser Veranstaltung als gelungen an.


KG
Ich sehe die didaktisch-methodische Umsetzung dieser Veranstaltung als gelungen an.


EG
Ich schätze meinen eigenen Lernerfolg als hoch ein.


KG
Ich schätze meinen eigenen Lernerfolg als hoch ein.

Eidesstattliche Erklärung

Hiermit versichere ich, dass ich die vorliegende Arbeit selbstständig und unter Benutzung keiner anderen Quellen als der genannten (gedruckte Werke, Werke in elektronischer Form im Internet, auf CD und anderen Speichermedien) verfasst habe. Alle aus solchen Quellen wörtlich oder sinngemäß übernommenen Passagen habe ich im Einzelnen unter genauer Angabe des Fundortes gekennzeichnet. Ich versichere außerdem, dass ich die beigefügte Dissertation nur in diesem und keinem anderen Promotionsverfahren eingereicht habe und, dass diesem Promotionsverfahren keine endgültig gescheiterten Promotionsverfahren vorausgegangen sind. Gleichfalls sind noch keine Teile der Arbeit veröffentlicht

Ort, Datum: Hornshagen, 02.02.2021 Unterschrift: _____