Dissertationen/Habilitationen

Natalya Pryazhnykova

Informationssicherheits-Awareness fördern

Eine empirische Studie mit Auszubildenden der Automobilindustrie

82 BERUFSBILDUNG, ARBEIT UND INNOVATION

wbv

Informationssicherheits-Awareness fördern

Eine empirische Studie mit Auszubildenden der Automobilindustrie

Natalya Pryazhnykova

Die Reihe **Berufsbildung, Arbeit und Innovation** bietet ein Forum für die grundlagen- und anwendungsorientierte Forschung zu den Entwicklungen der beruflichen Bildungspraxis. Adressiert werden insbesondere berufliche Bildungs- und Arbeitsprozesse, Übergänge zwischen dem Schul- und Beschäftigungssystem sowie die Qualifizierung des beruflichen Bildungspersonals in schulischen, außerschulischen und betrieblichen Handlungsfeldern.

Hiermit leistet die Reihe einen Beitrag für den wissenschaftlichen und bildungspolitischen Diskurs über aktuelle Entwicklungen und Innovationen. Angesprochen wird ein Fachpublikum aus Hochschulen und Forschungseinrichtungen sowie aus schulischen und betrieblichen Politik- und Praxisfeldern.

Die Reihe ist gegliedert in die **Hauptreihe** und in die Unterreihe **Dissertationen/Habilitationen**.

Weitere Informationen finden Sie auf **wbv.de/bai**

Natalya Pryazhnykova

Informationssicherheits-Awareness fördern

Eine empirische Studie mit Auszubildenden der Automobilindustrie

wbv

Die Dissertation zur Erlangung des Dr. phil. wurde unter dem Originaltitel „Informationssicherheits-Awareness fördern. Eine empirische Studie mit Auszubildenden der Automobilindustrie“ an der Fakultät für Humanwissenschaften der Otto-von-Guericke-Universität Magdeburg eingereicht.

Gutachter: Prof. Dr. Klaus Jenewein
Gutachter: Prof. Dr. Ralph Dreher

Berufsbildung, Arbeit und Innovation – Dissertationen/Habilitationen, Band 82

2025 wbv Publikation
ein Geschäftsbereich der
wbv Media GmbH & Co. KG, Bielefeld

Gesamtherstellung:
wbv Media GmbH & Co. KG
Auf dem Esch 4, 33619 Bielefeld,
service@wbv.de
wbv.de

Umschlagmotiv: 1expert, 123rf

Bestellnummer: 74115
ISBN (Print): 978-3-7639-7411-5
ISBN (E-Book): 978-3-7639-7412-2
DOI: 10.3278/9783763974122

Printed in Germany

Diese Publikation ist frei verfügbar zum Download unter wbv-open-access.de

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Die freie Verfügbarkeit der E-Book-Ausgabe dieser Publikation wurde ermöglicht durch ein Netzwerk wissenschaftlicher Bibliotheken und Institutionen zur Förderung von Open Access in den Sozial- und Geisteswissenschaften im Rahmen der *wbv OpenLibrary 2024*.

Die Publikation beachtet unsere Qualitätsstandards für Open-Access-Publikationen, die an folgender Stelle nachzulesen sind:
https://www.wbv.de/fileadmin/importiert/wbv/PDF_Website/Qualitaetsstandards_wbvOpenAccess.pdf

Großer Dank gebührt den Förderern der *wbv OpenLibrary 2024* im Fachbereich *Berufs- und Wirtschaftspädagogik*:

Otto-Friedrich-Universität **Bamberg** | Humboldt-Universität zu **Berlin** | Universitätsbibliothek **Bielefeld** | Bundesinstitut für Berufsbildung (BIBB, **Bonn**) | Rheinische Friedrich-Wilhelms-Universität **Bonn** | Universitäts- und Landesbibliothek **Darmstadt** | Goethe-Universität **Frankfurt am Main** | Pädagogische Hochschule **Freiburg** | Justus-Liebig-Universität **Gießen** | Fernuniversität **Hagen** | TIB **Hannover** | Universitätsbibliothek **Kassel** | **Karlsruhe** Institute of Technology (KIT) | Universitätsbibliothek **Kiel** | Universitäts- und Stadtbibliothek **Köln** | Zentral- und Hochschulbibliothek (ZHB, **Luzern**) | Hochschule der Bundesagentur für Arbeit (**Mannheim**) | Fachhochschule **Münster** | Carl von Ossietzky Universität **Oldenburg** | Landesbibliothek **Oldenburg** | Universitätsbibliothek **Osnabrück** | Universität **Potsdam** | Universitätsbibliothek **St. Gallen**

Inhalt

1 Einleitung

Seit Jahrzehnten ist die Gewährleistung der Informationssicherheit einer der wichtigsten Bestandteile eines jeden erfolgreichen Unternehmens (Hart et al., 2020). Treten jedoch Lücken in den Informationssicherheitssystemen von Unternehmen auf, birgt dies große Gefahrenpotenziale für ebenjene. Sicherheitslücken wie Cyberangriffe in Form von Malware-Infektionen, Hackerangriffen oder Manipulationen von Internetauftritten können zu großen finanziellen Schäden oder auch zu Image- und Datenverlusten für die betroffenen Unternehmen führen (Hart et al., 2020; Deloitte, 2018, S. 4). Die statistischen Ergebnisse einer Cyber-Sicherheits-Umfrage von 2017 (879 teilnehmende Institutionen) des Bundesamts für Sicherheit in der Informationstechnik (weiter als BSI) untermauern diesen Sachverhalt (BSI, 2018). Demnach gaben 70 % der befragten Institutionen an, in den Jahren 2016 und 2017 Opfer von Cyberangriffen geworden zu sein (BSI, 2018). Die Konsequenzen für die Institutionen und Unternehmen waren mitunter erheblich: 16,5 % der geschädigten Institutionen mussten mit Reputationsschäden kämpfen. Außerdem kam es bei 22 % der betroffenen Betriebe zum Diebstahl sensibler Informationen (BSI, 2018).

Doch worin liegen die Ursachen für den Erfolg von Cyberangriffen? Wie kann es immer wieder dazu kommen, dass Unternehmen, Betriebe, Institutionen etc. mit Sicherheitsproblemen bezüglich interner und eigentlich geschützter Daten zu kämpfen haben? Diese Fragen könnten mit den Ergebnissen einer Cyber-Sicherheits-Umfrage von 2015 beantwortet werden (BSI, 2015). Laut dieser Umfrage ließ sich der Erfolg eines effektiven Cyberangriffes in der Hälfte der Fälle auf ein *„unbeabsichtigtes Fehlverhalten von Mitarbeitern“* zurückführen, gefolgt von technischen Ursachen (Abb. 1).

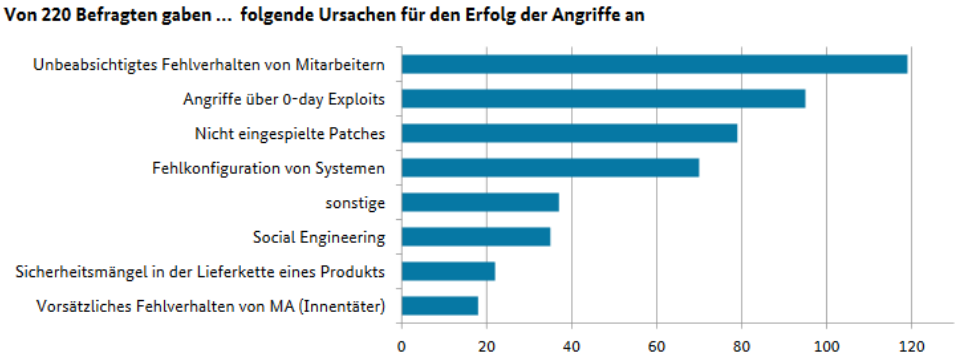


Abbildung 1: Ursachen für den Erfolg von Angriffen (BSI, 2015, S. 16)

Das bedeutet, dass zur Gewährleistung der Informationssicherheit nicht nur die Einrichtung und Sicherstellung der unternehmensinternen Informationstechnik (IT) gehört, sondern auch die effektive Sensibilisierung von Beschäftigten, die als „größter

Risikofaktor“ für Sicherheitslücken und Datenverluste bezeichnet werden (Fox & Kaun, 2005, S. 331). Laut Hart et al. (2020) sind das Training und die Sensibilisierung des Personals einer der wichtigsten Bestandteile der IT-Sicherheit in einem Unternehmen, um den sogenannten „kritischen Bestandteil“ (das Personal) im Rahmen der Gewährleistung von Informationssicherheit befähigen und stärken zu können.

Die gebräuchlichste Methode zur Erhöhung von Informationssicherheits-Awareness in Unternehmen sind Schulungen, in denen Fakten und Maßnahmen zum Umgang mit Informationssicherheitsvorfällen vermittelt werden (Hart et al., 2020). Diese Schulungsart vermittelt zwar gewisse theoretische Kenntnisse, bietet aber keine Möglichkeit zum praktischen Einstieg in das Thema Informationssicherheits-Awareness (Hart et al., 2020 nach Trickel et al., 2017).

Eine Möglichkeit, sich praktisch damit auseinanderzusetzen und die Informationssicherheits-Awareness von Beschäftigen zu erhöhen, bietet ein neuerer Ansatz – der sogenannten Serious Games (Hart et al., 2020). Als Serious Game wird ein Spiel bezeichnet, mit dem spezifische Inhalte vermittelt werden und das spielerische Interaktionselemente, vorwiegend aus Videospielen, beinhaltet (Högsdal, 2011, S. 117 in Anlehnung an Marr, 2010, S. 18). Die vorliegende Arbeit analysiert Serious Games als Awareness-Maßnahme und untersucht, auf welche Weise sie zur Förderung der Mitarbeitersensibilität im Umgang mit IT-Sicherheit und zur Erhöhung ihrer Informationssicherheits-Awareness beitragen können. Serious Games sind sowohl in der Theorie als auch in der Praxis zur Umsetzung von Awareness-Maßnahmen vertreten. Sie bieten dem Spieler[1] nicht nur die Möglichkeit, einen praktischen Einstieg ins Thema Informationssicherheit zu gewinnen, sondern führen zu einem spielerischen, interaktiven Erlebnis, das sich vorteilhaft auf die Informationssicherheits-Awareness auswirkt (Hart et al., 2020).

In der Forschung existieren bereits verschiedene Ansätze, die die Einführung und Benutzung von diversen Serious Games in unterschiedlichen Informationssicherheitskontexten thematisieren (Mostafa & Faragallah, 2019). Diese werden im Rahmen der vorliegenden Arbeit vorgestellt und diskutiert. Außerdem sollen die Eignung von Serious Games und deren Umsetzung im Rahmen von Sicherheits-Awareness-Maßnahmen bei der Volkswagen AG beleuchtet werden.

1.1 Problemstellung und Zielsetzung

Serious Games existieren im Vergleich zu „analogen“ Spielen ebenso wie kommerzielle elektronische Spiele erst seit der zweiten Hälfte des 20. Jahrhunderts (Korn, 2011). Das primäre Ziel der Serious Games ist es, Lerninhalte zu vermitteln, die sich dem Unterhaltungsfaktor zuordnen lassen (Tolks & Lampert, 2016, S. 193 in Anlehnung an Zyda, 2005, S. 17; Michael & Chen, 2006, S. 17; Sawyer, 2004, S. 12). Serious

1 Zur besseren Lesbarkeit wird darauf verzichtet, bei Personenbezeichnungen sowohl die männliche als auch die weibliche Form zu nennen. Die männliche Form gilt in allen Fällen, in denen dies nicht explizit ausgeschlossen wird, für alle (binären und non-binären) Geschlechter.

Games werden schon seit mehreren Jahren in diversen Bereichen im Rahmen der betrieblichen Bildung erfolgreich eingesetzt (vgl. Unger, Goossens & Becker, 2015).

Der Einsatz von Serious Games im Bereich der Informationssicherheits-Awareness ist jedoch ein neues Feld. Dementsprechend sind damit noch viele Herausforderungen und offene Fragen verbunden – nicht nur, was die betriebliche Einführung betrifft, sondern auch bezüglich der wissenschaftlichen Überprüfung, wie effektiv der Einsatz von Serious Games im Informationssicherheits-Awareness-Förderungskontext ist. In der bestehenden Forschung zu den Zusammenhängen zwischen Serious Games und Informationssicherheits-Awareness fällt auf, dass die didaktische Untermauerung der Spiele oftmals nicht durch Studien zur Herleitung der Spielelemente begleitet und vorwiegend basierend auf Elementen anderer bestehender Spiele entwickelt wird. So beschreiben Mostafa und Faragallah (2019), dass zur Vermittlung von Inhalten aus dem Informationssicherheits-Awareness-Bereich meist Serious Games entwickelt werden, die auf einem bestehenden Szenario aus einem gewissen Genre basieren und somit nur begrenzte Möglichkeiten an Spielaktionen bieten.

Die Ergebnisse der Studie von Mostafa und Faragallah (2019) zeigen, dass viele Spielgenres der Serious Games generell geeignet sind, um die Lerninhalte zu vermitteln. Denn sie bieten dem Spieler nicht nur ein hohes Interaktivitätsniveau, sondern stellen auch keine lose ins Spiel integrierten Inhalte dar (Mostafa & Faragallah, 2019). Die Forscher nennen in ihrer Studie verschiedene Faktoren, welche die Effektivität von Serious Games zum Thema Informationssicherheits-Awareness beeinflussen können. Dazu gehören beispielsweise: Spielgeschichte, Spieldynamik, Spielmechanik, etc. (Mostafa & Faragallah, 2019). Trotz dieser bereits vorhandenen Erkenntnisse ist die Forschung zum Einsatz von Serious Games zur Förderung von Informationssicherheits-Awareness noch nicht ausgereift und noch deutlich ausbaufähig. Denn in der bestehenden Literatur bleibt u. a. offen, welche Spielcharakteristika und welche Genres oder welche Mischungen dieser beiden Aspekte für die Vermittlung von Informationssicherheits-Awareness-Inhalten am geeignetsten und effektivsten sind.

Ergänzend dazu heben Hart et al. (2020 in Anlehnung u. a. an Aladawy et al., 2018; Graffer et al., 2015) in ihrer Studie hervor, dass einige Serious Games separat einzelne Themen der Informationssicherheit beleuchten (z. B. nur Umgang mit Social Engineering oder Management von Informationssicherheitsvorfällen) und somit dem Spieler keine Möglichkeit geben, andere Handlungsfelder der Informationssicherheits-Awareness kennenzulernen. Problematisch ist ebenfalls, dass aus der bestehenden Forschung nicht abgeleitet werden kann, welche Handlungsfelder der Informationssicherheits-Awareness konkret behandelt werden und wie diese in einem Serious Game dargestellt werden müssen, damit sie die Informationssicherheits-Awareness der Spieler (ergo der Beschäftigten) optimal steigern. Ferner bestehen keine Ansätze zur Effektivitätsüberprüfung solcher Maßnahmen.

Eine entscheidende Rolle für die Informationssicherheits-Awareness spielen die drei Aspekte Wissen, Einstellung und Verhalten. Inwiefern diese jedoch miteinander korrelieren, auf welche Weise Informationssicherheits-Awareness durch Serious Games am besten gefördert und deren Erfolg gemessen werden kann, geht aus dem

aktuellen Forschungsdiskurs nicht hervor. Obwohl in der Forschung Versuche existieren, allgemeine Informationssicherheits-Awareness zu messen (vgl. Kapitel 2.2), gibt es keine Untersuchung, die geeignete Messmethoden für die Effektivität von Serious Games vorstellt.

Aus den betrachteten Problemfeldern und dem aktuellen Forschungsstand lassen sich für die hier vorliegende Untersuchung daher folgende Forschungsfragen schlussfolgern:

Forschungsfrage 1: Welche Themen der Informationssicherheits-Awareness und welche spielerischen Charakteristiken sind im Rahmen eines Serious Games zu behandeln?

Forschungsfrage 2: Wie kann Informationssicherheits-Awareness gemessen werden?

Forschungsfrage 3: Wie effektiv und nachhaltig für die Förderung von Awareness-Aspekten (Wissen, Einstellung und Verhalten) ist das Konzept „Serious Games" und inwiefern korrelieren die einzelnen Awareness-Aspekte (Wissen, Einstellung und Verhalten) miteinander?

Die Forschungsfragen dieser Arbeit sollen im Rahmen einer Fallstudie in Kooperation mit der Volkswagen AG umgesetzt werden. Um eine praktische Anwendbarkeit der theoretisch entwickelten, didaktischen Elemente des Serious Games zu gewährleisten, soll ein Abgleich mit den didaktischen Konstrukten und bestehenden Awareness-Maßnahmen der Volkswagen AG stattfinden. Diese Awareness-Maßnahmen werden im Anschluss für die Überprüfung der didaktischen Konzepte verwendet.

Im Folgenden soll die Zielgruppe der Beschäftigten der Volkswagen AG genauer definiert werden, die in dieser Arbeit untersucht wird. Die Generation Z (die nach 1995 Geborenen) ist am häufigsten Opfer von Cyberkriminalität, wie Daten einer Studie aus den Niederlanden ergeben (siehe Abb. 2) (CBS, 2019). Jüngere Personen im Alter von 18 bis 40 Jahren werden häufiger Opfer von Cyberkriminalität als ältere Menschen, so eine Studie von US Federal Trade Commission und Atlas VPN (Cyber Security Intelligence, 2018; Engineering & Technology, 2021). Während ältere Menschen in der Regel diejenigen sind, die weniger Erfahrung mit modernen Technologien haben und daher anfälliger für Cyberkriminalität im Internet sind, deuten neue Daten, die auf der Umfrage Atlas VPN basieren, auf etwas anderes hin (Engineering & Technology, 2021). Die Generation Z und die Millennials (die Generation vor Generation Z) melden Cyberkriminalität seltener als andere Generationen und werden öfters Opfer davon (Engineering & Technology, 2021). Von den Befragten der Generation Z waren 49 % bisher überhaupt noch nie Opfer von Cyberkriminalität. 22 % von ihnen haben bis dato hingegen einen einzigen Cyberangriff erlitten und 21 % der Erwachsenen der Generation Z wurden zwei- bis dreimal Opfer schädlicher Cyberaktivitäten, die zu Daten- oder finanziellen Verlusten führten (Engineering & Technology, 2021). Darüber hinaus zeigt sich, dass junge Erwachsene am häufigsten Opfer von Cyber-Security-Vorfällen sind. Ergänzend dazu sind, aus der unternehmerischen Perspektive betrachtet, junge Erwachsene oft die Berufseinsteiger, die im beruflichen Leben erst eine Sensibilisierung zur Cyber-Security-Kultur im jeweiligen Unternehmen erhalten müssen und

sollen. Allerdings existiert zurzeit bei der Volkswagen AG keine gruppenspezifische Sensibilisierungsmaßnahme. In dieser Studie soll der Fokus explizit bei den jungen Erwachsenen (zwischen 18 und 24 Jahren) liegen. Somit ergibt sich die Zielgruppe für diese Arbeit, nämlich junge Erwachsene zwischen 18 und 24 Jahren, die bei der Volkswagen AG tätig sind. Unter diese Zielgruppe fallen bei der Volkswagen AG primär die Auszubildenden in den ersten Ausbildungsjahren.

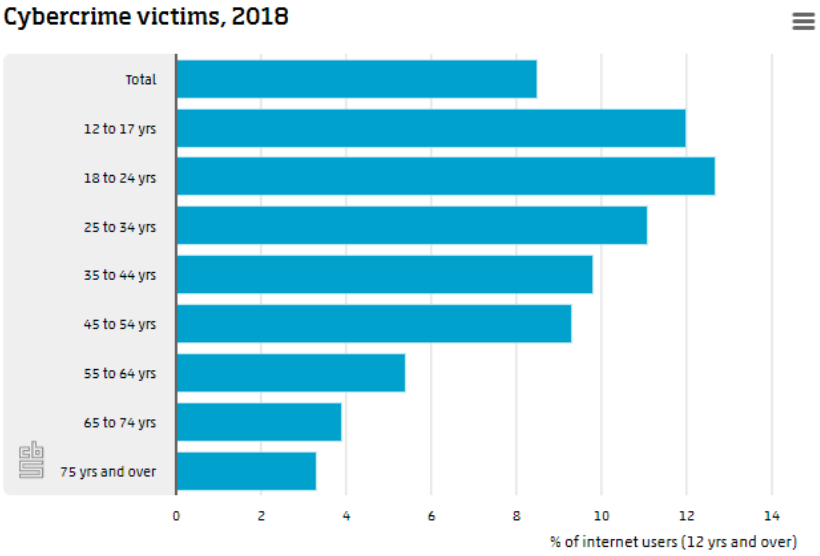


Abbildung 2: Opfer von Cyberkriminalität 2018 (CBS, 2019)

Aus theoretischer Perspektive werden verschiedene Mehrwerte von dieser Arbeit erwartet. Zum einen wird in den theoretischen Grundlagen eine Übersicht über bestehende Literatur gegeben, die einen Ansatz zur Erklärung von Mechanismen der Awareness-Maßnahme bietet. Diese Übersichtsergebnisse werden im Anschluss in den Serious-Games-Kontext eingeordnet. In Form einer qualitativen Studie werden didaktische Elemente eines Serious Games ermittelt und mit bestehender Literatur verglichen. Mithilfe einer quantitativen Studie werden diese Elemente hinsichtlich ihrer Wirksamkeit und basierend auf bestehenden Mechanismen von Awareness-Maßnahmen überprüft. Die wissenschaftlichen Erkenntnisse werden nicht nur zur allgemeinen Informationssicherheits-Awareness-Forschung beitragen, sondern auch wertvolle Informationen liefern, inwiefern sich Informationssicherheits-Awareness messen, fördern und analysieren lässt, welche Aspekte und Themen der Informationssicherheits-Awareness existieren und inwiefern sie miteinander korrelieren.

Aus praktischer Perspektive liefert die Arbeit zudem ein didaktisches Konzept zur Umsetzung eines Serious Games. Des Weiteren werden bestehende Maßnahmen hinsichtlich ihrer didaktischen Struktur untersucht, im Zeitverlauf analysiert sowie auf ihre Wirksamkeit hin überprüft. Die Ergebnisse zeigen zum einen die Wirkungsweise der

didaktisch ermittelten Konstrukte anhand konkreter Informationssicherheitskontexte, zum anderen offenbaren sie Verbesserungspotenziale hinsichtlich didaktischer Elemente in der Awareness-Maßnahme-Ausgestaltung. Die Ergebnisse können von der Volkswagen AG für die Weiterentwicklung bestehender Maßnahmen oder zur Entwicklung einer neuen Awareness-Maßnahme in Form eines Serious Games genutzt werden.

1.2 Vorgehensweise

Zu Beginn der Arbeit wird der Forschungsstand zum Thema Informationssicherheits-Awareness dargestellt. Um dem Leser einen besseren Überblick zu geben, werden in den ersten Kapiteln nicht nur das Konzept „Informationssicherheits-Awareness", sondern auch dessen Theorien, Messmodelle und Fördermaßnahmen präsentiert und analysiert. Danach werden die theoretischen Grundlagen von Serious Games und deren Abgrenzung zu anderen spielerischen Lernkonzepten erläutert. Das letzte Kapitel des theoretischen Teils umfasst die Hauptthemen der Informationssicherheits-Awareness sowie die Darstellung und Diskussion ihrer Relevanz.

Für die Bearbeitung der Forschungsfragen wird ein Mixed-Method-Ansatz verwendet. Dieser Ansatz kombiniert die Aspekte von quantitativen und qualitativen Methoden und kann als selbstständiger Forschungsmethode verstanden werden (Roch, 2017, S. 95 nach Bryman, 2006; Johnson, Onwuegbuzie & Turner, 2007). Um die Forschungsfragen bezüglich des Konzeptes eines gruppenspezifischen Serious Games zu beantworten, wird eine qualitative Studie in Form von Experteninterviews und Gruppendiskussionen durchgeführt. Teilaspekte dieser Arbeit sind bereits Gegenstand einer unveröffentlichten Masterarbeit gewesen, auf der diese Dissertation aufbaut. Insbesondere bei der Begründung der Forschungsmethode „Qualitative Inhaltsanalyse" wird auf Fragmente der besagten Masterarbeit zurückgegriffen (vgl. Pryazhnykova, 2018). Um die Unterschiede zwischen den bei der Volkwagen AG bereits verwendeten Methoden und einem gruppenspezifischen Lernangebot zur Awareness-Förderung herauszuarbeiten, soll ein didaktischer Vergleich erfolgen. Im Anschluss werden eine quantitative, fragebogenbasierte Analyse und Überprüfung der induktiv entwickelten Konzepte vorgenommen.

Die Arbeit schließt mit der Ausarbeitung der Implikationen für die Forschung und die Praxis und bezieht die Ergebnisse auf die vorgestellten Forschungsfragen. Den Abschluss bildet eine zusammenfassende Schlussbemerkung.

2 Informationssicherheits-Awareness

Das Ziel dieses Kapitels ist es, die Ergebnisse der Literaturrecherche zu den theoretischen Verhaltens- und Awareness-Messmodellen zu präsentieren. Nach der Awareness-Definitionserklärung werden die wichtigsten Theorien und Messmodelle dargestellt und analysiert. Insgesamt sollen eine Verständnisgrundlage bezüglich des theoretischen Awareness-Hintergrundes geschaffen sowie die quantitative Untersuchung und die Aktualität dieser Studie begründet werden. Am Ende des Kapitels wird ein Ausblick auf die im Rahmen der Arbeit verwendeten theoretischen Mechanismen gegeben, welche sich im Design und der Nutzung des Fragebogens zur Überprüfung der didaktisch entwickelten Serious-Game-Elemente wiederfinden.

2.1 Was ist Informationssicherheits-Awareness?

In der Forschung existieren mehrere Definitionen von Informationssicherheits-Awareness, da der Begriff relativ komplex ist und mehrere Aspekte beinhaltet (vgl. Jaeger, 2018). Um den Begriff Informationssicherheits-Awareness genauer zu beschreiben, soll zu Beginn der Begriff „Awareness“ eruiert werden.

Er stammt aus dem Englischen und wird als „Bewusstsein“, „gute Kenntnisse“ oder „Wahrnehmung“ übersetzt (Collins German Dictionary, 2004). In dieser Arbeit wird jedoch weiterhin der englische Begriff „Awareness“ benutzt, da er eine Sammlung von verschiedenen Stufen der Informationsverarbeitung in sich vereint (vgl. Jaeger, 2018). Laut Jaeger (2018, S. 4704 in Anlehnung an Bulgurcu, Cavusoglu & Benbasat, 2010; D'Arcy, Hovav & Galletta, 2009; Rhee, Ryu & Kim, 2005; Tsohou et al., 2015; Galvez & Guzman, 2009; Spears & Barki, 2010) kann unter Awareness Folgendes verstanden werden:

- ein bestimmter Bewusstseinszustand
- kognitive Prozesse, die zu dem Bewusstseinszustand beitragen
- eine bestimmte Verhaltensart

Ein vertiefendes Verständnis von Awareness bieten z. B. Schrader und Lawless (2004) analog zu Jaeger (2018) mit einem sogenannten Knowledge-Attitude-Behaviour-Modell (KAB-Modell, S. 9 in Anlehnung an Miller et al., 1990). Dies besagt, dass drei Aspekte des Modells in einer gewissen dynamischen Beziehung zueinander stehen (vgl. Schrader & Lawless, 2004 in Anlehnung an Alexander & Dochy, 1995; Ajzen & Fishbein, 1977; Bruvold, 1990; Kim & Hunter, 1993; Kirby, 1985). Es dient dazu, dass das Wissen (Knowledge-Aspekt) die Einstellung (Attitude-Aspekt) und somit auch das Verhalten (Behaviour-Aspekt) beeinflussen kann (Schrader & Lawless, 2004, S. 11). Allerdings wird das KAB-Modell in der Wissenschaft aufgrund seiner Anwendung stark kri-

tisiert (Parsons et al., 2014, S. 167 in Anlehnung an McGuire, 1969; Baranowski et al., 2003). Grund ist, dass andere individuelle Faktoren, die eventuell u. a. das Wissen beeinflussen können, beim KAB-Modell nicht berücksichtigt werden. Parsons et al. (2014, S. 167 in Anlehnung an Baranowski et al., 2003) geben hierfür ein Beispiel: Obwohl das persönliche Interesse an einem Thema oder die Motivation, ein Thema besser zu verstehen, das Wissen und somit auch die Einstellung und das Verhalten einer Person beeinflussen würden, werden diese Punkte beim KAB-Modell nicht einbezogen. Darüber hinaus bleibt unklar, wie individuelle Faktoren das KAB-Modell beeinflussen können.

Der Begriff Awareness ist mit dem Begriff Situationsbewusstsein oder Situations-Awareness verknüpft (Rauch, 2009). Nach Rauch (2009, S. 3 in Anlehnung an Endsley, 1988, S. 792) ist damit „[...] the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future" gemeint. Situationsbewusstsein besteht aus folgenden kognitiven Tätigkeiten:

- Wahrnehmung der Elemente einer dynamischen Umgebung
- Bedeutung dieser Elemente verstehen
- deren Zustände und nähere Zukunft antizipieren

Rauch (2009, S. 3 f. in Anlehnung an Breton & Rousseau, 2001) unterscheidet in ihrer Studie zwischen verschiedenen Kategorien der Definitionen, die jedoch synonym verwendet werden und voneinander nicht abgetrennt sein können:

- *Prozessorientierter Ansatz von Situationsbewusstsein*
  Situationsbewusstsein kennzeichnet im prozessorientierten Ansatz die kognitiven Prozesse, die in Situationen mit Mehrfachanforderungen entscheidend sind, z. B. bei der Kategorisierung von Informationen (Rauch, 2009, S. 3 f. nach Sarter & Woods, 1995). Die Autoren nennen diesen Ansatz „Erlangen von Wissen über die aktuelle Situation" (Rauch, 2009, S. 4 nach Sarter & Woods, 1995).
- *Zustandsorientierter Ansatz von Situationsbewusstsein*
  Rauch (2009, S. 4 nach Endsley, 1988) beschreibt Situationsbewusstsein „[...] als Produkt oder Wissenszustand [...], der von den Prozessen, die zu diesem Zustand führen, abgetrennt werden muss". Prozessorientierter Ansatz und zustandsorientierter Ansatz von Situationsbewusstsein werden allerdings oft synonym verwendet und nicht sauber voneinander getrennt (Rauch, 2009, S. 4 nach Pew & Mavor, 1998).
- *Operatorfokussierter Ansatz von Situationsbewusstsein*
  Der Fokus des operatorfokussierten Ansatzes liegt auf den persönlichen Charakteristiken, die das Situationsbewusstsein beeinflussen können (Rauch, 2009, S. 4 nach Durso & Gronlund, 1999). Rauch (2009, S. 4 in Anlehnung an Dominguez, 1994) nennt als Beispiel für diesen Ansatz den Aufbau eines mentalen Bildes. Informationsextraktion, Informationsintegration, Projektion und Antizipation sind nach Rauch (2009 in Anlehnung an Endsley, 1998; Dominguez, 1994) die entscheidenden kognitiven Prozesse, die Situationsbewusstsein beeinflussen.

- *Situationsfokussierte Definitionen von Situationsbewusstsein*
  Bei der Betrachtung aus der situationsfokussierten Perspektive wird eine Situation als eine Mischung von Objekten, Ereignissen und Interaktionen von anderen Personen verstanden. Nach Rauch (2009, S. 4 nach Pew, 2000) umfasst Situationsbewusstsein nicht nur den Wissensstand über die Umwelt, sondern auch die Ziele und psychischen und physischen Ressourcen eines Operators.

Schmidt, Gondolf und Haufs-Brusberg (2018, S. 3) beschreiben, dass Informationssicherheits-Awareness einen bestimmten Wissensstand, eine bestimmte innere Einstellung und darüber hinaus eine bestimmte Verhaltensart bezüglich Informationssicherheit darstellt.

Folglich lässt sich ableiten, dass unter Awareness ein Bewusstseinszustand bestehend aus drei Ebenen zu verstehen ist: Wissen, Einstellung und dementsprechendes Verhalten.

2.2 Theoretische Grundlagen

In der allgemeinen Literatur gibt es Studien, die anhand von verschiedenen (Verhaltens-)Modellen das menschliche Verhalten bzw. die menschliche Einstellung zu Informationssicherheit erklären (Parsons et al., 2014, S. 166 in Anlehnung an Bulgurcu, 2008; Ng, Kankanhalli & Xu, 2009; Vance, 2010; Fan & Zhang, 2011; Kruger & Kearney, 2006). Im Folgenden sollen die in der Literatur am meisten verwendeten und etablierten Theorien beschrieben und analysiert werden. Basierend darauf wird im Anschluss erörtert, welches Modell im Rahmen dieser Studie verwendet wird und warum.

Eine der meisterwähnten Theorien im wissenschaftlichen Diskurs bezüglich der Informationssicherheits-Awareness ist die Theorie des geplanten Verhaltens nach Ajzen (Graf, 2007, S. 34 in Anlehnung an Ajzen, 1985, 2005, 2006; Ajzen & Madden, 1986). Sie wurde aus der Theorie der überlegten Handlung nach Ajzen & Fishbein (1980) entwickelt (Graf, 2007, S. 34). Nach dieser Theorie wird ein Verhalten durch eine Verhaltensabsicht bestimmt (siehe Abb. 3).

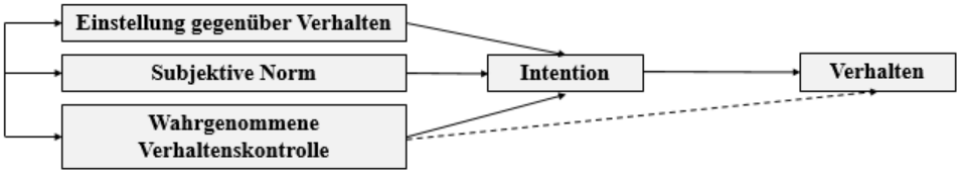


Abbildung 3: Theorie des geplanten Verhaltens (eigene Darstellung orientiert an Studienretter, o. J. in Anlehnung an Ajzen, 1991, S. 182)

Wie anhand der obigen Abbildung zu erkennen ist, wirkt sich nach Ajzens Modell die Einstellung gegenüber einem Verhalten in erster Linie auf die Verhaltensabsicht oder Intention eines Menschen und nicht direkt auf das Verhalten selbst aus (Graf, 2007).

Die Einstellung gegenüber Verhalten wird als eine allgemeine Bewertung eines Verhaltens verstanden und schließt kognitive oder konative Aspekte ein. Außerdem mündet sie in einer bewussten Entscheidung, ein gewisses Verhalten ausüben zu wollen (= Intention) (Graf, 2007). Eine bedeutende Wirkung auf das Verhalten eines Menschen hat auch die sogenannte subjektive Norm, das heißt die soziale Erwartung von anderen Menschen, die von außen auf eine Person einwirkt und die diese wahrnimmt. Neben der Verhaltensabsicht (Intention) ist die wahrgenommene Verhaltenskontrolle ein wichtiger Prädikator für die Ausübung eines Verhaltens. Letztere bezieht sich auf die Kontrolle, über die eine Person verfügt, um ein intendiertes Verhalten auszuüben (Graf, 2007).

Nach dieser Theorie wird das menschliche Verhalten nur vorhersehbar, wenn diese zwei Aspekte vorhanden sind (Graf, 2007, S. 35):

- die Einstellung zum Verhalten an sich
- die vermuteten Erwartungen, die die für die handelnde Person wichtigen Bezugspersonen bezüglich des Verhaltens haben

Einschränkend ist anzumerken, dass das Modell des geplanten Verhaltens nur jenes Verhalten vorhersagen kann, welches vollständig der Kontrolle des Willens unterliegt (Graf, 2007). Doch menschliches Verhalten ist nicht immer rein rational und wohldurchdacht. Unüberlegtes Verhalten aus dem Affekt heraus lässt sich mit dem Modell aber nicht deuten (Graf, 2007).

Safa und von Solms (2016, S. 444) unterstützen dieses Argument und hervorheben in ihrem Forschungsmodell, dass weitere wichtige Aspekte, die das menschliche Verhalten beeinflussen können (z. B. intrinsische oder extrinsische Motivation), jedoch außerhalb des Geltungsbereichs der Theorie des geplanten Verhaltens bleiben.

Eine weitere Theorie, die in Rahmen der Forschung zu Informationssicherheits-Awareness und Verhalten oft eingesetzt wird, ist die „Deterrence-Theorie" (Abschreckungstheorie) (D'Arcy & Herath, 2017). Die Hauptprinzipien dieser Theorie sind, dass Menschen nach Schmerzvermeidung streben und basierend darauf begründete Entscheidungen treffen (vgl. Williams & Hawkins, 1986; Abramovaite et al., 2023). Heißt, wenn eine Handlung mit einer Strafe belegt ist, wird die Wahrscheinlichkeit der Handlungsausübung (Missetat) minimiert (vgl. Williams & Hawkins, 1986). Entscheidend hier sind die Art, der Schweregrad und die Zeit, wann die Strafen oder Sanktionen eintreffen (vgl. Williams & Hawkins, 1986; Abramovaite et al., 2023).

Die Studien, die im Bereich Informationssicherheits-Awareness auf der Abschreckungstheorie basieren, haben das primäre Ziel, die Korrelation zwischen Bestrafung (Sanktionen) und dem konformen und nonkonformen Verhalten in Bezug auf Informationssicherheit (u. a. am Arbeitsplatz, z. B. Einhaltung der Informationssicherheitsregelungen und -richtlinien) zu untersuchen (D'Arcy, Hovav & Galetta, 2009 in Anlehnung an Gopal & Sanders, 1997; Kankanhalli et al., 2003; Straub, 1990; Foltz, 2000; Harrington, 1996; Lee, Lee & Yoo, 2004; Wiant, 2003). Laut Literaturrecherche, kann die Abschreckungstheorie nonkonformes Verhalten zu einem gewissen Grad erklären, aber nicht in allen Szenarien vorhersagen (Trang & Brendel, 2019).

Ein weiteres zu erwähnendes Modell im wissenschaftlichen Diskurs um Informationssicherheits-Awareness liefert Endsley (Rauch, 2009 in Anlehnung an Endsley, 1995). Es fokussiert sich primär auf den Informationsverarbeitungsprozess (Abb. 4). Laut diesem Modell wird eine falsche oder richtige Entscheidung nicht nur durch Situations-Awareness, sondern auch durch „individuelle" Faktoren wie z. B. Fähigkeiten, Informationsbearbeitungsmechanismen, Ziele etc. beeinflusst (Rauch, 2009, S. 5 in Anlehnung an Endsley, 1995). Obwohl dieses Modell erläutert, welche Faktoren Situations-Awareness beeinflussen, kann es nicht erklären, mit welchen Faktoren spezifisch Informationssicherheits-Awareness gemessen werden kann.

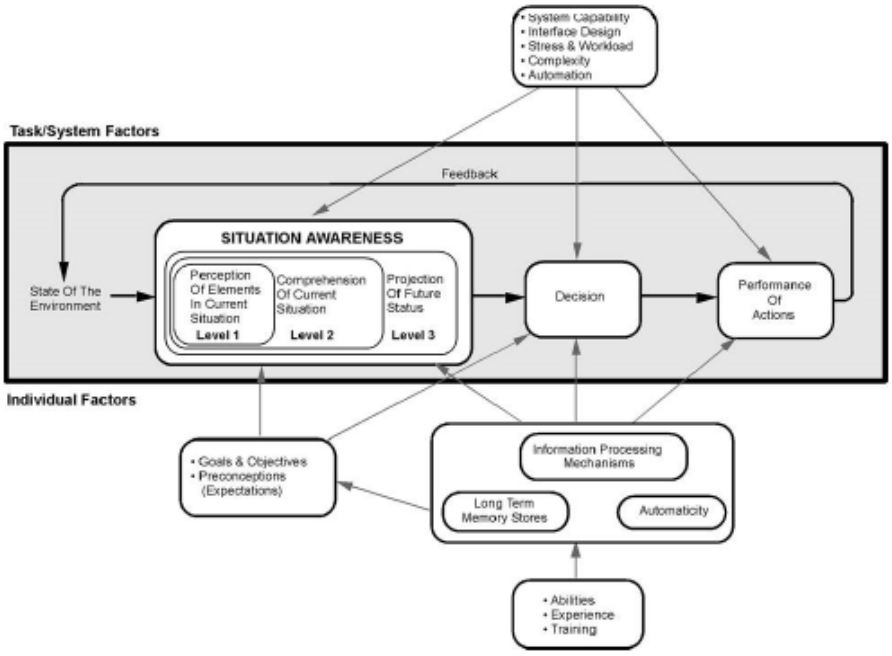


Abbildung 4: Modell von Endsley (Rauch, 2009, S. 5 in Anlehnung an Endsley, 1995, S. 35)

Kritische Anmerkungen zu den bisherigen Untersuchungen, die auf der theoretischen Überprüfung oder Validierung der existierenden Theorien zu menschlichem Verhalten und Informationssicherheit basieren (z. B. auf der Abschreckungstheorie oder der Theorie des geplanten Verhaltens), machen auch Parsons et al. (2014, S. 166 in Anlehnung an Bulgurcu, 2008; Fan & Zhang, 2011) in ihrer Studie „Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)" (weiter als HAIS-Q-Studie). Sie stellen fest, dass darin stets nur einige Variablen bewertet und analysiert werden, während weitere potenziell wichtige Variablen und Aspekte nicht untersucht werden (Parsons et al., 2014, S. 166 in Anlehnung an Karjalainen, 2011). Dies ist besonders wichtig in Bezug auf Informationssicherheits-Awareness innerhalb eines Unternehmens, da das Verhalten von Beschäftigten durch verschiedene Faktoren beeinflusst wird, wie z. B. Persönlichkeitsfaktoren, persönliche Motivation, die Organi-

sation und ihre Kultur etc. (Parsons et al., 2014, S. 166 in Anlehnung an Vroom & von Solms, 2004).

Parsons et al. (2014) betonen in ihrer Studie, dass viele Organisationen Informationssicherheitsbefragungen durchführen, um das allgemeine Awareness-Level der Beschäftigten zu überprüfen. Jedoch sind diese Befragungen primär auf Cybersicherheitsangriffe und deren Wirkungen und nicht auf das Verhalten und die Einstellung von Beschäftigten in Bezug auf Informationssicherheit fokussiert (Parsons et al., 2014, S. 166 in Anlehnung an Deloitte, 2011; Ernst & Young, 2011; PricewaterhouseCoopers, 2013). Die Autoren berichten beispielsweise auch von Untersuchungen zum Thema Informationssicherheit, in der IT-Experten mehrfach die Beschäftigten einer Organisation befragten (Parsons et al., 2014, S. 166 in Anlehnung an Anderson et al., 2012). Zwar verfügt dieses interne IT-Fachpersonal über die Expertise zu internen Sicherheitsvorfällen, zur Informationssicherheitsstruktur, zu Informationssicherheitsaudits etc., doch das heißt nicht, dass dies auch die Mehrheit der Computerbenutzer tut oder dass diese die gleichen Einstellungen zum Thema Informationssicherheit teilen wie die IT-Experten (Parsons et al., 2014, S. 166 in Anlehnung an Herath & Rao, 2009). Des Weiteren werden Informationssicherheitsbefragungen und -beratungen meist von externen Anbietern durchgeführt, die spezifische Lösungen in Form von Schulungen und Trainings zur Informations-Awareness anbieten (Parsons et al., 2014, S. 166 in Anlehnung an Anderson et al., 2012). Dies ist insofern problematisch, als dass der Fokus dieser Anbieter entsprechend auf ihren jeweiligen Produkten liegt, was mit widersprüchlichen Motiven ihrerseits verbunden sein könnte (z. B., dass einige bestimmte Informationssicherheitslücken zu oft gefunden und andere übersehen werden) (Parson et al., 2014, S. 166 in Anlehnung an Anderson et al., 2012).

Zudem sei hier noch mal betont, dass viele der bisherigen Untersuchungen das primäre Ziel hatten, nur ein spezifisches Element der Informationssicherheits-Awareness zu eruieren, wie z. B. das Verhalten im Umgang mit Passwortrichtlinien oder der Nutzung von USB-Geräten (Parsons et al., 2014 in Anlehnung an Stanton et al., 2005). Dadurch mangelt es an Forschung, die Informationssicherheits-Awareness umfänglich in den Blick nimmt.

Das Ziel der Studie von Parsons et al. (2014) lag wiederum darin, festzustellen, in welchem Zusammenhang Richtlinienkenntnisse, Einstellungen zu Richtlinien und Prozessen und daraus resultierendes Verhalten bei der Arbeit am Arbeitscomputer stehen. Die HAIS-Q-Studie von Parsons et al. (2014, S. 169) basiert auf dem Wissen-Einstellung-Verhalten-Modell der Informationssicherheits-Awareness. Die Forscher überprüfen in ihrer Studie drei Hypothesen, nämlich:

Hypothese 1. Bessere Richtlinien- und Prozesskenntnisse resultieren in einer besseren Einstellung und Akzeptanz bezüglich Richtlinien und Prozessen.

Hypothese 2. Eine bessere Einstellung zu Richtlinien führt zu einem Verhalten, das die handelnde Person als risikoavers einschätzt.

Hypothese 3. Bessere Richtlinienkenntnisse sind mit einem Verhalten verbunden, das als risikoavers eingeschätzt wird.

Das Forschungsmodell der HAIS-Q-Studie beruht wie oben bereits erwähnt auf drei Ebenen (Wissen, Einstellung und Verhalten), wobei „Wissen" hier als „Richtlinien- und Prozesskenntnisse" definiert wird. Folgende Untersuchungsgebiete wurden für den Bereich Informationssicherheits-Awareness definiert: Internetnutzung, E-Mail-Nutzung, Nutzung sozialer Netzwerke, Passwortmanagement (einschließlich Sperren von Arbeitscomputern), Incident-Management, Informationsverarbeitung und mobiles Arbeiten. Da im Fokus das menschliche Verhalten steht, wurde jeder Schwerpunkt in drei Ebenen differenziert (gutes, neutrales und schlechtes Verhalten).

Die Befragung der HAIS-Q-Studie fokussiert sich auf neutrales Verhalten. Das neutrale Verhalten ist mit menschlichen Fehlern verbunden, die aus Versehen, ohne Absicht, aus Naivität und Unwissenheit gemacht werden (Parsons et al., 2014, S. 167 in Anlehnung an Stanton et al., 2005).

Die Studie wurde mit 1073 Personen durchgeführt. Obwohl es den Forschern gelungen ist, die Hypothesen teilweise zu bestätigen (besseres Wissen über Richtlinien ist mit der besseren Einstellung zu Richtlinien verbunden; besseres Wissen und bessere Einstellung zu Richtlinien führen zu einem vorsichtigeren Verhalten in Bezug auf Informationssicherheitsrisiken und -gefahren), können die Richtlinienkenntnisse nur ca. 66 % der Abweichungen in der Einstellung der Teilnehmer prognostizieren (Parsons et al., 2014, S. 171 f.). Weitere Ergebnisse der Studie weisen darauf hin, dass ca. 78 % der Abweichung im Verhalten durch die Richtlinienkenntnisse und die Einstellung zu Richtlinien und Prozessen determiniert werden (Parsons et al., 2014, S. 172).

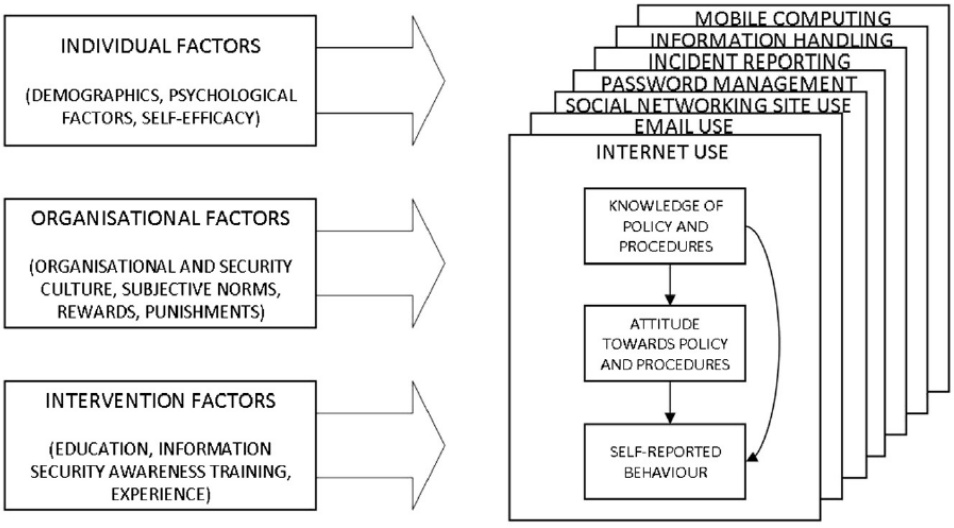


Abbildung 5: Faktoren, die das HAIS-Q-Modell beeinflussen (Parsons et al., 2014, S. 169)

Obwohl das HAIS-Q-Studie teilweise die Korrelation zwischen Wissen, Einstellung und Verhalten erklärt, sind folgende Punkte offengeblieben: Es wird nicht genau definiert und untersucht, welche individuellen und organisatorischen Faktoren Wissen, Einstellung und Verhalten beeinflussen und inwiefern sich solche Einflüsse auswirken.

Außerdem wurden die sieben Schwerpunkte der HAIS-Q-Befragung (Internetnutzung, E-Mail-Nutzung, Nutzung sozialer Netzwerke, Passwortmanagement, Incident-Management, Informationsverarbeitung und mobiles Arbeiten) nach Parsons et al. (2014) als separate, abgetrennte Modelle vorgestellt. Es gibt keinen Vergleich, ob Wissens-, Einstellungs- und Verhaltenselemente innerhalb dieser sieben Schwerpunkte einheitlich bleiben; auch nicht, ob und inwiefern das Wissen die Einstellung, die Einstellung das Verhalten sowie wiederum das Wissen das Verhalten beeinflusst.

Informationssicherheit ist ein sich schnell entwickelndes Feld. Es bleibt offen, inwiefern die Ergebnisse der HAIS-Q-Studie für weitere Branchen wie die Automobilindustrie in Deutschland in diesem Kontext noch in der Zukunft relevant ist. Außerdem wurden einige Aspekte der Informationssicherheits-Awareness gar nicht explizit präsentiert. Das Forschungsmodell der HAIS-Q-Studie gibt zudem keine Auskunft darüber, wie Informationssicherheits-Awareness gesteigert werden könnte und welche Maßnahmen eingesetzt werden sollten, um das Niveau der Informationssicherheits-Awareness der Beschäftigten nachhaltig zu verbessern.

2.3 Awareness-Maßnahmen in theoretischen und praktischen Kontext

Wie bereits angedeutet, stellt das unbeabsichtigte Verhalten von Beschäftigten die häufigste Ursache für einen Verstoß gegen bzw. Angriff auf die Informationssicherheit dar. Deswegen gibt es innerhalb der Unternehmen und Organisationen verschiedene Maßnahmen für die Sensibilisierung der Beschäftigten zum Thema Informationssicherheit. In diesem Abschnitt werden die schon existierenden Maßnahmen präsentiert und analysiert. Auf Basis der bestehenden Literatur kommen zwei nicht-technische Maßnahmen zur Verhinderung von Angriffen auf die Informationssicherheit durch das unbeabsichtigte Fehlverhalten der Beschäftigten infrage. Zum einen sind das Richtlinien (vgl. Lebek et al., 2014, S. 1050 in Anlehnung an Bulgurcu, Cavusoglu & Benbasat, 2010; Pahnila, 2007a, 2007b), welche die Regeln für den richtigen Umgang mit Informationen eines Unternehmens festhalten und oftmals als Grundlage für weitere Maßnahmen zur Sicherstellung von Informationssicherheit dienen. Zum anderen sind es Awareness-Programme bzw. -Kampagnen (vgl. Lebek et al., 2014, S. 1050 in Anlehnung an Abraham, 2011; D'Arcy & Hovav, 2009), welche oftmals aus den Richtlinien zur Gewährleistung von Informationssicherheit abgeleitet werden.

Es gibt verschiedene Wege, ein Informationssicherheits-Awareness-Lernprogramm bzw. eine Informationssicherheits-Awareness-Kampagne in einem Unternehmen zu gestalten. Khan et al. (2011) nennen Lernmaßnahmen wie z. B. Präsentationen,

Computerspiel, computerbasiertes Training, Gruppendiskussion, Newsletter etc. (Abb. 6), bei denen die Beschäftigten aktive bzw. teilweise aktive und passive Rollen übernehmen.

S/No.	Tool and technique	Component of knowledge	Component of attitude change	Component of subjective norms	Component of intention	Change in behavior	Overall effectiveness
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

Abbildung 6: Verschiedene Awareness-Maßnahmen (Khan et al., 2011, S. 10863)

Interessant ist, dass eine Methode wie ein Computerspiel laut Khan et al. (2011) als eine eher ungeeignete Methode für Awareness-Maßnahmen betrachtet wird, da diese Methode keine Komponente des Wissenstransfers beinhaltet, es sei denn, der Spieler hat sich das Wissen über Informationssicherheit bereits vor Spielbeginn angeeignet. Die Forscher weisen darauf hin, dass diese Methode gut ist, um den Spieler zu motivieren und Verhaltensänderungen zu erzielen, allerdings ist sie laut Khan et al. (2011) keine gute Wissensaneignungsmethode. Kontrovers zur Meinung von Khan et al. (2011) stellt Scholl (2018a, S. 7 in Anlehnung u. a. an. Albrechtsen, 2007; Straub & Welke, 1998; San Nicolas-Rocca, Schooley & Spears, 2014) in ihrer Studie die Idee vor, dass Informationssicherheits-Awareness-Maßnahmen, deren Hauptziel reiner Wissenstransfer ist (wie Präsentationen, webbasiertes Training), keine dauerhafte Informationssicherheits-Awareness bei den Mitarbeitern generieren können. Die verschiedenen Ansätze und Ansichten in der Forschung bezüglich Informationssicherheits-Awareness-Maßnahmen lassen sich dadurch erklären, dass die Forscher Maßnahmen beschreiben, die keine einheitliche Lösung für die Steigerung der Informationssicherheits-Awareness anbieten können, sondern sich immer nur auf Teilaspekte der Informationssicherheit konzentrieren.

Nach Scholl (2018a, S. 17 in Anlehnung an Pokoyski, 2009; Haucke & Pokoyski, 2018) sollen Informationssicherheits-Awareness-Maßnahmen (abgesehen vom Wissenstransfer-Ansatz) zudem folgende Aspekte mit in die Entwicklung entsprechender Maßnahmen einbeziehen: Zum einen müssen Informationssicherheits-Awareness-Maßnahmen die Beschäftigten „emotional ansprechen", z. B. mit einem Marketingansatz, und zum anderen sollen sie eine soziale und individuelle Partizipation möglich machen.

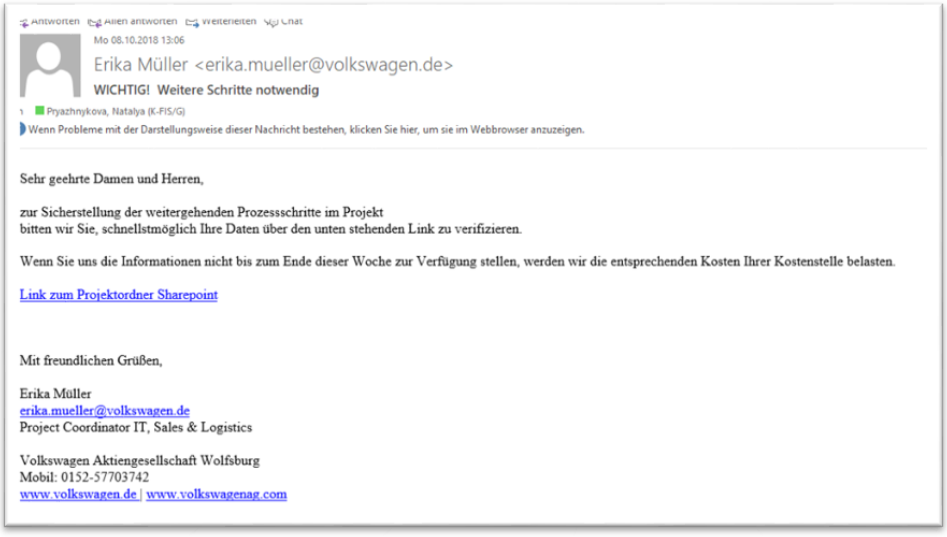
Als mögliche Umsetzung eines solchen Konzeptes stellt Scholl (2018a, S. 10 ff., 2018b, S. 33 f.) eine sogenannte Security Arena vor. Im Rahmen der Security Arena werden verschiedene analoge Spiele zum Thema Informationssicherheit (wie z. B. „Phishing", „Social Engineering", „Sicher unterwegs", „Cyber Security", „Informationsklassifizierung" und „Passwort-Hacking") präsentiert und konzipiert. Das Ziel der Security Arena ist es, eine nachhaltige Steigerung der Informationssicherheits-Awareness bei den Beschäftigten zu fördern. Auch bei der Volkswagen AG gibt es verschiedene Awareness-Maßnahmen. Auf die in dieser Arbeit relevanten Awareness-

Maßnahmen der Volkswagen AG wird im Folgenden eingegangen. Eine didaktische Bewertung dieser erfolgt im Rahmen der qualitativen Studie.

Awareness-Maßnahmen bei Volkswagen

Zurzeit finden bei der Volkswagen AG verschiedene Informationssicherheits-Awareness-Veranstaltungen statt, deren Ziel es ist, die Beschäftigten für das Thema Informationssicherheit zu sensibilisieren. Im Jahre 2019 haben u. a. folgende Informationssicherheitsmaßnahmen bei der Volkswagen AG stattgefunden:

- Phishing-Kampagne
  Ziel dieser Maßnahme war es, herauszufinden, wie viele Beschäftigten der Volkswagen AG auf eine angebliche Phishing-E-Mail klicken würden. Die E-Mail wies viele Besonderheiten einer Phishing-E-Mail (Bedrohung, Link ohne inhaltliche Beschreibung etc.) auf, trotzdem war die Klickrate extrem hoch (Abb. 7).


Antworten Allen antworten Weiterleiten Chat

Mo 08.10.2018 13:06

Erika Müller <erika.mueller@volkswagen.de>

WICHTIG! Weitere Schritte notwendig

Pryazhnykova, Natalya (K-FIS/G)

Wenn Probleme mit der Darstellungsweise dieser Nachricht bestehen, klicken Sie hier, um sie im Webbrowser anzuzeigen.

Sehr geehrte Damen und Herren,

zur Sicherstellung der weitergehenden Prozessschritte im Projekt
bitten wir Sie, schnellstmöglich Ihre Daten über den unten stehenden Link zu verifizieren.

Wenn Sie uns die Informationen nicht bis zum Ende dieser Woche zur Verfügung stellen, werden wir die entsprechenden Kosten Ihrer Kostenstelle belasten.

Link zum Projektordner Sharepoint

Mit freundlichen Grüßen,

Erika Müller
erika.mueller@volkswagen.de
Project Coordinator IT, Sales & Logistics

Volkswagen Aktiengesellschaft Wolfsburg
Mobil: 0152-57703742
www.volkswagen.de | www.volkswagenag.com

Abbildung 7: Beispiel einer Phishing-E-Mail (Phishing-Kampagne der Volkswagen AG, 2019)

- Expertenvorträge
  Externe und interne Experten halten ihre Vorträge zu den Themen Datenschutzgrundverordnung, Datenschutz im Unternehmen, Hacking etc. digital und auch als Präsenzveranstaltung an verschiedenen Standorten der Volkswagen AG.
- Sensibilisierungsveranstaltung „Start@IT“
  Ziel dieser Sensibilisierungsveranstaltung ist es, bei den neuen IT-Beschäftigten eine gewisse Informationssicherheits-Awareness zu schaffen und die IT-Abteilungen zu präsentieren.
- Security Arena
  Analog zu Scholls (2018a; 2018b) Security Arena finden bei der Volkswagen AG regelmäßig Security Arenen statt (Abb. 8). Die Security Arena bei Volkswagen

stellt ein interaktives, spielbasiertes und analoges Lernkonzept zu Themen aus dem Bereich der Informationssicherheit dar. Bei der Security Arena von Volkswagen gibt es sechs Spielstationen, die als Team-Circuit-Training verwendet werden können, wo die Teams (max. 10 Teilnehmer) von einer „Spielstation" zu einer anderen rotieren.

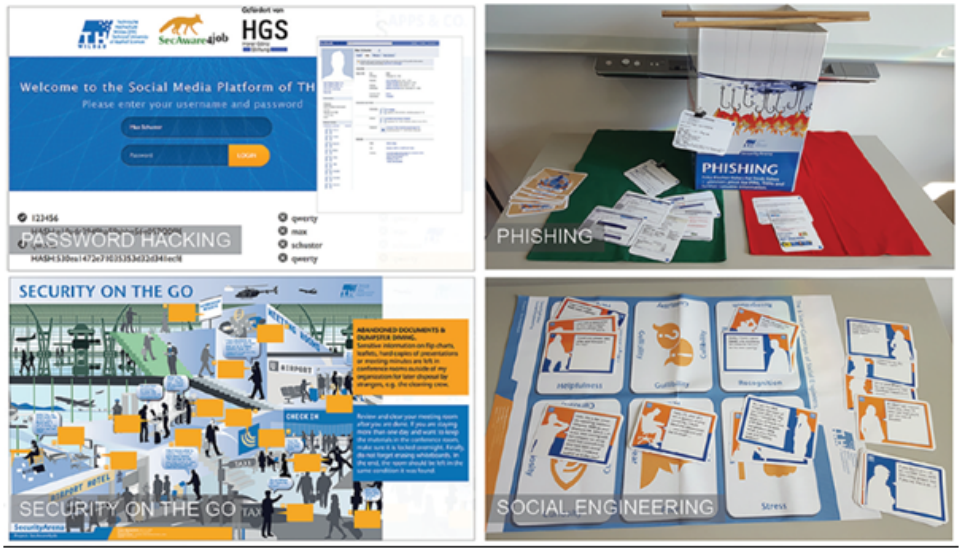


Abbildung 8: Security Arena (Scholl, 2018b, S. 33)

2.4 Serious Games

„Serious Games" ist ein umstrittener Begriff in der Forschungsliteratur. Nach Bopp (2009) sind Serious Games digitale spielbasierte Anwendungen zur Vermittlung eines Lerninhaltes. Nach Högsdal (2011, S. 117 nach Kriz, 2010) existierte der Begriff „Serious Games" bereits vor der Erfindung von Computer- und Onlinespielen und wurde ursprünglich primär für Brett- und Kartenspiele benutzt. Mit zunehmender Digitalisierung wurden auch die Serious Games zu computerbasierten Spielen (Högsdal, 2011). Drei Aspekte, die ein modernes Serious Game definieren, sind „[...] die Interaktion zwischen den Beteiligten, die Künstlichkeit der Spielwelt und die Regeln, die den Handlungsraum beschränken" (Bopp, 2009, S. 2 in Anlehnung an Wechselberger, 2009, S. 98).

Der Lernprozess beim Spielen eines Serious Games kann durch verschiedene Lerneffekte entstehen. Laut Bopp (2009, S. 3) können die Lerneffekte „[...] feinmotorische (z. B. Hand-Auge-Koordination), kognitive (z. B. Problemlösungsstrategien), persönliche (z. B. Handlungsmuster), soziale (e. g. Zusammenarbeit und Kommunikation) und kulturelle (z. B. Vermittlung von Werten und Normen) Bereiche umfassen".

Was aber kommerzielle Computerspiele und Serious Games unterscheidet, ist, dass Serious Games einen intendierten Lerninhalt aufweisen und nicht primär zur Unterhaltung dienen (Bopp, 2009, S. 3; Högsdal, 2011 in Anlehnung an Abt, 1970). Auch wenn es nach Bopp (2009) nicht entscheidend ist, ob ein Spieler spielt, um Spaß zu haben oder um zu lernen.

Bopp (2009, S. 4 ff.) kategorisiert Serious Games nach ihren Anwendungsbereichen in folgende Kategorien:

- Educational Games sind Lernspiele, deren Hauptziel es ist, ein Basiswissen zu vermitteln und einen bestimmten Lernstoff spielerisch zu lehren.
- Corporate Games vermitteln spezifische Fähigkeiten und finden in der beruflichen Aus- und Weiterbildung ihren Einsatz. Bei diesen Serious Games geht es in erster Linie um das Erlernen von bestimmten Fertigkeiten.
- Bei sogenannten Health Games handelt es sich um die Förderung von konkreten medizinischen Trainings, die positive psychologische oder physiologische Effekte bei den Spielern hervorrufen sollen. Eine Anbindung solcher Spiele findet z. B. im Rahmen psychotherapeutischer Zwecke statt.
- Persuasive Games haben das Ziel, den Spielern bestimmte Ideen (politische, ökologische oder religiöse) näherzubringen und zu erläutern.
- Music Games helfen den Spielern dabei, Gehörbildung und generelles musikalisches Verständnis zu entwickeln.

Eine weitere Unterscheidung lässt sich zwischen Serious Games und anderen spielerischen Konzepten wie z. B. Gamifikation und Simulation machen. Wie bereits beschrieben, sind Serious Games eigenständige computerbasierte Spiele oder auch Brett- und Kartenspiele mit definierten Bildungs- oder Trainingszielen. Bei einem Gamifikationseinsatz hingegen werden verschiedene spielerische Elemente in spielfremde Kontexte integriert, um z. B. Produktangebote oder Services zu fördern und Nutzer durch Belohnungspunkte, diverse Erfahrungsabzeichen etc. dazu zu motivieren, mehr mit einem Produkt zu interagieren (Tolks & Lampert, 2016, S. 197 in Anlehnung an Deterding et al., 2011, S. 10; Werbach & Hunter, 2012). Simulationen haben im Vergleich zu Serious Games das Ziel, die Realität so nah wie möglich nachzubilden (Tolks & Lampert, 2016, S. 202). Simulationen stellen oft eine Möglichkeit zur Erprobung einer bereits erworbenen Fähigkeit dar und haben kein klar definiertes „Spielziel“, mit dem ein entsprechendes Belohnungssystem verbunden ist (Tolks & Lampert, 2016, S. 202; Unger, Goossens & Becker 2015, S. 159). Wie schon eruiert, haben Serious Games bestimmte definierte Kriterien, nämlich ein Lernziel sowie Spielregeln, und sie stellen eine künstliche Spielwelt dar (Tolks & Lampert, 2016; Bopp, 2009, S. 2 in Anlehnung an Wechselberger, 2009, S. 98). Diese Kriterien finden in dieser Arbeit für die Definition von Serious Games weiterhin Anwendung.

2.5 Handlungsfelder der Informationssicherheits-Awareness-Maßnahmen

In der Theorie und der Praxis werden immer wieder verschiedene Kontexte genannt, in denen gegen Informationssicherheitsrichtlinien verstoßen wird. Venkatraman et al. (2018) analysierten verschiedenste Verstöße gegen Richtlinien zur Gewährleistung von Informationssicherheit, basierend auf einer Erhebung solcher Verstöße in verschiedenen Unternehmen und Branchen. Als Ergebnis zeigen die Autoren unterschiedliche Bestandteile von Verstößen in Form einer Taxonomie und zudem die häufigsten Typen von Verstößen gegen Richtlinien der Informationssicherheit auf. Darunter zählen vor allem unautorisierte Bearbeitung privater E-Mails, unautorisierte Nutzung der IT-Systeme, Social Engineering, inkorrekter Umgang mit Informationen im Unternehmen (Venkatraman et al., 2018 in Anlehnung an u. a Whitty & Carr, 2006; Dhillon & Moores, 2001; Vance, Lowry, & Eggett, 2015).

Allerdings existieren in der Forschung weitere wichtige Arten von Informationssicherheitsverstößen wie mangelnde Passwortsicherheit (Raza et al., 2012; Parsons et al., 2014; Parsons et al., 2017; Shen et al., 2016) und unachtsame Endgerätenutzung (Hoffmann, 2019; Parsons et al., 2014, Parsons et al., 2017). Basierend auf der Annahme, dass diese Arten von Verstößen die häufigsten in Unternehmen sind, greift diese Arbeit die genannten Kontexte auf. Bevor eine Einordnung in den Forschungskontext geschieht, werden die unterschiedlichen Arten von Vergehen gegen die Informationssicherheit vorgestellt und beschrieben.

2.5.1 E-Mail-Bearbeitung

Das Thema E-Mail-Bearbeitung wurde im vorherigen Kapitel bereits als „Phishing" adressiert, wird aber auch explizit in der HAIS-Q-Studie hervorgehoben (Parsons et al., 2014; Parsons et al., 2017). Auch andere Forscher inkludieren den Aspekt „E-Mail-Bearbeitung" in den wissenschaftlichen Diskurs über Informationssicherheits-Awareness wie z. B. Desolda et al. (2022) oder Naqvi et al. (2023), in deren Studien ebenfalls Phishing adressiert wurde.

Außerdem geht aus dem Verizon Data Breach Investigations Report von 2019 geht hervor, dass mehr als 90 % der Malware per E-Mail übermittelt wurden. Darüber hinaus stellt Phishing eine der größten Gefahren für die Informationssicherheit dar, aus diesem Grund soll das Thema „E-Mail-Bearbeitung" in dieser Arbeit mitadressiert werden.

Darüber hinaus sind folgende Aspekte der E-Mail-Bearbeitung für diese Arbeit relevant (basierend auf Parsons et al., 2014; Parsons et al., 2017):

- Phishing-E-Mails sind anhand von diversen Merkmalen erkennbar (gefälschte E-Mail-Adresse, Anhänge, Links in den E-Mails)
- Mitarbeiter wissen, wie man eine Phishing-E-Mail bearbeiten soll (keine Anhänge aufmachen, Links in den Phishing-E-Mails nicht anklicken, Phishing-E-Mails löschen).

In weiteren Kapiteln wird detaillierter erklärt, wie diese Aspekte untersucht werden.

2.5.2 Passwortmanagement

Das Thema „Passwortmanagement" spielt eine wichtige Rolle im wissenschaftlichen Diskurs. Einer der bedeutendsten Aspekte im Bereich des Passwortmanagements ist die Wiederverwertung von Passwörtern (obwohl Unternehmen immer mehr in Sicherheitstools wie Multifaktor-Authentifizierung investieren). Dies hat der neue Global Password Security Report von LastPass ergeben (Sieger, 2019). Zudem sind laut dem Magazin Digital Business Cloud (Sieger, 2019) bei 80 % der Hackerangriffe gestohlene und wiederverwendete Anmeldeinformationen das Einfallstor. Daher müssen Unternehmen mehr Maßnahmen ergreifen, um die Passwort- und Zugriffssicherheit zu verbessern und damit das Risiko von (erfolgreichen) Angriffen aus eigener Kraft zu mindern (Sieger, 2019). Denn eine überwältigende Anzahl von Passwörtern führt zu einer schlechten Passworthygiene, wenn es keine Technologie gibt, die bei der Verwaltung hilft.

Auch in der HAIS-Q-Studie sind diese Aspekte inkludiert (Parsons et al., 2017). Die Autoren erwähnen in ihrer Taxonomie ähnlich zu den anderen Wissenschaftlern, dass die wichtigsten Aspekte des Passwortmanagements folgende sind: Passwortverwendung (Benutzung desselben Passworts für diverse IT-Systeme) und Teilung des Passwortes sowie Benutzung eines starken Passworts (unter der Bezeichnung „starkes Passwort" ist gemeint, dass das Passwort sicher ist und verschiedene Richtlinien des Passwortmanagements inkludiert, z. B. Passwörter bestehend aus Klein- und Großbuchstaben, Sonderzeichen, Zahlen).

Dementsprechend lässt sich ableiten, dass das Thema Passwortmanagement für die vorliegende Studie und Untersuchung der Informationssicherheits-Awareness bei Volkswagen entscheidend ist. Die zu untersuchenden Aspekte des Passwortmanagements, die auch in der Literatur (vgl. Parsons et al., 2017) aufgeführt werden, sind:

- Wiederverwendung von Passwörtern
- Benutzung desselben Passworts privat (für z. B. soziale Netzwerke) und beruflich (für diverse Volkswagen-IT-Systeme)
- Teilung des Passworts mit den Kollegen

Das Thema Passwortmanagement wird im Rahmen dieser Arbeit auch in den weiteren Kapiteln genauer diskutiert und analysiert.

2.5.3 Umgang mit Informationen

Wie die Ergebnisse der Cyber-Sicherheits-Umfrage von 2015 zeigen, haben mehr als 70 % der befragten Institutionen angegeben, dass sogenanntes „Social Engineering" das größte Bedrohungspotenzial in der näheren Zukunft darstellen wird, gefolgt von Datendiebstahl, E-Mail-Spam, Sabotage von IT-Systemen, Hacking zum Missbrauch von Websites usw. (BSI, 2015). Laut Keyworth (2016) wurde Social Engineering-Betrug von der internationalen Polizeibehörde Interpol als einer der weltweit aufkommenden Betrugstrends identifiziert. Daher sollen im nächsten Abschnitt die Definition von

Social Engineering vorgestellt, Beispiele des Social Engineerings beleuchtet und Maßnahmen zur Prävention erläutert werden.

Social Engineering bedeutet die „[...] gezielte Nutzung psychologischer Manipulationstechniken, um jemanden zu Handlungen zu bewegen, die nicht seiner Einstellung entsprechen" (Weidenhammer, 2023, o. S.). Das Ziel des Social Engineerings ist es nicht, direkt technische Systeme zu manipulieren, sondern Informationen zu gewinnen bzw. den Nutzer dazu zu bringen, eine vom Angreifer gewünschte Aktion durchzuführen (Hommel & Reiser, 2016, S. 3).

Es gibt verschiedene Taktiken, die Social Engineers benutzen:

- Vishing/Phishing. Die Angriffsart, bei der Opfer von Cyberangriffen via Telefon oder Voice Mail (Vishing) bzw. per E-Mail und durchs Internet (Phishing) kontaktiert werden (vgl. Bisson, 2023; Ashfaq et al., 2024; Tiwari, 2018).
- Baiting. Social Engineers lassen USB-Sticks oder CD-Discs an öffentlichen Orten liegen, in der Hoffnung, dass jemand sie aus Neugierde aufnimmt und auf seinen Geräten verwendet (Bisson, 2023; Tiwari, 2018).
- Identitätsdiebstahl. Das Bundesamt für Sicherheit und Informationstechnik (2023) warnt vor weiteren Gefahren online, die oft unterschätzt werden, nämlich den Gefahren sozialer Netzwerke – beispielsweise Identitätsdiebstahl oder das Ausspähen privater Informationen, die Social Engineers über soziale Netzwerke bekommen können. Folglich ist der informationssicherheitskonforme Umgang mit privaten Informationen in sozialen Netzwerken von einer großen Bedeutung. Jedoch kann der Diebstahl persönlicher oder vertraulicher Daten nicht nur online erfolgen, sondern z. B. auch, indem Social Engineers ihre Opfer bei der Verwendung ihrer Endgeräte (Handy, etc.) beobachten (sogenanntes „Shoulder Surfing") und dabei wichtige persönliche Daten wie z. B. Passwörter, PIN-Nummer etc. stehlen (vgl. Bošnjak & Brumen, 2019; Saad, 2023).

Andere Aspekte des Social Engineerings werden in anderen Kapiteln detaillierter angesprochen (wie z. B. Phishing in Kapitel 2.5.1 oder Baiting in Kapitel 2.5.4), jedoch spielen der Umgang mit Informationen in sozialen Netzwerken und der damit verbundene Identitätsdiebstahl eine sehr große Rolle im wissenschaftlichen Diskurs, deshalb wird in diesem Kapitel näher darauf eingegangen.

Als ein Beispiel für den Umgang mit Informationen in sozialen Netzwerken gelten folgende Experimente: Das „Robin Sage Experiment" von Thomas Ryan (2010) und die fingierte Person „Emily Williams" von Muniz und Lakhani (2013). Bei beiden Experimenten wurde mit der Erstellung eines „Fake-Social-Accounts" auf solchen Plattformen wie Facebook (FB), LinkedIn, Twitter etc. gearbeitet, um zu überprüfen, welche sensiblen und vertraulichen Informationen die anderen Nutzer der sozialen Netzwerke bereit sind, preiszugeben (Muniz & Lakhani, 2013).

„Robin Sage" (Abb. 9) wurde entwickelt, um sensible Informationen von US-Militärangehörigen zu erhalten. Laut den Social-Networking-Profilen von Sage ist sie eine 25-jährige IT-Sicherheitsberaterin beim Naval Network Warfare Command in Norfolk,

Virginia (Ryan, 2010, S. 3; Hommel & Reiser, 2016, S. 6). Sie machte ihren Abschluss am Massachusetts Institute of Technology und hat angeblich zehn Jahre Berufserfahrung, trotz ihres jungen Alters (Ryan, 2010; Hommel & Reiser, 2016). Ryan ist es mit seinem Fakeprofil „Robin Sage" gelungen, fast 300 Personen zu kontaktieren, die meisten davon Sicherheitsspezialisten, Militärangehörige, Mitarbeiter von Nachrichtendiensten und Verteidigungsunternehmen (Hommel & Reiser, 2016, S. 6).

Das Experiment „Robin Sage" dauerte vier Wochen und währenddessen hat „Robin Sage" nicht nur Zugang zu vertraulichen Informationen und Dokumenten erhalten (wie z. B. Bankkonten, Truppenstandorte etc.), sondern auch diverse Jobangebote von Google und Lockheed Martin bekommen (Hommel & Reiser, 2016, S. 6). Doch „Robin Sage" hatte auch Schwachstellen, so haben beispielsweise einige Nutzer versucht, „Robin Sage" über das Alumni-Netzwerk des Massachusetts Institute of Technology zu finden oder ihre Telefonnummer bzw. E-Mail-Adresse zu überprüfen (Waterman, 2010).

Analog zu „Robin Sage" wurde „Emily Williams" von Joey Muniz and Aamir Lakhani im Jahr 2011 entwickelt (Abb. 9) (Muniz & Lakhani, 2013). Muniz und Lakhani wollten mit „Emily Williams" nicht nur sensible Information, sondern auch Zugang zur virtuellen privaten Netzwerkverbindung (VPN) der US-Regierung sowie die Kontrolle über deren E-Mail-System usw. erhalten (Henderson et al., 2015 in Anlehnung an Muniz & Lakhani, 2013).

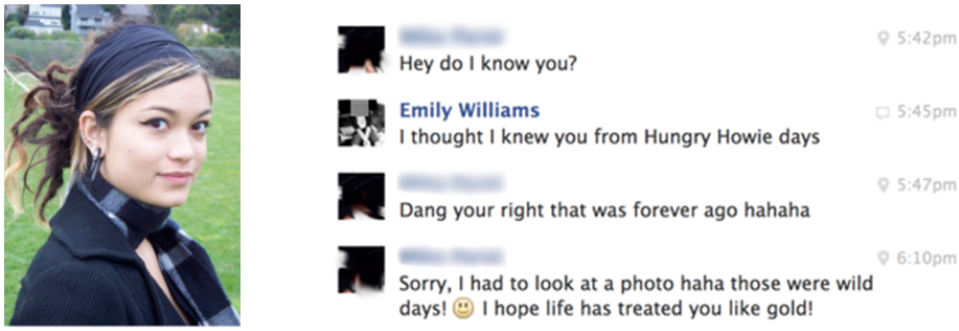


Abbildung 9: Social-Engineering-Beispiel nach „Robin Sage" (links) und Chatverlauf „Emily Williams" (rechts) (Hommel & Reiser, 2016, S. 6; Muniz & Lakhani, 2013)

Das Experiment lief wie folgt ab: Im ersten Schritt wurde ein gefälschtes Profil von einer Frau auf verschiedenen sozialen Netzwerken angelegt. Die Profilfotos waren private Fotos von einer Kellnerin aus dem Restaurant in der Nähe von der Firma, die angegriffen werden sollte (Henderson et al., 2015, S. 3 in Anlehnung an Muniz & Lakhani, 2013). „Emily Williams" hat die Fotos für das Experiment freiwillig zur Verfügung gestellt.

Danach haben Muniz und Lakhani als „Emily" über 100 Facebook-Nutzern Freundschaftsanfragen geschickt. In diesem Schritt haben nur einige Facebook-Nutzer hinterfragt, warum Emily Williams mit ihnen befreundet sein möchte (Henderson et al.,

2015). In solchen Fällen hat „Emily Williams“ ihnen mit Informationen geantwortet, die sie aus den Profilen dieser Nutzer erhalten hatte (Henderson et al., 2015).

Nachdem „Frau Williams“ genug Facebook-Freunde hatte, hat sie einen Titel und eine neue Arbeitsposition „bekommen“ (Henderson et al., 2015 in Anlehnung an Muniz & Lakhani, 2013). Über Facebook hat es eine junge, attraktive, imaginäre Frau also auf diese Weise geschafft, mehrere IT-Mitarbeiter und Mitarbeiter in Führungspositionen zu kontaktieren und sich mit ihnen auf der Social-Media-Plattform zu befreunden (Henderson et al., 2015 in Anlehnung an Muniz & Lakhani, 2013). Das Experiment hat während der Vorweihnachtszeit stattgefunden, deswegen war es nicht verdächtig, wenn Emily einigen ihrer Freunde eine „Weihnachtsgruß-Postkarte“ in Facebook gesendet hat, auf die einige Facebook-Freunde dann auch geklickt haben. Da einige Mitarbeiter soziale Netzwerke bzw. Facebook auf den Arbeitscomputern aufgerufen haben, haben Muniz und Lakhani einen Zugriff auf einige interne Systeme erhalten (Henderson et al., 2015 in Anlehnung an Muniz & Lakhani, 2013). Folglich spielt der Umgang mit Informationen (Shoulder Surfing und auch der Umgang mit Informationen in den sozialen Netzwerken) eine große Rolle in Bezug auf die Informationssicherheit in einem Unternehmen.

Eine weitere wichtige Angriffsart von Social Engineering ist „Tailgating/Piggybacking“ (Rouse, 2022). Ein Beispiel für diese Angriffsart ist, wenn eine nicht autorisierte Person einer autorisierten Person physisch in einen eingeschränkten Unternehmensbereich oder ein IT-System folgt (Rouse, 2022). Eine bewährte Methode ist es, wenn ein Hacker einen Unternehmensmitarbeiter anspricht, damit dieser ihm eine Tür offen hält, da er z. B. angeblich seine ID-Karte (Beschäftigtenausweis) vergessen hat (Rouse, 2022). Laut den Volkswagen-AG-Richtlinien ist die Sicherung der ID-Karte (Arbeitsausweis) von großer Bedeutung, denn mit dieser Karte kann man sich nicht nur einen physischen Zugang ins Unternehmen verschaffen, sondern auch einen digitalen Zugriff auf die verschiedenen internen Systeme bekommen. Entsprechend wichtig ist die Sicherung der eigenen ID-Karte für die Volkswagen-Beschäftigten.

Das Thema Umgang mit Informationen bleibt jedoch entscheidend und beinhaltet in dieser Studie folgende Aspekte:

- Shoulder Surfing
- Umgang mit Informationen in sozialen Netzwerken
- Arbeitsausweis sichern

Das Thema Umgang mit Informationen wird in weiteren Kapiteln detaillierter präsentiert und diskutiert.

2.5.4 Umgang mit (mobilen) Speicher- und Endgeräten

Parsons et al. (2017) beschreiben folgende Aspekte des Umgangs mit Endgeräten, die relevant für die Informationssicherheits-Awareness sind: z. B. die physische Sicherheit der Endgeräte (hierzu zählt vor allem die Sicherheit der mobilen Endgeräte vor Diebstahl) oder das Senden vertraulicher oder geheimer Daten via ungesichertem WLAN.

Obwohl einige der oben genannten Aspekte nicht relevant für die Beschäftigten von Volkswagen sind (Sendung vertraulicher oder geheimer Daten via ungesichertem WLAN), sind andere wiederum von großer Bedeutung. Dazu gehören (vgl. Parsons et. al., 2017):

- Benutzung der privaten Endgeräte in Arbeitskontexten
- Benutzung von unbekannten USB-Sticks in Arbeitskontexten

Das Thema „Benutzung von Endgeräten“ wird auch im weiteren Verlauf dieser Arbeit noch von Bedeutung sein.

2.5.5 Zutritts- und Zugriffsschutz

Laut Nebel (2018) sind für IT-Sicherheitsverstöße die Leiter der jeweiligen Abteilung im Unternehmen verantwortlich, jedoch untersuchen Parsons et al. (2014) und Parsons et al. (2017) diesen Aspekt anders und heben hervor, dass das Bewusstsein der Beschäftigten gegenüber der Meldung von Vorfällen generell adressiert werden sollte. Informationssicherheitsvorfälle bewusst zu ignorieren, führt zu einem Unternehmensregelverstoß gegen Integrität und Compliance bei der Volkswagen AG. Es lassen sich folgende Hauptpunkte für diesen Aspekt der Informationssicherheit ableiten:

- Informationssicherheitsvorfälle ignorieren
- Informationssicherheitsvorfälle melden

Im weiteren Verlauf der Arbeit geht es darum, dass für diese Arbeit relevante Aspekte bezüglich der Verstöße und der Meldung von Verstößen gegen die Informationssicherheit detaillierter beschrieben und analysiert werden.

3 Qualitative Studie

Diese Studie verfolgt u. a. das Ziel, zu untersuchen, wie eine gruppenspezifische spielerische Lernmethode didaktisch zu konzipieren ist, welche Charakteristiken diese Methode haben soll und wie das Thema Informationssicherheit in den Kontext der spielerischen Lernmethode eingeordnet werden kann.

In diesem Kapitel wird das methodische Vorgehen präsentiert und analysiert. Zuerst werden die Methoden für die Spielentwicklung dargestellt und reflektiert. Dies erfolgt in zwei Schritten: Die Spielentwicklung soll nicht nur didaktisch aufgearbeitet werden (welche spielerischen Charakteristika sollen beinhaltet sein), sondern auch inhaltlich (welche Themen der Informationssicherheit sollen im Spiel vorhanden sein).

Zu Beginn jeder empirischen Arbeit wird entschieden, ob mit einer qualitativen oder quantitativen Erhebungsmethode geforscht wird. Mittels qualitativer Forschungsmethoden können Einzelfälle untersucht werden. Aus den daraus gewonnenen Forschungserkenntnissen lassen sich dann verallgemeinerbare Aussagen ableiten (Wolf, 2008, S. 21 f. nach Bortz & Döring, 2005, S. 295 f.; Brosius & Koschel, 2001, S. 18). Das geht mit dem Forschungsinteresse dieser Studie – aus den persönlichen Meinungen der Zielgruppe Erkenntnisse zur Entwicklung einer übergeordneten gruppenspezifischen Awareness-Maßnahme zu gewinnen – einher.

Vor der Spielentwicklung soll eine Zielgruppenanalyse erfolgen. Außerdem soll die Zielgruppe, die dieses Spiel spielen wird, an der Spielentwicklung teilnehmen (vgl. Ermi & Mäyrä, 2005). Für die Konzeptionierung des digitalen Spiels wurde eine qualitative Erhebungsmethodik ausgewählt, in deren Rahmen zwei Methoden zum Einsatz kommen: Gruppendiskussionen und Experteninterviews.

Da es beim Spieldesign um die Einstellungen einer großen Zielgruppe geht, wurde für die Konzeptionierung der didaktischen Rahmenbedingungen des Spiels die Gruppendiskussionsmethode ausgewählt. Für die theoretische Entwicklung des Spiels wurde hingegen die Experteninterviewmethode gewählt. Im Folgenden wird im ersten Schritt die Gruppendiskussion präsentiert und im zweiten Schritt erfolgen die Darstellung und die Analyse der Experteninterviews. Danach sollen die Ergebnisse der Untersuchung dargestellt und mit den anderen bei der Volkswagen AG eingesetzten Maßnahmen zur Messung bzw. Erhöhung der Sicherheits-Awareness (z. B. Unterweisung oder Security Arena) verglichen werden. Am Ende des Kapitels werden die beiden Methoden auf Limitationen überprüft und die Ergebnisse auf ihre Gültigkeit untersucht. Abschließend werden die Forschungsfragen bezüglich der spielerischen Lernmethode im Informationssicherheits-Awareness-Kontext beantwortet.

3.1 Gruppendiskussion – Definition, Prinzipien und Ablauf

Die Gruppendiskussion ist eine Methode der qualitativen Forschung und stellt einen Raum für ein Gespräch mehrerer Teilnehmer zu einem bestimmten Thema dar (Wagner & Schönhagen, 2009, S. 274 in Anlehnung an Lamnek, 1995). Somit können mithilfe von Gruppendiskussionen qualitative Daten gesammelt und im späteren Forschungsverlauf analysiert werden. Nach Kruse (2015, S. 193) ist das Gruppendiskussionsverfahren eine „eigenständige qualitative Erhebungsmethode rekonstruktiver Sozialforschung" und muss von der Interviewform der Einzelinterviews differenziert werden. Bei der Gruppendiskussion handelt es sich um „kollektive Orientierungsmuster" und der Analysekern liegt darauf, wie sich die Teilnehmer einer Gruppendiskussion innerhalb derselben positionieren und organisieren (Kruse, 2015, S. 186 f. in Anlehnung an Bohnsack, 2000, 2010). Jedoch gibt es verschiedene Dimensionen, anhand welcher eine Gruppendiskussion ausgestaltet werden kann, wie Diskussionsverfahren, Art der Diskussionsleitung, Art der Stimuli, Gruppenzusammensetzung etc. Welche davon genauer betrachtet und analysiert werden, ist von den jeweiligen Forschungszielen und Forschungsinteressen abhängig. Im Mittelpunkt dieses Forschungsvorhabens steht die Konzeptionierung eines gruppenspezifischen Spiels (Serious Game), deswegen sind die Meinungen und Einstellungen von einer bestimmten Gruppe von großem Interesse. Wie schon im Theoriekapitel (siehe Kapitel 1.1) beschrieben wurde, liegt der Fokus dieser Arbeit bei der Zielgruppe junger Erwachsene (18 bis 24 Jahre), die bei der Volkswagen AG beschäftigt sind, weshalb die Meinungen und Einstellungen dieser Zielgruppe vom besonderem Interesse für die Entwicklung einer gruppenspezifischen Lernmethode sind.

In den folgenden Unterkapiteln wird genauer auf die Gestaltung und Umsetzung der Gruppendiskussionen im Rahmen dieser Arbeit eingegangen. Es folgen eine Darstellung des Ablaufes der Gruppendiskussion, die Beschreibung der Auswertungsmethoden sowie ein Diskurs über die Ergebnisse und deren Interpretation. Daran schließt sich die Reflexion der Forschungsmethodik an.

3.1.1 Ablauf

Wagner und Schönhagen (2009, S. 295) schlagen folgenden Ablauf für die Durchführung einer Gruppendiskussion vor (Abb. 10):

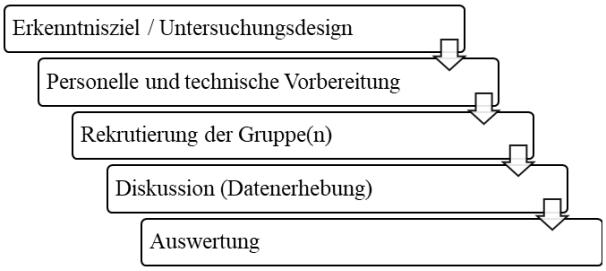


Abbildung 10: Das Verfahren einer Gruppendiskussion (eigene Darstellung in Anlehnung an Wagner & Schönhagen, 2009, S. 295)

Im ersten Schritt sollen das *Erkenntnisziel und Untersuchungsdesign festgelegt* werden.

Wie bei allen anderen wissenschaftlichen Methoden gilt auch bei der Gruppendiskussion, dass zu Anfang die Erkenntnisziele des Forschungsablaufs präzisiert werden müssen. Das gesamte Forschungsdesign und die weiteren Schritte wie die Auswahl der Gesprächsteilnehmer, die Anzahl der Gruppendiskussionen etc. müssen auf dieses Ziel hin orientiert sein (Wagner & Schönhagen, 2009, S. 292 f.). In diesem Schritt soll außerdem der Diskussionsleitfaden formuliert werden, um zu gewährleisten, dass alle wesentliche Aspekte während der Diskussion thematisiert werden.

Erst wenn der Diskussionsleitfaden formuliert ist, können weitere Schritte der Gruppendiskussion vorbereiten werden. Zur *personellen und technischen Vorbereitung* gehören die Wahl des Raums für die Gruppendiskussion, eine angemessene Zeitplanung für die Gruppendiskussion und die tatsächliche Vorbereitung der technischen Geräte (Videokamera, Mikrofone), falls solche gefordert werden.

Im Anschluss folgt *die Rekrutierung der Gruppe(n)*. In diesem Schritt wird entschieden, wie groß die Teilnehmergruppe sein soll. Viel zu kleine Gruppen führen dazu, dass einzelne „Meinungsführer" den Diskussionsprozess dominieren (Wagner & Schönhagen, 2009, S. 296). Daher empfehlen Wagner und Schönhagen (2009, S. 296 in Anlehnung an Lamnek, 1998, S. 101) eine ungerade Anzahl an Gruppendiskussionsteilnehmern, um eine Pattsituation zu vermeiden, wobei sie generell eine Gruppengröße zwischen 8 und 12 Teilnehmern als sinnig erachten. Laut Mayring (2002) könnte eine Gruppendiskussion auch ab 5 Personen durchgeführt werden, wobei die größte Teilnehmeranzahl 15 Personen nicht übersteigen sollte. Empfehlenswert ist, dass das Thema der Gruppendiskussion für die Gruppe eine gewisse Relevanz hat, denn ohne Interesse am Thema werden die Gruppendiskussionsmitglieder keine fruchtbare Diskussion führen können (Wagner & Schönhagen, 2009). Laut Wagner und Schönhagen (2009, S. 297 in Anlehnung an Lamnek, 1998, S. 96 ff.) sollen die Gruppen möglichst heterogen gestaltet sein, da durch die Einbindung von verschiedenen Meinungen kontroverser diskutiert wird.

Nachdem die Gruppediskussionsmitglieder rekrutiert wurden, soll im nächsten Schritt die tatsächliche *Datenerhebung* erfolgen.

In der Wissenschaft existiert folgendes Phasenmodell der Durchführung einer Gruppendiskussion (vgl. Wagner & Schönhagen, 2009, S. 295; Kruse, 2015, S. 201 f. in Anlehnung an Lamnek, 2005, S. 130 ff.)

1. Eröffnungsphase
   Hier soll die Vorstellung der Diskussionsleiter und der Teilnehmer erfolgen und eine kurze Einführung in das Forschungsvorhaben stattfinden. Außerdem empfiehlt Kruse (2015, S. 202) einen Hinweis auf Datenschutz und Anonymisierung der Daten, die erhoben werden.
2. Einstiegsphase
   In diesem Schritt soll der Grundreiz in Form eines Bild, eines Filmausschnitts oder einer Diskussionsaufforderung erfolgen.
3. Erhöhte Aktionsphase
   Ziel in dieser Phase ist ein selbstläufiger Diskurs zwischen den Diskussionsteilnehmern. Nichtdestotrotz soll eine non-direktive Gesprächsführung durch den erstellten Gruppendiskussionsleitfaden stattfinden. Kruse (2015, S. 202) empfiehlt, ggf. durch Konfrontationen, Provokationen etc. zu intervenieren.
4. Auslaufphase
   Falls die Gruppendiskussion nicht ergiebig genug ist, soll an dieser Stelle die Reaktivierung der Gruppendiskussion erfolgen. Die Abschlussmarkierung durch die Teilnehmer deutet den Schluss der Gruppendiskussion an. Diese endet mit einem an die Teilnehmer gerichteten Dank des Diskussionsleiters (Kruse, 2015).

Nachdem die tatsächliche Durchführung der Gruppendiskussion abgeschlossen ist, kann *die Auswertung* der Gruppendiskussion beginnen (Wagner & Schönhagen, 2009, S. 302). Die Auswertungsmethodik wird in Kapitel 3.1.3 detaillierter beschrieben. Zuvor wird noch der tatsächliche Ablauf der in dieser Arbeit durchgeführten Gruppendiskussionen näher beleuchtet.

Erkenntnisziel und Untersuchungsdesign

Die erste Forschungsfrage lautet: Welche Themen der Informationssicherheits-Awareness und welche spielerischen Charakteristiken sind im Rahmen eines Serious Games zu behandeln?

Für die Beantwortung des zweiten Teils der Forschungsfrage wurde entschieden, die Meinungen der Auszubildenden der Volkswagen AG im Rahmen von Gruppendiskussionen zu erfassen, da diese die Zielgruppe dieser Studie darstellen. Um eine große Datenmenge zu bekommen, wurden 3 Gruppendiskussionen mit einer Teilnehmeranzahl von je 5 Personen durchgeführt, damit insgesamt die Meinungen und Ansichten von 15 Personen gesammelt werden können.

Es wurden Fragestellungen für die Gruppendiskussion entwickelt, die das Ziel verfolgen, herauszufinden, welche Merkmale ein gruppenspezifisches Spiel hat. Da Serious Games verschiedene Genres haben können (Mostafa & Faragallah, 2019,

S. 169294), ist es sinnvoll, zu eruieren, welches Spielegenre die Zielgruppe dieser Studie am attraktivsten findet. Folglich wurde in der Gruppendiskussion nach der Einstiegsfrage erhoben, welche allgemeinen Präferenzen die Diskussionsteilnehmer bezüglich eines Computerspiels (Gruppendiskussionsfrage 1 und 2) haben und welche Spielgenres sie bevorzugen (Gruppendiskussionsfrage 3). Durch eine spielerische Identifikation des Spielers/Lerners mit der Spielfigur wird die Spielerfahrung generiert und gleichermaßen entsteht Lernmotivation (vgl. Blötz, Ballin & Gust, 2015, S. 27). Darüber hinaus scheint es von besonderem Interesse, herauszufinden, über welche Merkmale die Hauptfigur im Spiel verfügen sollen und welche Korrelation es zwischen dem Spieler und z. B. der Hauptfigur und anderen Figuren laut der Zielgruppe im Spiel geben soll. Mit der Gruppendiskussionsfrage 4 sollen die Meinungen der Gruppendiskussionsteilnehmer diesbezüglich eruiert werden. Um die Einstellungen der Gruppendiskussionsteilnehmer bezüglich weiterer möglicher gewünschter Merkmale eines Computerspiels abzufragen, wurde die Gruppendiskussionsfrage 5 entwickelt und den Teilnehmern gestellt. Tabelle 1 präsentiert die Fragen, die in der Gruppendiskussion besprochen wurden.

Tabelle 1: Fragestellungen in der Gruppendiskussion

Nr.	Frage
1	Wenn Sie an das interessanteste und coolste digitale Spiel überhaupt denken, wie ist das Spiel ausgestaltet? Können Sie dafür Beispiele benennen?
2	Was macht ein digitales Spiel uninteressant für Sie?
3	Welche Genres im Spiel mögen Sie? Warum?
4	Was ist bezüglich der Hauptfigur und der anderen Spielfiguren für Sie wichtig? Warum?
5	Wenn Sie ein Spiel stundenlang spielen würden – welche Merkmale soll das Spiel haben?

Personelle und technische Vorbereitung

Die tatsächliche Durchführung der Gruppendiskussionen erfolgte im Werk der Volkswagen AG. Sie fand am 25.06.2019 (zwei Gruppendiskussionen) und am 03.07.2019 (eine Gruppendiskussion) statt. Die technische Vorbereitung inkludierte den Gruppendiskussionsleitfaden, einen Video-Beamer für die Präsentation eines Einstiegsvideos und ein Tonaufnahmegerät für die Gruppendiskussionsaufnahmen, damit die Daten dann später transkribiert und ausgewertet werden können.

Die Rekrutierung der Gruppe(n)

Für diese Forschungsarbeit war es von großer Bedeutung, eine möglichst heterogene Gruppe für die Gruppendiskussionen auszuwählen und zu befragen, da das zu konzipierende Serious Game perspektivisch nicht nur für die Marke Volkswagen Personenkraftwagen (PKW) zur Sensibilisierung der Beschäftigten dienen soll, sondern auch für die anderen Marken der Volkswagen AG zur Verfügung stehen soll. Insgesamt haben an drei Gruppendiskussionen 15 Teilnehmer (TN) teilgenommen. Um ein mög-

lichst hohes Maß an Heterogenität in einer im Alltag bestehenden Zielgruppe zu gewährleisten, wurden Auszubildende der Volkswagen AG als Zielgruppe ausgewählt, da sich die Probanden regelmäßig innerhalb eines gemeinsamen Umfelds bewegen und sich ihre beruflichen Hintergründe basierend auf ihrem Ausbildungsberuf unterscheiden. Die Gruppen bestehen in den gewählten Konstellationen teilweise im Alltag (z. B. bei Lehrgängen). Die Teilnehmer kennen sich und haben mitunter bereits in anderen Kontexten zusammengearbeitet. Eine Übersicht dazu, in welchem Ausbildungsjahr sich die Probanden befinden, welchen Beruf sie erlernen und welchem Geschlecht (männlich (m); weiblich (w); divers (d)) sie angehören, ist aus den Tabellen 2, 3 und 4 ersichtlich.

Tabelle 2: Zusammensetzung der ersten Gruppendiskussion

Gruppendiskussion 1		
TN-Nummer/Geschlecht	**Ausbildungsjahr**	**Beruf**
TN 1/m	1	Werkzeugmechaniker
TN 2/m	1	Werkzeugmechaniker
TN 3/w	2	Industriekauffrau
TN 4/m	3	Werkzeugmechaniker
TN 5/m	2	Fachinformatiker in Anwendungsentwicklung

Tabelle 3: Zusammensetzung der zweiten Gruppendiskussion

Gruppendiskussion 2		
TN-Nummer/Geschlecht	**Ausbildungsjahr**	**Beruf**
TN 1/m	2	Technischer Produktionsdesigner
TN 2/m	2	Werkzeugmechaniker
TN 3/m	2	Technischer Produktionsdesigner
TN 4/w	2	Industriekauffrau
TN 5/w	2	Industriekauffrau

Tabelle 4: Zusammensetzung der dritten Gruppendiskussion

Gruppendiskussion 3		
TN-Nummer/Geschlecht	**Ausbildungsjahr**	**Beruf**
TN 1/m	2	Fachinformatiker in Anwendungsentwicklung
TN 2/m	1	Werkzeugmechaniker

(Fortsetzung Tabelle 4)

Gruppendiskussion 3		
TN-Nummer/Geschlecht	**Ausbildungsjahr**	**Beruf**
TN 3/w	2	Industriekauffrau
TN 4/w	1	Industriekauffrau
TN 5/w	2	Industriekauffrau

Es wurde gewährleistet, dass die Gruppendiskussionsteilnehmer ein gewisses Interesse an dem Thema haben, denn zwei Wochen vor der geplanten Gruppendiskussionen wurde ein Einladungsschreiben durch die Ausbilder rausgeschickt. Die Gruppendiskussionsteilnehmer konnten sich dann entsprechend bei Interesse melden.

Datenerhebung

Zuerst hat sich die Gruppendiskussionsleiterin in der Eröffnungsphase vorgestellt, das Forschungsvorhaben präsentiert und einen Hinweis auf Datenschutz und Anonymisierung der zu erhebenden Daten gegeben. Als Grundreiz für die im Rahmen dieser Arbeit durchgeführten Gruppendiskussionen diente die Darstellung der Problematik der Informationssicherheits-Awareness und der fehlenden bzw. nicht ausreichenden Sensibilisierung der Volkwagen-Beschäftigten bezüglich dieses Themas. Am Anfang der Einstiegsphase wurde ein provokatives Video zum Thema Social Engineering gezeigt. Danach wurde das Dissertationsvorhaben erläutert und angedeutet, dass ein neues Lernformat zusammen mit den Probanden konzipiert und später in Form einer Serious-Game-Entwicklung umgesetzt werden soll. Nach dem Video wurde die erste Frage der Gruppendiskussion gestellt (siehe Tabelle 1).

Im Anschluss an die Darbietung des Grundreizes folgte die freie Diskussion bezüglich des gestellten Themas. Nach weniger Zeit hatten die Gruppendiskussionen eine erhöhte Aktionsphase erreicht, während die Gruppendiskussionsleiterin nondirektiv die Gruppendiskussion geleitet hat, um zu gewährleisten, dass die geforderten Elemente der Konzeption Bestandteil der Diskussion waren und keine Aspekte vernachlässigt wurden. Als Stimuli wurden die schon dargestellten Fragen der Gruppendiskussion implementiert, in deren Anschluss jeweils die freie Gruppendiskussion stattfand.

Nachdem die Abschlussmarkierung der Gruppendiskussion durch die Teilnehmer erfolgt war, kam die Gruppendiskussion in die Auslaufphase.

Nach der Gruppendiskussion wurde eine Feedbackrunde zum Thema der Gruppendiskussion mit den Teilnehmern durchgeführt. Anschließend sollte eine Einschätzung von den Teilnehmern getroffen werden, wie sie die Gruppendiskussion generell als eine Methode zur Spielentwicklung wahrgenommen haben.

Nachdem die Gruppendiskussionen durchgeführt und die Daten erhoben wurden, kann *die Auswertung* der Daten beginnen. Diese stellt nach Wagner und Schönha-

gen (2009, S. 302) den aufwendigsten Schritt der Forschungsarbeit dar und soll im Folgenden detaillierter beschrieben werden.

3.1.2 Auswertungsmethodik

In diesem Unterkapitel werden die Methodik der Transkription als Vorbereitung für die Auswertung von verbalem Datenmaterial sowie die qualitative Inhaltsanalyse als angewandte Auswertungsmethode vorgestellt.

Für die Auswertung des im Rahmen dieser Arbeit erhobenen Datenmaterials wird die Methode der qualitativen Inhaltsanalyse nach Mayring (2015) angewandt. Hierbei werden die Textbestandteile durch Analyseschritte und Analyseregeln systematisch und überprüfbar interpretiert (Mayring, 2015, S. 51). Zunächst werden die Grundsätze und die Prinzipien der qualitativen Inhaltsanalyse erörtert, daraufhin werden einzelne Schritte und die Technik der ausgewählten Analyse beschrieben. Insgesamt beschreibt Mayring (2015, S. 12 f.) sechs Merkmale der Inhaltsanalyse.

1. Gegenstand der Inhaltsanalyse ist Kommunikation und eine der Aufgaben ist es, Kommunikation zu analysieren (Mayring, 2015, S. 13). An dieser Stelle muss besonders betont werden, dass es sich bei Kommunikation zwar primär um Sprache handelt, aber auch Bilder oder Musik als Gegenstand fungieren können (Mayring, 2015 in Anlehnung an Berelson, 1952, S. 13). Das in der Gruppendiskussion gezeigte Video zum Thema Social Engineering diente allerdings ausschließlich als Anregung zu Gruppendiskussion und gehört somit nicht zu den auszuwertenden Materialien.
2. Die Kommunikation soll in irgendeiner Form fixiert oder protokoliert werden, somit ist die Aufgabe, fixierte Kommunikation zu analysieren, ein weiteres Merkmal der qualitativen Inhaltsanalyse (Mayring, 2015, S. 12). In der vorliegenden Arbeit sind die drei transkribierten Gruppendiskussionen das zu analysierende Material.
3. Das systematische Vorgehen der Inhaltsanalyse grenzt sich gegen das hermeneutische Verfahren und dessen freie Interpretation des zu analysierenden Materials ab (Mayring, 2015, S. 12). Dies bedeutet, dass sich Inhaltsanalytiker für einen systematischen Weg entscheiden und nicht für eine impressionistische Ausdeutung des zu analysierenden Materials (Mayring, 2015, S. 12).
4. Das systematische Vorgehen der Inhaltsanalyse lässt sich besonders anhand der Regelgeleitetheit zeigen, da andere die Analyse hierdurch nachvollziehen und überprüfen können (Mayring, 2015, S. 13).
5. Das systematische Vorgehen stellt sich auch durch Theoriegeleitetheit dar, was auch Ergebnisse anderer Wissenschaftler mit dem zu untersuchenden Material verknüpft. In dieser Arbeit werden der empirische Teil und dessen Ergebnisse mit dem theoretischen Teil verglichen.
6. Die Inhaltsanalyse hat auch das Ziel, das zu analysierende Material als Teil des Kommunikationsprozesses zu betrachten und Rückschlüsse auf bestimmte Aspekte der Kommunikation zu ziehen (Mayring, 2015, S. 13).

Die Qualität der Ergebnisse und deren Mehrwert werden zusammen mit der abschließenden Diskussion im Abschlusskapitel präsentiert und analysiert.

Darüber hinaus gibt es sechs allgemeine Gütekriterien, die für die qualitative Forschung entwickelt wurden (Mayring, 2002, S. 144 f. in Anlehnung u. a. an Kirk & Miller, 1986; Flick, 1987):

1. Verfahrensdokumentation
   Da in der qualitativen Forschung die Forschungstechniken und Messinstrumente standardisiert sind, reicht es in der Regel, eine detaillierte Dokumentation über die verwendeten Techniken und Messinstrumente zu notieren, um dieses Kriterium zu erfüllen (Mayring, 2002). Die Auswertungsmethode dieser Arbeit wird in den folgenden Kapiteln ausführlich erklärt und analysiert.
2. Interpretationsabsicherung
   Interpretationen sollen argumentativ begründet werden (Mayring, 2002). Dazu gibt es einige wichtige Aspekte, die beachtet werden sollen. Das Vorverständnis der jeweiligen Interpretation soll angemessen sowie schlüssig sein und „[...] dort, wo Brüche sind, sollen sie geklärt werden" (Mayring, 2002, S. 145 in Anlehnung an Hirsch, 1967). Es ist auch sehr wichtig, nach Alternativinterpretationen zu suchen und diese zu analysieren (Mayring, 2002).
3. Regelgeleitetheit
   Es darf nicht nach einem unsystematischen Vorgehen geforscht werden, sondern es sollen bestimmte Verfahrensregeln eingehalten werden (Mayring, 2002). Darüber hinaus ist zuerst eine Voranalyse durchzuführen, gefolgt von der Unterteilung des ganzen Materials in Einheiten. Die Schritte der Auswertung der Gruppendiskussionen werden in den weiteren Kapiteln erklärt.
4. Nähe zum Gegenstand
   Es ist sehr wichtig, dass „[...] man möglichst nahe an der Alltagswelt der beforschten Subjekte anknüpft" (Mayring, 2002, S. 146). Das heißt, es soll nicht im Labor geforscht werden, sondern in der realen Welt. Eine der wichtigsten Aufgaben der qualitativen Forschung ist es, konkrete soziale Probleme zu analysieren, ein offenes, gleichberechtigtes Verhältnis zwischen dem Forscher und den Gruppendiskussionsteilnehmern herzustellen und die Interessenübereinstimmung mit den Gruppendiskussionsteilnehmern zu erreichen (Mayring, 2002). Die Interessenübereinstimmung ermöglicht eine größtmögliche Nähe zum Gegenstand.
5. Kommunikative Validierung
   Der Forscher nimmt den Dialog mit den Beforschten auf, um ihre Ideen und Meinungen zu analysieren. Daher soll auch die Interpretation an die subjektiven Bedeutungsstrukturen der Interviewpartner geknüpft werden (Mayring, 2002). Unter der kommunikativen Validierung ist gemeint, dass die Interpretationen durch die Diskussionen mit den Beforschten überprüft werden können (Mayring, 2002).
6. Triangulation
   Das Ziel der Triangulation ist, verschiedene Lösungswege zu finden, um die Ergebnisse zu vergleichen. Auch die verschiedenen Perspektiven, Stärken und Schwächen der Analysemethode sowie qualitative und quantitative Forschungsmethoden können verglichen werden (Mayring, 2002).

3.1.3 Analyseschritte

Die Analyseschritte der qualitativen Inhaltsanalyse nach Mayring (2015) werden zur Analyse der Ergebnisse dieser Arbeit angewandt. Jene sind in der folgenden Abbildung beschrieben (siehe Abb. 11).

Im Folgenden werden die einzelnen Analyseschritte nach Mayring (2015, S. 54 f.) und deren Ausführung im Rahmen dieser Studie näher beleuchtet.

Festlegung des Materials

Mayring (2015) betont, dass zunächst definiert werden muss, welches Material analysiert wird, und dass dieser „Corpus" nur unter begründbaren Notwendigkeiten verändert werden sollte. Mayring (2015 in Anlehnung an Friedrichs, 1973; Lisch, 1978) schlägt einige Regeln zur Festlegung der Analyse vor, um die sogenannte Stichprobenziehungsproblematik zu vermeiden, die bei der Festlegung des Materials in den Vordergrund treten kann.

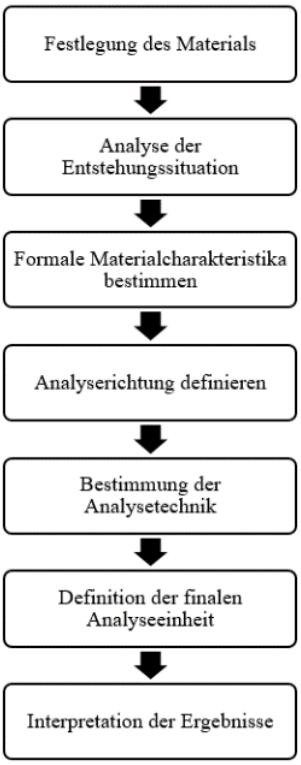


Abbildung 11: Analyseschritte der qualitativen Inhaltsanalyse nach Mayring (2015, S. 54 f.)

Zunächst muss eine klare Definition der Grundgesamtheit der Analyse vorliegen. Des Weiteren soll die Festlegung des Stichprobenumfangs der Analyse nur nach Repräsentativitätsüberlegungen und ökonomischen Erwägungen durchgeführt werden. Ferner

soll die Stichprobe der Analyse nach einem bestimmten Modell vorgenommen werden (z. B. reine Zufallsauswahl, Auswahl nach vorher festgelegten Kriterien etc.).

Der „Corpus" der zu analysierenden Gruppendiskussionen für diese Studie besteht aus den drei transkribierten Gruppendiskussionen, die im Folgenden näher beschrieben werden.

Analyse der Entstehungssituation

Nach Mayring (2015, S. 55) soll im Analyseschritt „Analyse der Entstehungssituation" beschrieben werden, von wem und unter welchen Bedingungen das Material produziert wurde. Im Rahmen der vorliegenden Arbeit ist der Faktor „Zielgruppe" entscheidend bzw. die an der Entstehungssituation beteiligten Mitarbeiter sind wichtig. Weitere von Mayring (2015, S. 55) genannte Aspekte wie z. B. der kognitive oder emotionale Handlungshintergrund des Verfassers oder der soziokulturelle Hintergrund sind für diese Arbeit nicht von Interesse, denn im Vordergrund der Arbeit stehen die persönlichen Meinungen der Gruppendiskussionsteilnehmer.

Ferner spielt der Kontext der vorliegenden Arbeit für die qualitative Inhaltsanalyse eine wichtige Rolle. Das Material wurde durch Gruppendiskussionen erhoben. Die Teilnahme daran war für die Teilnehmer freiwillig und die Durchführung der empirischen Erhebungen war seitens des Unternehmens genehmigt. Die Daten der Gruppendiskussionspartner wurden vertraulich behandelt. Die Teilnehmer wurden vor den Gruppendiskussionen über die Forschungsfrage und das Forschungsziel informiert. Die Zielgruppe der Gruppendiskussionen besteht aus 15 internen Mitarbeitern (Auszubildenden) der Volkswagen AG, die sich für das Konzept „Serious Games" interessierten und an einer didaktischen Konzeptionierung eines Serious Games teilnehmen wollten.

Formale Materialcharakteristika

Nach Mayring (2015, S. 55) muss im Schritt „Formale Materialcharakteristika" veranschaulicht werden, in welcher Form das zu analysierende Material vorliegt. Er hebt hervor, dass die Grundlage der Inhaltsanalyse der niedergeschriebene Text ist. Die gesprochene Sprache wird üblicherweise auf Tonband aufgenommen und später transkribiert. Ergänzend dazu werden bei Interviews oder Gruppendiskussionen oft Beobachtungen in das Protokoll aufgenommen (Mayring, 2015).

Das Material dieser Arbeit besteht aus den Ergebnissen der Gruppendiskussionen. Die angewendeten Transkriptionsregeln stützen sich auf Kruses (2015) fünf moderate Grundregeln der Transkription: Alles, was gehört wurde, muss weitgehend genauso verschriftet sein. Ergänzend dazu erklärt Kruse, dass „[…] die konkreten Versprachlichungen nicht in die Formen der Standard- oder Schriftsprache transformiert werden sollen" (Kruse, 2015, S. 351). Der Autor ergänzt dazu, dass umgangssprachliche und dialektische Ausdrücke sowie „berühmt-berüchtigte", „ähs" und „hms" ebenfalls transkribiert sein sollen. Er hebt zudem hervor, dass diese Regel auch für grammatikalisch „falsche" Konstruktionen gilt, heißt, dass diese nicht korrigiert werden sollen. Betonungen und Pausen sind konsekutiv für die Transkription, weitere prosodische Merkmale sollen

jedoch nur dann benutzt werden, wenn es für die Interpretation wichtig erscheint (Kruse, 2015).

Für diese Arbeit wurde teilweise das von Kruse (2015, S. 354 f.) entwickelte System zur Transkription übernommen (siehe Tabelle 5):

Tabelle 5: Transkriptionssystem (basierend auf Kruse, 2015, S. 354 f.)

Prosodische Merkmale	Erklärung
(1) (2) (3)	Pause mit Sekundenlänge
[ahja] [mhm]	Redewendungen innerhalb des Kommunikationsbeitrags
{gleichzeitig}	Gleichzeitige Rede
Iv:	Interviewer
TN1, TN2, TN3...	Teilnehmer 1, Teilnehmer 2, Teilnehmer 3
?	Steigende Endintonation (Frage)
.	Fallende Endintonation
<lacht>, <hustet>	Außersprachliche Handlungen
[Name], [Beruf]	Anonymisierung
(unv)	Unverständlich

Ergänzend dazu betont Kruse (2015), dass auf einem immer feineren Niveau transkribiert werden soll, wenn sprachlich-kommunikative Auffälligkeiten auftreten. Da ein Transkript eine niedergeschriebene Wiedergabe des Gesagten skizziert und kein reales Gespräch abbildet, soll es nicht durch unnötige und/oder gefälschte Notationen verkompliziert werden, wie z. B. durch die Beschreibung der Emotionen der Teilnehmer beim Gespräch, der allgemeinen Atmosphäre im Raum etc. (Kruse, 2015). Außersprachliche oder sprachliche Handlungen, wie z. B. „der Interviewte lacht" oder „der Interviewte erzählt lachend", sollen zwar transkribiert, jedoch nicht vorinterpretiert werden (beispielsweise im Sinne von: „der Interviewte lacht bösartig"). Bei Pausen im Erzähl- bzw. Gesprächsverlauf, die kürzer als eine Sekunde sind, ist fraglich, ob diese tatsächlich transkribiert werden sollen. Oft wird darauf verzichtet. Anders ist das hingegen bei Pausen, die länger als eine Sekunde dauern, da es einen wesentlichen Unterschied macht, ob eine Pausenlänge fünf Sekunden oder zehn Sekunden beträgt (Kruse, 2015). Daher sind in dieser Arbeit nur die Pausen transkribiert worden, die eine Sekunde und länger dauern. Der Diskussionsverlauf muss zudem so klar wie möglich transkribiert werden (Kruse, 2015).

Analyserichtung

Nach Mayring (2015, S. 58) kann man die Analyse des Materials in verschiedene Richtungen gestalten: in Bezug auf die Beschreibung des Gegenstandes, des Textverfassers oder aber der Wirkung des Materials auf die Zielgruppe. Mayring (2015) stützt sich

hier auf Lagerberg (1975) und betrachtet den Text in seinem Kommunikationsmodell als Teil einer Kommunikationskette. Das Ausgangsmaterial entstand wie beschrieben aus den drei Gruppendiskussionen mit 15 Volkswagen-Auszubildenden verschiedener Berufe, die sich für konzeptionelle Spielentwicklung zum Thema Informationssicherheit interessieren. Beispielsweise ihr Wissenshintergrund, ihre Erwartungen, Einstellungen, Intentionen und Pläne sowie die bisherigen auf den Gegenstand bezogenen Handlungen werden analysiert (vgl. Mayring, 2015).

In diesem Schritt der inhaltlichen Analyse unterscheidet Mayring (2015) zwei Merkmale der theoretischen Differenzierung der Fragestellung: die Regelgeleitetheit und die Theoriegeleitetheit der Analyserichtung. Darauf basierend folgt die Analyse einer „[...] präzisen theoretisch begründeten inhaltlichen Fragestellung" (Mayring, 2015, S. 59). Die Fragestellung der Analyse muss an die bisherige Forschung über den Gegenstand angebunden werden und ergänzend dazu muss die Analyse vorab genau bestimmt und in Subfragestellungen differenziert werden.

Bestimmung der Analysetechnik

Laut Kruse (2015, S. 398) ist die Inhaltsanalyse in der Sozialforschung die am häufigsten angewendete Analysemethode. Jedoch muss unterschieden werden, an welche Art der Inhaltsanalyse die Anlehnung erfolgt, denn drei Grobformen (Zusammenfassung, Explikation und Strukturierung) des Inhaltsanalyseverfahrens haben sich insgesamt etabliert (Kruse, 2015). Die Analysetechnik soll in Bezug auf das Material und die Forschungsfrage ausgewählt werden (Mayring, 2015). Bei dieser Studie handelt es sich um eine zusammenfassende Inhaltanalyse. Die zusammenfassende Inhaltsanalyse ermöglicht es, durch die Abstraktionen Kategorien zu bilden, die das Material beschreiben (Kruse, 2015).

Für diese Studie wird eine induktive Vorgehensweise ausgewählt. Dabei werden die Kategorien direkt aus dem Material abgeleitet, ohne sich vorab auf formulierte Theoriekonzepte zu beziehen. Mayring (2015) schreibt, dass die induktive Vorgehensweise eine große Bedeutung innerhalb qualitativer Ansätze hat, denn sie strebt nach einer möglichst naturalistischen, gegenstandsnahen Abbildung des zu analysierenden Materials, ohne Verzerrungen durch Vorannahmen des Forschers (Mayring, 2015).

Mayring (2015) beschreibt folgende Schritte der induktiven Kategorienbildung: Zuerst soll ein Selektionskriterium oder ein Thema der Kategorienbildung eingeführt werden. Nach dieser Festlegung wird das Material Zeile für Zeile durchgearbeitet. Mayring (2015, S. 87) führt an, dass die Kategorien möglichst nahe an dieser Festlegung gebildet werden sollen, wenn das erste Mal das Selektionskriterium erfüllt ist. Beim nächsten Mal, wenn das Selektionskriterium erfüllt ist, wird entschieden, ob die Textstelle unter die bereits gebildeten Kategorien fällt oder eine neue Kategorie gebildet werden soll. Zusätzlich sollen auch Codierregeln für die konkreten Kategorien und die Ankerbeispiele entwickelt werden. Wenn etwa die Hälfte des Materials auf diese Art bearbeitet wurde, ist es Zeit für eine Revision des Kategoriensystems, das bedeutet, es muss überprüft werden, ob die Kategorien immer noch dem Ziel der Analyse entsprechen. Sollten sich Veränderungen ergeben, muss das Material erneut von vorne

analysiert werden, ansonsten wird es weiter analysiert, allerdings müssen dann eventuell im weiteren Verlauf neue Kategorien gebildet werden (Mayring, 2015).

Das Grundprinzip der zusammenfassenden Inhaltsanalyse ist, die „Abstraktionsebene der Zusammenfassung" genau festzulegen (Mayring, 2015, S. 69). Die Abstraktionsebene wird schrittweise verallgemeinert, was dazu führt, dass die Zusammenfassung immer abstrakter wird (Mayring, 2015, S. 69). Im ersten Schritt werden die einzelnen Codiereinheiten in eine knappe, nur auf den Inhalt beschränkte Form umgeschrieben (Paraphrasierung), danach erfolgt erst eine Generalisierung auf das Abstraktionsniveau und schließlich eine Reduktion (Mayring, 2015, S. 72).

Am Ende der Analyse ergibt sich daraus ein Kategoriensystem, das im Sinne der Fragestellung interpretiert werden kann.

Definition der finalen Analyseeinheiten und Ergebnisdarstellung

Die genaue Durchführung der Schritte der induktiven Kategorienbildung ist im Anhang zu finden (s. Anhang 1.4 Auswertung der Gruppendiskussionen). In diesem Kapitel wird das finale Kategoriensystem dargestellt und diskutiert. Die finale Version des Kategoriensystems beinhaltet folgende Kategorien:

Kategorie I	Transparenter Spielanfang als kurzes Video
Kategorie II	Aufgabenvielfalt fördert Interesse
Kategorie III	Dynamische und unvorhersehbare Spielentwicklung ist interessefördernd
Kategorie IV	Entscheidungsmöglichkeiten im Spiel sind motivierend
Kategorie V	Offene Spielwelten mit gewissen Spielregeln sind interessefördernd
Kategorie VI	Realitätsnahe Spiele werden bevorzugt
Kategorie VII	Realitätsnahe Grafik wird bevorzugt
Kategorie VIII	Transparentes Belohnungssystem
Kategorie IX	Das Spiel soll verschiedene Genres inkludieren
Kategorie X	Quiz als Spielgenre
Kategorie XI	Ziele im Spiel sollen transparent sein
Kategorie XII	Multiplayer-Spiele sind interessefördernd
Kategorie XIII	Gegner im Spiel motiviert
Kategorie XIV	Hintergrundgeschichte fördert Interesse
Kategorie XV	Wenige Avatar-Auswahloptionen werden bevorzugt
Kategorie XVI	Selbstidentifikation mit Avatar ist wichtig
Kategorie XVII	Zeitdruck motiviert
Kategorie XVIII	Möglichkeit, untypische Rollen auszuprobieren
Kategorie XIX	Spannendes Spielende

Das gesamte Gruppendiskussionsmaterial wurde den induktiv gebildeten Kategorien zugeordnet. Die induktive Kategorienbildung entwickelt die Kategorien aus dem Material und leitet diese aus einem „Verallgemeinerungsprozess" ab, ohne sie davor auf die vorab formulierten Theorien zu stützen (Mayring, 2015, S. 85).

Im anschließenden Kapitel wird die Erhebungsmethode „Experteninterview“ (vgl. Meuser & Nagel, 2009; Kruse, 2015) präsentiert und diskutiert. Danach werden der Datenerhebungsprozess, die Auswertungsmethode und die Ergebnisse der Experteninterviews veranschaulicht.

3.2 Experteninterviews – Definition, Prinzipien und Ablauf

Wie schon erwähnt wurde, soll parallel zur Entwicklung der didaktischen Rahmenbedingungen auch das inhaltliche Thema des Spiels ausgearbeitet werden. Dafür wurde die Erhebungsmethode Experteninterview nach Meuser & Nagel (2009) und Kruse (2015) ausgewählt.

Nach Kruse (2015) ist ein Experteninterview keine eigene Interviewform, sondern eine Variante des Leitfadeninterviews. Das besondere Merkmal des Experteninterviews und der Unterschied zu einem offenen, narrativ orientierten Interview liegt darin, dass der Fokus dieser Form des Interviews nicht im methodischen Vorgehen liegt, sondern in seiner Zielgruppe, sprich beim Experteninterview werden nicht absichtlich verschiedene Erzählstrategien eingesetzt, um eine bestimmte Textsorte, nämlich die Narration, zu generieren (Kruse, 2015). Im Mittelpunkt des Experteninterviews stehen Experten nicht als „Personen“, sondern als Repräsentanten für die Meinungen oder Sichtweisen bestimmter Expertenzielgruppen bzw. eines fachlichen Feldes (Kruse, 2015, S. 166 in Anlehnung an Gläser & Laudel, 2004). Es gibt drei verschiedene Formen der Experteninterviews: exploratives Experteninterview, systematisierendes Experteninterview und theoriegenerierendes Experteninterview (Kruse, 2015 S. 167 in Anlehnung an Bogner & Menz, 2005). Für dieses Dissertationsvorhaben wurde das explorative Experteninterview ausgewählt (Kruse, 2015, S. 167 in Anlehnung an Bogner & Menz, 2005, S. 36 ff.). Kruse (2015) beschreibt, dass explorative Experteninterviews in der Feldsondierungsphase zu Wissensdimensionen eingesetzt werden, die noch kaum aufgearbeitet oder dokumentiert sind. Das Thema Social Engineering wurde bis jetzt im deutschsprachigen Raum in Bezug auf die Entwicklung spielerischer Awareness-Maßnahmen kaum erforscht, deswegen ist diese Form der Experteninterviews für das Dissertationsvorhaben relevant. Um diese Form des Experteninterviews besser zu beschreiben, stellt Kruse (2015, S. 167 in Anlehnung an Bogner & Menz, 2005, S. 36 ff.) folgende Experteninterviewaspekte vor:

- Die Informationen werden explorativ generiert.
- Die Interviewleitfäden dienen als Rahmenbedingungen eines Interviews.
- Diese Form des Experteninterviews ist sehr monologisch. Jedoch erlaubt sie dialogische Sequenzen, wenn Wissensthemen angesprochen, jedoch nicht ausgeführt werden.
- Der Experte setzt Themenschwerpunkte im Gespräch.

Wie beschrieben, liegt der Fokus beim Experteninterview auf den interviewten Experten. Wer gilt jedoch als Experte? Nach Kruse (2015, S. 173 in Anlehnung an Bogner &

Menz, 2005, S. 41) gilt als Experte ein Funktionsträger, der zur Funktionselite gehört und über ein Sonderwissen verfügt. Dieses Sonderwissen unterscheidet sich in zwei Formen: Zum einen gibt es *das Betriebswissen* (ein Prozesswissen, das „ein selbst reflektiertes Wissen und Kontextwissen" darstellt) und zum anderen *das Kontextwissen* (ein „gutachtliches Wissen über das Handlungsfeld") (Kruse, 2015, S. 174 nach Meuser & Nagel, 2005, S. 75 f.).

Im Rahmen dieser Arbeit wurden ergänzend zu den Gruppendiskussionen drei Experteninterviews durchgeführt. Experten waren interne Beschäftigte der Volkswagen AG, die durch ihre Arbeit in der Abteilung Informationssicherheit über einen bestimmten Wissensstand zum Thema Social Engineering verfügen.

Als nächster Schritt erfolgen die Transkription der Experteninterviews und die Auswertung nach Meuser & Nagel (2009). In den folgenden Unterkapiteln wird genauer auf die Gestaltung und Umsetzung der Experteninterviews im Rahmen dieser Arbeit eingegangen. Es folgen eine Darstellung der Leitfadenentwicklung, die Auswahl der Teilnehmer, die Beschreibung der Auswertungsmethode, die Festlegung des zu analysierenden Materials und die Analyse der Entstehungssituation. Im Anschluss werden die formalen Materialcharakteristika festgelegt, die Analyserichtung bestimmt und die Ergebnisse dargestellt sowie die Forschungsmethode reflektiert.

3.2.1 Ablauf

Nachfolgend sollen die Schritte der Durchführung von Experteninterviews präsentiert und ausdiskutiert werden.

Leitfadenfragenentwicklung

Wie in der Einleitung zu dieser Studie schon erwähnt wurde, benutzen Social Engineers verschiedene Techniken, um entsprechende Angriffe durchzuführen. Aus der Literaturrecherche ergibt sich, dass Social Engineers dabei nicht nur technische Möglichkeiten benutzen (wie z. B. Vishing/Phishing), sondern oft auch auf psychologische Manipulationsmethoden (wie z. B. Identitätsfälschung etc.) zurückgreifen, um erfolgreich ihre Ziele zu erreichen. Es ist jedoch unklar, ob es eine Tendenz für eine bestimmte Art von Social Engineering-Angriffen explizit innerhalb der Automobilindustrie gibt und ob und wie sich diese weiterentwickelt. Daher ist es entscheidend, herauszufinden, welche Techniken laut den Experten wichtig sind und wie sich diese in den nächsten Jahren entwickeln werden, daraus ergeben sich die Experteninterviewfragen 1 und 2, mit denen nach den wichtigsten Techniken des Social Engineerings und deren weiterer Entwicklung gefragt wird.

Da Social Engineers nicht nur private Personen, sondern auch Unternehmen attackieren (s. Kapitel 1 und 2.5), ist es bedeutsam, sowohl die Meinungen der Experten in Bezug auf private Schutzmaßnahmen als auch zu Schutzmaßnahmen von Unternehmen gegen Social Engineering-Angriffe zu eruieren. Aus diesem Grund ergeben sich die Fragen 3 und 4, die die Expertenmeinungen zur Rolle des Social Engineerings in Bezug auf Unternehmen und mögliche Schutzmaßnahmen ermitteln. Darüber hinaus ist es von besonderem Interesse, die Experten zu befragen, ob sie schon mal

einen Social-Engineering-Angriff erlebt oder gestaltet haben. Deswegen wurde die Leitfadenfrage 5 entwickelt, die sich mit den Expertenerfahrungen diesbezüglich befasst. Da alle Experten in der Automobilindustrie im Bereich der Informationssicherheit beschäftigt sind, ist es von großer Bedeutung, deren Ansichten zur Social-Engineering-Awareness-Förderung explizit in diesem Bereich zu erforschen. Die letzte Frage des Experteninterviewleitfadens fokussiert sich entsprechend auf dieses Thema. Für die inhaltliche Spielentwicklung wurden schließlich die folgenden Leitfadenfragen ausgewählt (siehe Tabelle 6):

Tabelle 6: Leitfadenfragen für die Experteninterviews

Nr.	Frage
1	Was sind Ihrer Meinung nach die wichtigsten Techniken, die Social Engineers anwenden? Warum?
2	Wie sieht Social Engineering in fünf Jahren aus? Welche Techniken werden wichtiger und warum?
3	Welche Rolle spielt Social Engineering in Bezug auf Unternehmen?
4	Wie kann ein durchschnittlicher User es vermeiden, Opfer von Social Engineering (privat und im Arbeitsleben) zu werden?
5	Haben Sie jemals einen Social-Engineering-Angriff erlebt bzw. gemacht? Könnten Sie bitte über diese Erfahrung erzählen?
6	Welche Maßnahmen sollten ergriffen werden, um die Awareness für Social Engineering zu fördern?

Auswahl der Teilnehmer – wer gilt als Experte?

Nach Kruse (2015, S. 175) verfügen Experten über folgende Dimensionen des „höhersymbolischen Sonderwissens“:

- Erstens: technisches Wissen – das formelle und explizite Wissen über „Operationen und Regelabläufe, fachspezifische Anwendungsroutinen, bürokratische Kompetenzen usw.“ (Kruse, 2015, S. 176 in Anlehnung an Bogner & Menz, 2005, S. 43). Diese Dimension des Wissens wird auch als objektives Sachwissen bezeichnet (Kruse, 2015, S. 176 in Anlehnung an Bogner & Menz, 2005, S. 43)
- Zweitens: Wissen über diverse Prozesse. Kruse (2015, S. 176) beschreibt dies als Wissen über „[...] Handlungsabläufe, Interaktionsroutinen, organisationale Konstellationen, sowie vergangene oder aktuelle Ereignisse“. Darunter ist informelles bzw. implizites Wissen zu verstehen, das insbesondere praktisches Erfahrungswissen umfasst.
- Drittens: Deutungswissen. Das Deutungswissen umfasst nach Kruse (2016, S. 176 in Anlehnung an Bogner & Menz, 2005, S. 43 f.) „[...] subjektive Wissensheuristiken und implizites Erfahrungswissen“ und ist als Wissensdimension besonders wichtig.

Die Experten für die Experteninterviews wurden aus einem Kreis an internen Kollegen ausgewählt, die nicht nur lange Erfahrung im Informationssicherheitsbereich haben,

sondern auch in anderen Bereichen (Wirtschaftswissenschaft, Mathematik, Finanzen etc.).

Insgesamt wurden drei Experteninterviews durchgeführt und vollständig mit einem Diktiergerät aufgenommen, um eine weitere Auswertung zu gewährleisten. Die Experten wurden im Vorfeld über die Interviewsituation informiert und haben freiwillig am Interview teilgenommen. Das erste Interview wurde am 24.06.2019, das zweite Interview am 08.07.2019 und das dritte Interview am 05.08.2019 durchgeführt.

3.2.2 Auswertungsmethodik und Analyseschritte

Die Auswertung der Experteninterviews orientiert sich primär an den Äußerungen der Experten, die „[...] von Anfang an im Kontext ihrer institutionell-organisatorischen Handlungsbedingungen verortet" werden und „[...] von hierher ihre Bedeutung [erhalten] und nicht von daher, an welcher Stelle des Interviews sie fallen" (Meuser & Nagel, 2009, S. 476). Meuser und Nagel (2009, S. 476) empfehlen die folgenden Schritte für die Auswertung von Experteninterviews:

1. Transkription
   Hierbei ist es nicht notwendig, die gesamte Tonaufnahme der audiografisch aufgezeichneten Interviews zu transkribieren, sondern es reicht die Transkription der thematisch relevanten Passagen.
2. Paraphrasierung
   Die Paraphrase kann zwar in der Manier des Alltagsverstandes erfolgen, darf aber nicht ausschließen, was die Experten insgesamt äußern.
3. Codierung
   In diesem Schritt sollen die paraphrasierten Passagen thematisch den textnahen Überschriften, den Codes, zugeordnet werden. Dabei kann es vorkommen, dass eine Passage mehreren Überschriften zugeordnet werden kann. Bezugsgröße ist in diesem Schritt jedoch immer noch das einzelne Interview. In diesem Schritt erfolgt die Verdichtung und somit auch die Reduktion des Textes.
4. Thematischer Vergleich von Interviews
   Die Logik dieses Schrittes entspricht der der Codierung, jedoch werden in diesem Schritt die thematisch-vergleichbaren Testpassagen aus verschiedenen Interviews zusammengefasst. Eine Überprüfung und ggf. eine Revision des zugeordneten Datenvolums und der Überschriften sind hierbei ggf. notwendig.
5. Soziologische Konzeptualisierung
   Hier soll die Ablösung von den Texten und der Terminologie der Interviewten erfolgen. In diesem Schritt sollen die Aussagen über das Expertenwissen getroffen werden.
6. Theoretische Generalisierung
   Hier sollen die Ergebnisse rekonstruiert und zu empirischen Theorien verknüpft werden.

Die genaue Durchführung der Auswertung wird im Anhang erläutert (s. Anhang 1.8 Auswertung der Experteninterviews). Im folgenden Kapitel werden die Ergebnisse der

Experteninterviews dargestellt und analysiert. Abschließend sollen die Ergebnisse der Gruppendiskussionen und der Experteninterviews zusammengeführt werden, um die Forschungsfragen zu beantworten.

3.2.3 Ergebnisdarstellung der Experteninterviews

In diesem Abschnitt werden die Ergebnisse der Auswertung der Experteninterviews nach Meuser und Nagel (2009) dargestellt. Im Abschluss soll der thematische Vergleich der Interviews erfolgen. Erst danach erfolgt die theoretische Generalisierung. Im Anhang 1.8 Auswertung der Experteninterviews sind die transkribierten und ausgewerteten Experteninterviews zu finden.

Das erste Interview wurde am 07.06.2019 durchgeführt, komplett nach Meuser und Nagel (2009) transkribiert und paraphrasiert. Danach wurden die thematischen Überschriften für die paraphrasierten Abschnitte entwickelt. Im Folgenden werden die finalen Überschriften präsentiert.

- Social Engineering ist eine Manipulationsmethode, um gewisse Informationen herauszufinden
- Phishing-Angriffe können personalisiert (Spear-Phishing) und unpersonalisiert (Phishing-Welle) gestaltet und durchgeführt werden
- Spear-Phishing ist eine personalisierte Attacke, die ihre Opfer dazu zwingt, eine bestimmte Aktion (z. B. das Anklicken eines Links in einer erhaltenen E-Mail) durchzuführen
- Ein effektiver Hackerangriff inkludiert mehrere Social-Engineering-Methoden
- Eine Phishing-Attacke in Kombination mit anderen Methoden kann effektiv sein
- Es muss eine Sensibilisierung für das Thema Social Engineering und dessen Techniken geschaffen werden
- Der Diebstahl persönlicher Daten wird eins der Zukunftsziele der Hacker sein
- Hackerattacken der Zukunft werden komplexer und elaborierter sein. Hacker werden versuchen, bei ihren Opfern verschiedene Emotionen zu erzeugen
- Die meistbenutzte Zukunftsmethode der Hacker wird weiter Phishing bleiben
- Ein Ziel der Hacker könnte es sein, z. B. einen gewissen Beschäftigten auszuspionieren und somit einen Imageverlust für das Unternehmen zu verursachen
- Ein Hackerangriff könnte im Rahmen eines Unternehmens zu Imageverlust führen
- Benutzung verschiedener Passwörter für verschiedene Systeme
- Keine Nutzung von Fremdfirmenhardware
- Phishing ist eine Methode des Social Engineerings
- Phishing-E-Mails haben verschiedene Merkmale
- Informationsklassifikation soll eingehalten werden
- Informationen sollen nach Klassifikationsstufen behandelt werden
- Unbekannte Links anzuklicken, entspricht nicht der IT-Sicherheitskonformität

- Es sollen möglichst viele Schulungen und Sensibilisierungsmaßnahmen stattfinden
- Informationssicherheits-Awareness-Schulungen sollen diverse Formate und Themen beinhalten

Interview 2 wurde am 08.07.2019 durchgeführt, ebenfalls vollständig nach Meuser und Nagel (2009) transkribiert und paraphrasiert. Anschließend wurden die thematischen Überschriften für die paraphrasierten Abschnitte entwickelt, die final wie folgt lauten:

- Die wichtigste Methode des Social Engineerings ist es, Informationen über das Internet oder soziale Medien herauszusuchen
- Soziale Medien gehören zu den wichtigsten Plattformen, die Social Engineers benutzen, um an Personeninformationen zu gelangen
- Nutzer tendieren dazu, vertrauensvoll zu sein und nicht weiter zu überprüfen, ob z. B. die benutzte Applikation oder ein IT-System tatsächlich datenschutzkonform ist. Obwohl die Techniken der Social Engineers sich weiterentwickeln, wird z. B. Phishing weiter eine der wichtigsten Methoden bleiben
- Phishing und Erpressung sind die effektivsten Methoden der Social Engineers, wenn es beispielsweise darum geht, Nutzer mit stark ausgeprägtem Konsumverhalten anzugreifen
- Social Engineering spielt für die einzelnen Mitarbeiter keine große Rolle, denn sie sind alle in einem Unternehmen verbunden. Wenn es allerdings um Unternehmensinteressen auf einem neuen Markt geht, dann erfolgt SE häufig über die Anknüpfung von persönlichen Kontakten
- Eine Kompromittierung eines einzelnen Mitarbeiters ist nicht zielführend für Social Engineers, da alle Aktivitäten, die derjenige unternimmt, transparent in den Unternehmenssystemen dargestellt werden. Wenn es jedoch um Machtgewinn geht, benutzen Social Engineers Kompromittierung und Manipulation
- Der bewusste Umgang mit sozialen Medien ist sehr wichtig für die Nutzer, denn Social Engineers benutzen soziale Netzwerke häufig, um an deren persönliche Informationen heranzukommen
- Fremdfirmenhardware, die man auf einer Konferenz oder Veranstaltung bekommt, darf nicht an Volkswagen-IT-Systeme oder -Hardware angeschlossen werden
- Wichtigste Awareness-Maßnahmen sind die Überprüfung der IT-Systeme und die Sensibilisierung der Mitarbeiter

Das dritte Interview wurde am 05.08.2020 durchgeführt. Auch bei der Auswertung des dritten Interviews wurde die Auswertungsmethode nach Meuser und Nagel (2009) implementiert. Im Folgenden werden die finalen Überschriften präsentiert:

- Die wichtigsten Methoden Phishing und Vishing werden nicht nur bei generellen Angriffen benutzt, sondern auch bei personalisierten Angriffen
- Eine der Methoden, die Social Engineers benutzen, sind persönliche Gespräche, um das Vertrauen anderer Menschen zu gewinnen

- Methoden und Strategien des Angriffs beinhalten persönliche Kontaktaufnahme, Anrufe und E-Mail-Austausch
- Kontaktaufnahme erfolgt öfters durch soziale Medien
- Diverses technisches Know-how hilft dem Angreifer, die Angriffe so elaboriert wie möglich zu gestalten. Zurzeit ist es auch möglich, den Schadcode durch das Öffnen einer E-Mail anzustoßen
- Die Vorsortierung der E-Mails, die bei diversen IT-Systemen vorhanden ist, ist jedoch nicht zuverlässig
- Persönliche Informationen werden beim Angriff benutzt
- Technische Möglichkeiten bieten den Angreifern die Möglichkeit zur Identitätsmanipulation
- Neue Technologien werden in fünf Jahren mehr anbieten können und die Menschen, die darauf verzichten werden, werden wirtschaftlich benachteiligt
- Das Ziel von Social Engineering ist und bleibt in den nächsten fünf Jahren Identitätsmanipulation
- Unternehmen sind auch von großem Interesse bei Social Engineers
- Die Sensibilisierung der Mitarbeiter ist die wichtigste Maßnahme gegen Social Engineering
- Sensibilisierungsmaßnahmen als eine der wichtigsten Methoden, Angriffe zu vermeiden, sollen mit Emotionen verbunden werden, damit ein entsprechender Lerneffekt da ist

Nach Meuser und Nagel (2009) sollen am Ende der Auswertungsmethode ein thematischer Vergleich der Interviews und eine soziologische Konzeptualisierung erfolgen. Grundsätzlich lassen sich die Interviews thematisch anhand von Interviewfragen vergleichen, da die Interviewfragen in dieser Arbeit die Themen präsentieren, denen die paraphrasierten Passagen zugeordnet werden sollen.

Interviewfrage 1: Was sind Ihrer Meinung nach die wichtigsten Techniken, die Social Engineers anwenden?

Interview 1

- Ein effektiver Hackerangriff inkludiert mehrere Social-Engineering-Methoden
- Eine Phishing-Attacke in Kombination mit anderen Methoden kann effektiv sein
- Social Engineering ist eine Manipulationsmethode, um gewisse Informationen herauszufinden
- Phishing-Angriffe können personalisiert (Spear-Phishing) und unpersonalisiert (Phishing-Welle) gestaltet und durchgeführt werden
- Spear-Phishing ist eine personalisierte Attacke, die ihre Opfer dazu zwingt, eine Aktion (z. B. das Anklicken eines Links in einer erhaltenen E-Mail) durchzuführen

Interview 2

- Die wichtigste Methode des Social Engineerings besteht darin, Informationen über das Internet oder soziale Medien herauszusuchen
- Soziale Medien sind eine der wichtigsten Plattformen, die Social Engineers benutzen, um an persönliche Informationen heranzukommen
- Phishing und Erpressung sind die effektivsten Methoden der Social Engineers, wenn es z. B. darum geht, Nutzer mit stark ausgeprägtem Konsumverhalten anzugreifen

Interview 3

- Die wichtigsten Methoden Phishing und Vishing werden nicht nur bei generellen Angriffen benutzt, sondern auch bei personalisierten Angriffen
- Eine der Methoden, die Social Engineers benutzen, sind persönliche Gespräche, um das Vertrauen von anderen Menschen zu gewinnen
- Methoden und Strategien des Angriffs beinhalten persönliche Kontaktaufnahme, Anrufe und E-Mail-Austausch
- Die Kontaktaufnahme erfolgt öfters durch soziale Medien

Alle Experten erwähnen Phishing und Vishing als die meistbenutzten Methoden der Social Engineers. Außerdem können diese Angriffe laut den Experten sowohl personalisiert als auch unpersonalisiert gestaltet werden. Ein effektiver Hackerangriff inkludiert viele Methoden und der Erstkontakt erfolgt in der Regel über soziale Medien oder die persönliche Kontaktaufnahme. Experte 2 nennt außer Phishing noch eine weitere effektive Methode des Social Engineerings, nämlich Erpressung.

Interviewfrage 2: Wie sieht Social Engineering in fünf Jahren aus? Welche Techniken werden wichtiger?

Interview 1

- Der Diebstahl der persönlichen Daten wird eins der Zukunftsziele der Hacker sein
- Hackerattacken der Zukunft werden komplexer und elaborierter sein. Hacker werden versuchen, bei ihren Opfern verschiedene Emotionen zu erzeugen
- Die meistbenutzte Zukunftsmethode der Hacker wird weiter Phishing bleiben

Interview 2

- Nutzer tendieren dazu, vertrauensvoll zu sein und nicht weiter zu überprüfen, ob z. B. die benutzte Applikation oder ein IT-System tatsächlich datenschutzkonform ist. Obwohl die Techniken der Social Engineers sich weiterentwickeln, wird z. B. Phishing weiter eine der wichtigsten Methoden bleiben

Interview 3

- Neue Technologien werden in fünf Jahren mehr anbieten können und die Menschen, die darauf verzichten werden, werden wirtschaftlich benachteiligt
- Das Ziel von Social Engineering ist und bleibt in den nächsten fünf Jahren Identitätsmanipulation

Alle drei Experten gehen davon aus, dass Phishing die meistbenutzte Methode im Kontext des Social Engineerings bleiben wird. Außerdem erwähnt der dritte Experte die Identitätsmanipulation als eine weitere der möglichen Methoden, die Social Engineers benutzen werden.

Interviewfrage 3: Welche Rolle spielt Social Engineering in Bezug auf ein Unternehmen?

Interview 1

- Ein Ziel der Hacker könnte es sein, z. B. einen gewissen Beschäftigten auszuspionieren und somit einen Imageverlust für das Unternehmen zu verursachen
- Ein Hackerangriff könnte im Rahmen eines Unternehmens zu Imageverlust führen

Interview 2

- Social Engineering spielt für die einzelnen Mitarbeiter keine große Rolle, denn sie sind alle in einem Unternehmen verbunden. Wenn es allerdings um Unternehmensinteressen auf einem neuen Markt geht, dann erfolgt Social Engineering-Angriff häufig über die Anknüpfung von persönlichen Kontakten
- Die Kompromittierung eines einzelnen Mitarbeiters ist nicht zielführend für Social Engineers, da alle Aktivitäten, die dieser unternimmt, transparent in den Unternehmenssystemen dargestellt werden. Wenn es jedoch um Machtgewinn geht, benutzen Social Engineers Kompromittierung und Manipulation

Interview 3

- Unternehmen sind auch von großem Interesse für Social Engineers

Der erste Experte benennt die potenzielle Ausspionierung einzelner Beschäftigter als mögliches Ziel von Social Engineers, mit dem Imageverluste für das entsprechende Unternehmen bezweckt werden. Der dritte Experte stimmt dem zu und ist der Ansicht, dass Unternehmen für Social Engineers von großem Interesse sind. Dem wiederum widerspricht der zweite Experte und meint, dass die Ausspionierung einzelner Mitarbeiter für Social Engineers keine große Bedeutung hat.

Interviewfrage 4: Mit welchen Maßnahmen kann der durchschnittliche User verhindern, im privaten Umfeld und im Arbeitsleben Opfer von Social Engineering zu werden?

Interview 1

- Benutzung verschiedener Passwörter für verschiedene Systeme
- Keine Nutzung von Fremdfirmenhardware
- Phishing-E-Mails haben verschiedene Merkmale
- Informationsklassifikation soll eingehalten werden
- Informationen sollen nach Klassifikationsstufen behandelt werden
- Unbekannte Links anzuklicken, entspricht nicht der IT-Sicherheitskonformität

Interview 2

- Der bewusste Umgang mit sozialen Medien ist sehr wichtig für die Nutzer, denn Social Engineers benutzen soziale Netzwerke, um an persönliche Informationen heranzukommen

Interview 3

- Die Vorsortierung der E-Mails, die bei diversen IT-Systemen vorhanden ist, ist jedoch nicht zuverlässig

Damit der durchschnittliche User verhindern kann, dass er Opfer von Social Engineering wird, schätzt der erste Experte es als besonders hilfreich ein, verschiedene Passwörter für verschiedene Systeme zu verwenden, Informationsklassifikationen einzuhalten und in der Folge auch die entsprechenden Regeln, die verschiedenen Informationen unterschiedlich zu schützen, zu beachten. Er weist zudem darauf hin, dass Phishing-E-Mails verschiedene Merkmale haben können und es sicherheitstechnisch nicht nachvollziehbar sei, unbekannte Lins anzuklicken, ohne zu wissen, was sich dahinter verbirgt. Für den zweiten Experten ist der bewusste Umgang mit sozialen Medien eine der effektivsten Maßnahmen gegen Social Engineering. Der dritte Experte ist der Meinung, dass die technischen Sicherheitsmaßnahmen bei IT-Systemen nicht zuverlässig sind, was bedeutet, dass sich der User den Merkmalen von Phishings-E-Mails und der Gefahr dahinter bewusst sein soll.

Interviewfrage 5: Haben Sie jemals einen Social Engineering-Angriff erlebt bzw. gemacht? Könnten Sie bitte über diese Erfahrung berichten?

Interview 2

- Fremdfirmenhardware, die man auf einer Konferenz oder Veranstaltung bekommt, darf nicht an Volkswagen-IT-Systeme oder -Hardware angeschlossen werden

Nur der zweite Experte hat sich dazu geäußert und ist der Ansicht, dass zur Vermeidung von Sicherheitsrisiken und Hackerangriffen Fremdfirmenhardware von den

Volkswagen-IT-Systemen fernzuhalten ist und jeglicher Anschluss ebensolcher zu vermeiden ist.

Interviewfrage 6: Welche Maßnahmen sollten ergriffen werden, um die Awareness für Social Engineering zu fördern?

Interview 1

- Es muss eine Sensibilisierung für das Thema Social Engineering und dessen Techniken geschaffen werden
- Es sollen möglichst viele Schulungen und Sensibilisierungsmaßnahmen stattfinden
- Informationssicherheits-Awareness-Schulungen sollen diverse Formate und Themen beinhalten

Interview 2

- Die wichtigste Awareness-Maßnahmen sind die Überprüfung der IT-Systeme und die Sensibilisierung der Mitarbeiter

Interview 3

- Die Sensibilisierung der Mitarbeiter ist die wichtigste Maßnahme gegen Social Engineering
- Sensibilisierungsmaßnahmen als eine der wichtigsten Methoden, Angriffe zu vermeiden, sollen mit Emotionen verbunden werden, damit ein entsprechender Lerneffekt da ist

Alle Experten teilen die Meinung, dass die wichtigste Maßnahme gegen Social Engineering die Sensibilisierung der Mitarbeiter zu diesem Thema ist. Entsprechende Informationssicherheitsschulungen sollen demnach diverse Formate und Themen beinhalten und Emotionen hervorrufen, damit bessere Lerneffekte erzeugt werden.

Nach der soziologischen Konzeptualisierung soll die theoretische Generalisierung erfolgen und die Ergebnisse der Interviews sollen mit den bereits existierenden Theorien verknüpft werden. Generell entsprechen diese Expertenaussagen der in Kapitel 2.5 aufgeführten Empirie. Aus dem Verizon Data Breach Investigations Report von 2019 geht hervor, dass über 90 % der Malware per E-Mail übermittelt wurden. Zudem existieren diverse Hackerangriffe, wo die Erstkontaktaufnahme über soziale Medien erfolgt (vgl. Hommel & Reiser, 2016; Muniz & Lakhani, 2013) Daher sollen diese Themen in der finalen Präsentation der Ergebnisse thematisiert werden. Das BSI (2023) bezeichnet Identitätsdiebstahl zusammen mit Diebstahl persönlicher oder vertraulicher Daten als eine der größten Gefahren online.

Obwohl sich die Experten nicht einig sind, ob die Ausspionierung einzelner Beschäftigter ein Ziel von Social Engineers sein kann, belegen die Experimente „Robin Sage“ und „Emily Williams“ (Hommel & Reiser, 2016; Muniz & Lakhani, 2013) eindeutig, dass auch einzelne Beschäftigte und somit deren Unternehmen Opfer von Hackerattacken werden können.

Die Experten und auch die Ergebnisse der empirischen Forschung aus dem Kapitel 2.5 waren sich einig, dass verschiedene Passwörter für verschiedene Systeme verwendet werden sollen, da laut dem Magazin Digital Business Cloud (Sieger, 2019) bei 80 % der Hackerangriffe gestohlene und wiederverwendete Anmeldeinformationen (und somit auch Passwörter) das Einfallstor sind.

Obwohl das Thema Nutzung von Fremdfirmenhardware in der Literatur in Bezug auf Cyber Security eine wichtige Rolle spielt, hat sich nur ein Experte dazu geäußert, dass zur Vermeidung von Sicherheitsrisiken und Hackerangriffen Fremdfirmenhardware von den Volkswagen-IT-Systemen fernzuhalten und deren Anschluss zu vermeiden ist. In der Literatur zur Informationssicherheitsforschung hingegen herrscht allgemein Konsens, dass der Umgang mit Speicher- und Endgeräten für Informationssicherheit von hoher Relevanz ist, da die Endgeräte zu den wichtigsten Angriffszielen für Cyberkriminelle gehören (Tiwari, 2018; Parsons et al., 2017).

Um weiter die Forschungsfrage 1 *„Welche Themen der Informationssicherheits-Awareness und welche spielerischen Charakteristiken sind im Rahmen eines Serious Game zu behandeln?“* zu beantworten, sollen in den nächsten Kapiteln die Ergebnisse der Experteninterviews und Gruppendiskussionen zusammengeführt und präsentiert werden.

3.3 Darstellung der Ergebnisse aus den Experteninterviews und Gruppendiskussionen in Form einer didaktischen Spielentwicklung

Vor dem Abgleich der qualitativen Ergebnisse mit den bestehenden Methoden (u. a. die Informationssicherheits-Awareness-Unterweisung, Security Arena) bei der Volkswagen AG sollen die qualitativen Ergebnisse aus den Gruppendiskussionen und Experteninterviews zusammengefügt werden. Da eins der Ziele dieser Dissertation eine didaktische Spielentwicklung ist, soll aus den zusammengeführten Ergebnissen ein didaktisches Konzept für ein Serious Game zum Thema Informationssicherheits-Awareness entwickelt werden. Vor der vorläufigen Spielpräsentation soll eine didaktische und inhaltliche Darstellung der Lernziele erfolgen, die mit dem Serious Game angestrebt werden.

3.3.1 Kurze Darstellung der Spielmechaniken

Im wissenschaftlichen Diskurs existieren zwei Vorgehensweisen, um ein Spiel und entsprechende Lernaufgaben zu kombinieren (vgl. Kerres et al., 2009). Zum einen kann „[..] das Spiel in eine didaktisch aufbereitete Lernsituation eingebettet werden“ und zum anderen können „[...] didaktisch aufbereitete Elemente in das Spiel eingebettet werden“ (Kerres et al., 2009, S. 8 ff.).

Für die Entwicklung des Spiels im Rahmen dieser Arbeit wurde die Strategie „Einbettung des Spiels in eine didaktische Lernsituation“ nach Kerres et al. (2009) ausgewählt, denn eins der Primärziele dieser Studie ist es, ein konzeptionelles Serious

Game zu entwickeln, und nicht, die lose Folge voneinander abgetrennter spielerischer und berufsrelevanter Inhalte zu erproben. Obwohl sich die Lernziele, genauso wie die didaktischen Rahmenbedingungen des Spiels, immer noch in der konzeptionellen Entwicklungsphase befinden, können jedoch schon jetzt die wichtigsten Schwerpunkte der inhaltlichen Spielentwicklung identifiziert werden.

In Tabelle 7 sind sowohl Beispiele für Lernziele für die wichtigsten Schwerpunkte als auch kurze Erläuterungen dargestellt. Die Inhalte für die Spielentwicklung wurden nicht nur auf Basis der Ergebnisse der Gruppendiskussionen und der Experteninterviews, sondern auch mithilfe diverser Richtlinien der Volkswagen AG zu informationssicherheitskonformem Verhalten erstellt.

Tabelle 7: Inhaltliche Schwerpunkte des Spiels

Inhaltliche Schwerpunkte	**Beispiele des informationskonformen Verhaltens**
E-Mail-Bearbeitung	• Jeder Beschäftigte soll in der Lage sein, eine Phishing-E-Mail nach gewissen Merkmalen zu identifizieren (z. B.: Ist der Absender bekannt? Ist diese E-Mail zu erwarten? Ist der E-Mail-Inhalt verständlich?) • Verdächtige E-Mails sollen nicht angeklickt/geöffnet werden und sind sofort zu vernichten. • Jede verdächtige E-Mail kann durch das Computer Emergency Response Team (CERT) kostenlos überprüft werden.
Passwortmanagement	• Computerpasswörter, Windows-Passwörter etc. sind geheim und dürfen nicht veröffentlicht oder weitergegeben werden. • Beim Verlassen des Arbeitsplatzes soll jeder Volkswagen-Computer mit einem entsprechenden Passwort gesperrt werden. • Nutzer sollen über das Wissen verfügen, dass jedes IT-System ein separates Passwort haben soll. • Das Volkswagen-Passwort soll verschiedene Anforderungen erfüllen (Länge, Sonderzeichen, Klein- und Großbuchstaben etc.).
Umgang mit (mobilen) Speicher- und Endgeräten	• Keine privaten oder firmenfremden Endgeräte (Handy, USB-Stick etc.) sollen an die Volkswagen-Hardware angeschlossen werden.
Umgang mit Informationen u. a. im Kontext mobiler Arbeit	• Updates an den Volkswagen-Computern, -Laptops etc. werden automatisch bzw. nach der lokalen Freigabe durchgeführt und nicht durch z. B. Microsoft bzw. eine IT-Abteilung. • Das Surfen im Internet ohne Volkswagen-VPN-Verbindung, wenn der Nutzer z. B. nicht auf dem Werksgelände ist, ist verboten. • Auf dem Werksgelände dürfen keine Fotos gemacht werden. • Es ist nicht erlaubt, arbeitsrelevante Fotos zu veröffentlichen.
Zutritts- und Zugriffsschutz	• Wenn der Nutzer seinen Arbeitsplatz verlässt, muss sein Bildschirm auf seinem Arbeitslaptop/Arbeitscomputer gesperrt sein. • Die Public-Key-Infrastruktur-Karte (PKI-Karte) muss immer mitgenommen werden.

In Anbetracht der Ergebnisse der Gruppendiskussionen und Experteninterviews ergeben sich folgende Aussagen für Forschungsfrage 1: *Welche Themen der Informationssicherheits-Awareness und welche spielerischen Charakteristiken sind im Rahmen eines Serious Games zu behandeln?*

Im folgenden Abschnitt soll der ausgearbeitete Vorschlag für eine didaktische Spielentwicklung dargestellt werden. Zuerst wird der Spielablauf zusammen mit den didaktischen Rahmenbedingungen des Spiels präsentiert. Danach erfolgt die Präsentation der Einbettung von Informationssicherheits-Awareness-Themen ins Spiel sowie der spielerischen Charakteristiken.

Der Spielablauf wurden auf Basis der Ergebnisse aus den Gruppendiskussionen entwickelt. Damit es für den Leser plausibel ist, warum die folgenden Spielmechaniken und Themen der Informationssicherheit ausgewählt wurden, werden auch die Kategorien und die Fragen aus den Experteninterviews erwähnt.

- *Storytelling und Spielablauf* (siehe Kategorie I *„Transparenter Spielanfang als kurzes Video“*, Kategorie III *„Dynamische und unvorhersehbare Spielentwicklung ist interessefördernd“*, Kategorie XI *„Ziele im Spiel sollen transparent sein“*, Kategorie XIX *„Spannendes Spielende“*)
  Das Spiel besteht aus drei Teilen und soll nicht länger als 20 Min. insgesamt dauern. Am Anfang des Spiels soll ein kurzes Erklärungsvideo abgespielt werden, in dem beschrieben wird, worum es geht (im Stil eines Filmblockbusters). Danach soll das Spiel konzipiert werden und final soll der Spieler ein Endspiel nach dem Spiel spielen. Informationen in Form von Handouts sollen dann nach dem Spiel zur Verfügung gestellt werden.
- *Charaktere/Spielfiguren* (siehe Kategorie XII *„Multiplayer-Spiele sind interessefördernd“*, Kategorie XIII *„Gegner im Spiel motiviert“*, Kategorie XVIII *„Möglichkeit, untypische Rollen auszuprobieren“*)
  Die Ergebnisse der Gruppendiskussion zeigen, dass sich die Spieler ein Multiplayer-Spiel wünschen. Leider ist dies aufgrund von begrenzten technischen Möglichkeiten kaum zu realisieren, deswegen wurde die Entscheidung getroffen, die Spieleroptionen möglichst polar zu entwickeln – ein Antagonist und ein Protagonist –, denn die Gruppendiskussionsmitglieder haben sich gewünscht, untypische Rollen auszuprobieren und die Möglichkeit zu haben, nicht nur einen Protagonisten zu spielen, sondern auch einen Antagonisten.

Grundsätzlich sollen im Spiel zwei Perspektiven zur Auswahl stehen: „Hacker“ (bzw. ein Social Engineer) und „Nutzer“. Die Auswahl einer Spielfigur führt zum Spiel auf einem von zwei möglichen Spielfeldern.

- Spielperspektive „Nutzer“: ein junger Angestellter bei VW, Held, Protagonist, weiß, dass ein Hacker versucht, an Informationen zu kommen, indem er in den Büroräumen etc. nach Auffälligkeiten sucht
- Spielperspektive „Social Engineer“: ein Antagonist, ein Hacker, der versucht, Systeme zu hacken und an Informationen zu kommen, agiert in den Büroräumen, im Flur, an der Rezeption etc.

Wenn eine Spielperspektive ausgewählt wird, soll das System als Gegner mitspielen, wenn also der Spieler die Social Engineer-Perspektive auswählt, wird das System als „Nutzer“ spielen.

Sowohl die Spielperspektive „Hacker“ als auch die des „Nutzers“ sollen möglichst attraktiv für den Spieler dargestellt werden.

- *Avatar* (siehe Kategorie XV *„Wenige Avatar-Auswahloptionen werden bevorzugt“*, Kategorie XVI *„Selbstidentifikation mit Avatar ist wichtig“*)
  Die Ergebnisse der Gruppendiskussionen zeigen, dass, obwohl die Spieler eine Avatar-Auswahl im Spiel präferieren, die Avatar-Auswahlmöglichkeiten eher über weniger Optionen verfügen sollten. Nichtdestotrotz soll der Spieler die Möglichkeit haben, seine Spielfigur bzw. seinen Avatar zu personalisieren. Das macht es in Zusammenhang mit der Spieldynamik für den Spieler möglich, sich mit (s)einem Avatar zu identifizieren.
- *Spielentwicklung* (siehe Kategorie II *„Aufgabenvielfalt fördert Interesse“*, Kategorie IV *„Entscheidungsmöglichkeiten im Spiel sind motivierend“*, Kategorie V *„Offene Spielwelten mit gewissen Spielregeln sind interessefördernd“*, Kategorie VI *„Realitätsnahe Spiele werden bevorzugt“*, Kategorie VIII *„Transparentes Belohnungssystem“*)
  Es müssen verschiedene Themen der Informationssicherheit erläutert werden (Passwortmanagement, E-Mail-Bearbeitung etc.), die als diverse Aufgaben oder Missionen dargestellt sein sollen. Nach jeder Aufgabe oder Mission soll der Spieler eine Erläuterung und eine bestimmte Punktanzahl bekommen. Die Aufgaben sollen tägliche Situationen mit Informationssicherheitsbezug darstellen.

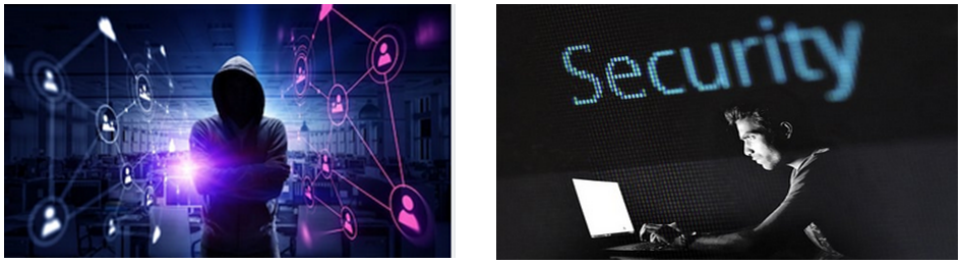


Abbildung 12: Grafische Darstellung „Hacker“ und „Nutzer“ (pixabay, o. J.)

- *Zeitdruck* (siehe Kategorie XVII *„Zeitdruck motiviert“)*
  Laut Gruppendiskussionsergebnissen ist Zeitdruck ein wichtiger Faktor und kann als eine zusätzliche Spielanregung eingesetzt werden. Dabei kann zwischen einem Zeitdruck bei jeder Aufgabe oder einem generellen Spielzeitdruck unterschieden werden.
- *Grafische Darstellung* (siehe Kategorie VII *„Realitätsnahe Grafik wird bevorzugt“*)
  Den Ergebnissen der Gruppendiskussionen zufolge soll die grafische Darstellung im Spiel einen realitätsnahen Charakter haben.
- *Didaktische Einsetzung (Lernszenario)*
  Grundsätzlich soll das Spiel als eine zusätzliche obligatorische Sensibilisierungsmaßnahme am Anfang der Ausbildung bei neuen Auszubildenden bzw. Studenten im Praxisverbund eingesetzt werden. Die Sprache des Spiels soll Deutsch

sein. Später kann das Spiel als eine zusätzliche Sensibilisierungsmaßnahme konzernweit eingesetzt werden.

- *Spielsituationen*
  In diesem Abschnitt sollen Beispiele für die mögliche Entwicklung des Spiels aus der Perspektive des „Nutzers" und aus der Hackerperspektive präsentiert werden. Die Beispiele sind generisch, wurden jedoch auf Basis der Experteninterviews und Gruppendiskussionen entwickelt. Die Themen können kombiniert werden und müssen nicht in einer Reihenfolge gespielt werden. Dies entspricht auch den Ergebnissen der Gruppendiskussionen (siehe Kategorie V *„Offene Spielwelten mit gewissen Spielregeln sind interessefördernd"*), denn so eine Spielgestaltung bietet eine gewisse Freiheit an, basiert jedoch auf bestimmten Regeln.

Bei jedem Thema soll der Spieler einen Überblick über die alltäglichen Berufssituationen bekommen, in welchen das Thema Informationssicherheit eine besondere Rolle spielt.

3.3.2 Die Spielperspektive „Nutzer"

1. E-Mail-Bearbeitung

Die Ergebnisse aus den Experteninterviews zeigen deutlich, dass Phishing nicht nur zurzeit eine beliebte Methode von Social Engineers ist, sondern auch in der Zukunft eine wichtige Methode bleiben wird. Daher ist es bedeutsam, dass die Spieler die wichtigsten Merkmale des Phishings erlernen und generell zu diesem Thema sensibilisiert werden.

Aus den Ergebnissen der Gruppendiskussionen wurde ersichtlich, dass die folgenden Spielmerkmale für Spieler wichtig sind: eine transparente Einführung in das Spiel (Kategorie I *„Transparenter Spielanfang als kurzes Video"*), Hintergrundgeschichte der Spielfigur (Kategorie XIV *„Hintergrundgeschichte fördert Interesse"*), Identifikation mit dem Avatar (Kategorie XVI *„Selbstidentifikation mit Avatar ist wichtig"*), Spiele, die auf realen Situationen basieren (Kategorie VI *„Realitätsnahe Spiele werden bevorzugt"*), klar definierte Ziele im Spiel (Kategorie *„Ziele im Spiel sollen transparent sein"*) und die Möglichkeit, einen realen oder vorprogrammierten Gegner zu haben (Kategorie XIII *„Gegner im Spiel motiviert"*).

Nachdem der Spieler sich für eine Spielperspektive (z. B. „Nutzer") entschieden und seinen Avatar personalisiert hat, bekommt er Informationen über seinen Charakter. Der Nutzer ist ein Beschäftigter bei der Volkswagen AG, weiß, dass er gerade ausspioniert wird, und versucht, im Rahmen des Spiels in realen Arbeitssituationen nicht auf den Gegner hereinzufallen.

Angenommen, der Spieler hat sich für die Spielperspektive des Nutzers entschieden, so wird im Einführungsvideo gezeigt, dass der Nutzer seine Karte in seinen Laptop steckt und die PIN-Nummer eintippt. Das Spiel beginnt damit, dass er anfängt, seine E-Mails zu bearbeiten. Der Nutzer hat drei neue E-Mails. Bei jeder E-Mail ist es möglich, sich die Absenderadresse anzuschauen, allerdings wird dies erst nicht explizit angezeigt. Die erste E-Mail beinhaltet eine Einladung zu einem Termin, die zweite

E-Mail ist eine Abstimmungsmail für ein Teamevent (z. B. Ich habe Zeit (ja/nein), am 27. Februar mit den Kollegen nach der Arbeit ins Restaurant zu gehen) und die dritte E-Mail ist eine Phishing-E-Mail mit einem gefährlichen Link.

Da den Ergebnissen der Gruppendiskussionen zufolge ein transparentes Belohnungssystem (Kategorie VIII) für die Spieler wichtig ist, erfolgt die Punktvergabe in diesem Abschnitt des Spiels folgendermaßen: Zum Anfang des Spiels bekommt der Nutzer 5 Punkte – er ist ein kompetenter Mitarbeiter und kennt sich mit den Regeln der Informationssicherheit aus. Für das Anklicken des Links in der Phishing-E-Mail werden dem Spieler 2 Punkte abgezogen. Um weitere Punkte zu bekommen, muss der Spieler entweder weiter seine E-Mails bearbeiten, in einem Feld eintippen, worauf man bei der Bearbeitung von E-Mails achten muss, oder das Spiel weiter erkunden.

2. Umgang mit (mobilen) Speicher- und Endgeräten

Einer der Experten ist der Meinung, dass die Benutzung von Fremdfirmenhardware (beispielsweise USB-Sticks) ein großes Risiko- und Angriffspotenzial birgt, und die anderen beiden Experten haben erwähnt, dass Mitarbeiter generell zu den Methoden des Social Engineerings sensibilisiert werden sollten. Daher scheint es logisch, die Sensibilität der Mitarbeiter im Spiel zum Umgang mit Fremdfirmenhardware zu schärfen.

Für die Entwicklung des folgenden Abschnitts wurden u. a. die Kategorien aus der Gruppendiskussion benutzt: Kategorie II *„Aufgabenvielfalt fördert Interesse“*, Kategorie III *„Dynamische und unvorhersehbare Spielentwicklung ist interesseförderndd“*, Kategorie VI *„Realitätsnahe Spiele werden bevorzugt“*, Kategorie VII *„Ziele im Spiel sollen transparent sein“* und Kategorie XIII *„Gegner im Spiel motiviert“*.

Die Ergebnisse der Gruppendiskussionen und der Experteninterviews wurden in einem Spielsequenzbeispiel konsolidiert, das wie folgt aussieht:

Der Nutzer bekommt eine E-Mail von einem Kollegen aus einer anderen Firma, den er auf einer Messe kennengelernt hat. Der Kollege hat dem Nutzer ein Päckchen von dieser Firma gesendet, in dem u. a. Notizblöcke, Tassen, Stifte und ein USB-Stick mit E-Mail-Link zu finden sind. In der E-Mail steht auch, dass sich auf dem USB-Stick ein Angebot für Dienstleistungen von der anderen Firma befindet. Der Nutzer soll sich nun entscheiden, ob er die Fremdfirmenhardware benutzt.

Es entspricht nicht den Regeln der Informationssicherheitskonformität, die Speicher- und Endgeräte einer fremden Firma zu benutzen und an die Arbeitscomputer anzuschließen. Sollte sich der Spieler für die Benutzung des USB-Sticks der fremden Firma entscheiden, sollen ihm entsprechend Punkte abgezogen werden. Danach soll dem Spieler die Erklärung dafür in Form eines Videos oder Texts zur Verfügung gestellt werden (siehe Kategorie VIII *„Transparentes Belohnungssystem“*).

3. Umgang mit Informationen u. a. im Kontext mobiler Arbeit

Die Experten erwähnen, dass verschiedene Informationen unterschiedlich zu schützen sind. Eines der Ziele von Social Engineers kann sein, bei Unternehmen Imageverluste hervorzurufen. etwa über die Ausspionierung von einzelnen bestimmten Mitar-

beitern. Diese beiden Themen werden im Spiel in der Spielsequenz „Umgang mit Informationen u. a. im Kontext mobiler Arbeit“ konsolidiert.

Die folgenden Kategorien und Unterkategorien wurden in dieser Spielsequenz benutzt: Kategorie I *„Transparenter Spielanfang als kurzes Video“*, Kategorie VI *„Realitätsnahe Spiele werden bevorzugt“*, Kategorie XI *„Ziele im Spiel sollen transparent sein“*, Kategorie XIII *„Gegner im Spiel motiviert“*, Kategorie II *„Aufgabenvielfalt fördert Interesse“*, Kategorie III *„Dynamische und unvorhersehbare Spielentwicklung ist interessefördernd“* sowie Kategorie V *„Offene Spielwelten mit gewissen Spielregeln sind interessefördernd“*.

Im Einführungsvideo wird gezeigt, wie der Nutzer in einem Café sitzt und einen Kaffee trinkt. Der Nutzer bekommt einen Anruf von seinem Kollegen. Sein Kollege führt gerade eine Videokonferenz mit wichtigen Investoren und braucht nun ganz dringend vertrauliche Informationen (z. B. die beauftragte Summe für das letzte Jahr für das Thema A und für das Thema B). Der Nutzer hat folgende Antwortmöglichkeiten: dem Kollegen sofort zu helfen oder dem Kollegen später eine Antwort schriftlich zuzuschicken.

Die Informationsklassifikation bei der Volkswagen AG verfügt über vier Vertraulichkeitsstufen: geheim (z. B. Aufsichtsratsvorlagen), vertraulich (dazu zählen beispielsweise Budgetpläne, Konstruktionsdaten, Ad-hoc-Mitteilungen vor Veröffentlichung), intern (Organisationsrichtlinien, Bereichsdarstellungen) und öffentlich (veröffentlichte Pressemitteilung etc.). Die Volkswagen-AG-Richtlinien besagen, dass mit vertraulichen Informationen besonders umzugehen ist, nämlich, dass sie unter Schutz stehen und daher ausschließlich einer begrenzten Gruppe von Berechtigten zugänglich gemacht werden dürfen. Von daher wäre hier eine informationssicherheitskonforme Antwort, dass der Nutzer später eine Antwort mit den wichtigen Zahlen per E-Mail schickt und diese nicht mündlich mitteilt.

Wenn sich der Spieler für eine mündliche Antwort entscheidet, werden ihm Punkte abgezogen. Am Ende dieses Spielteils soll der Spieler eine Erklärung bekommen, was ein informationssicherheitskonformes Verhalten wäre, welche Informationsklassifikationsstufen es gibt und wie unterschiedliche Informationen zu schützen sind.

Am Ende der Spielsequenz soll es ein kurzes Video geben, was den Spieler dazu motiviert, die andere Spielperspektive auszuprobieren und einmal die Rolle des richtigen Hackers einzunehmen. Dies entspricht auch den Ergebnissen der Gruppendiskussionen (Kategorie XIX *„Spannendes Spielende“*).

Laut Experten sammeln Social Engineers Informationen über ihre Opfer mithilfe von sozialen Medien, um Identitätsmanipulationen durchzuführen. Social Engineers haben über soziale Netzwerke die Möglichkeit, Zugriff auf private Informationen von Nutzern zu bekommen. Deswegen haben die Experten auch erwähnt, dass die Kontaktaufnahme der Social Engineers oft über die sozialen Medien erfolgt und die Nutzer äußerst bewusst mit sozialen Medien umgehen sollten. Daher soll im Spiel auch zum Umgang mit Informationen in sozialen Medien sensibilisiert werden.

Die folgenden Kategorien und Unterkategorien wurden für diese Spielsequenz benutzt: Kategorie VI *„Realitätsnahe Spiele werden bevorzugt“*, Kategorie XI *„Ziele im Spiel sollen transparent sein“*, Kategorie XIII *„Gegner im Spiel motiviert“*, Kategorie II *„Aufgabenvielfalt fördert Interesse“*, Kategorie III *„Dynamische und unvorhersehbare Spielentwicklung ist interessefördernd“* und Kategorie V *„Offene Spielwelten mit gewissen Spielregeln sind interessefördernd“*.

Der Nutzer folgt einigen Profilen in den sozialen Medien. Auf dem Instagram-Profil „Volkswagen_de“ sieht er einen Kommentar zu einem neuen Fahrzeug in der Entwicklung, an der er selber betätigt ist. Der Kommentar ist nach Meinung des Nutzers nicht ganz inhaltlich korrekt. Der Spieler hat in diesem Fall nun mehrere Optionen, wie er daraufhin agieren sollte, nämlich: entweder den Kommentar zu ignorieren, selber zu beantworten oder diesen an die Presseabteilung der Volkswagen AG weiterzuleiten. Das informationssicherheitskonforme Verhalten wäre hier, die Informationen an die Presseabteilung der Volkswagen AG weiterzugeben oder den Kommentar zu ignorieren. Ihn selber zu kommentieren, würde nicht den Informationssicherheitsrichtlinien entsprechen. Nachdem die Punktvergabe und Erklärung erfolgt sind, sollen dem Spieler die weiteren Spielsituationen für den Umgang mit sozialen Medien präsentiert werden, z. B. der Nutzer kriegt eine direkte Nachricht von einem Bekannten (z. B. aus dem Sportverein). Aus dem Gesprächsverlauf ist ersichtlich, dass die beiden schon öfter miteinander kommuniziert haben, jedoch über den Alltag, Hobbys, Rezepte, Sportgeräte etc. Die besagte Person aus dem Sportverein fragt nun auf einmal nach berufsrelevanten Informationen, beispielsweise: „Ist es so, dass bei Volkswagen der Gewinn für ID-Modelle steigt?“. Der Nutzer hat folgende Reaktionsmöglichkeiten: entweder die konkrete Antwort bzw. entsprechende Dokumente zu liefern oder auf die entsprechende offizielle Stelle zu verweisen. Generell gilt in einem solchen Fall, dass es nicht angebracht ist, in privaten Nachrichten derlei Inhalte zu teilen, und dass es zum anderen auch verboten ist, interne Unterlagen rauszuschicken.

Wählt der Spieler die Antwortmöglichkeit „inhaltliche Antwort liefern“ aus, bekommt er Minuspunkte und auch die entsprechende Erklärung. Wählt der Spieler die Antwortmöglichkeit „auf die offizielle Stelle verweisen“ aus, bekommt der Spieler Pluspunkte und auch die Erklärung, warum die andere Antwortmöglichkeit falsch gewesen wäre.

4. Zutritts- und Zugriffsschutz

Die Experten haben geäußert, dass Identitätsmanipulation eine der möglichen Methoden sein könnte, die Social Engineers in der Zukunft benutzen werden, und dass die Ausspionierung einzelner Mitarbeiter eins der wichtigsten Zukunftsthemen in Bezug auf Sicherheitsbedrohungen für Unternehmen sein könnte. Die Vermeidung der Identitätsmanipulation bezüglich eines Volkswagen-Mitarbeiters könnte u. a. als ein Manipulationsschutz im Rahmen des Volkswagen-IT-Systemschutzes verstanden werden. Daher erscheint es plausibel, das Thema Identitätsmanipulationsschutz im Spiel zu erwähnen und den Spieler für mögliche Identitätsmanipulationen zu sensibilisieren.

Eine weitere Konsolidierung der Ergebnisse der Gruppendiskussionen und Experteninterviews zeigt sich im nachfolgenden Spielsequenzbeispiel:

Für die Entwicklung des anstehenden Abschnitts wurden u. a. diese Kategorien aus der Gruppendiskussion benutzt: Kategorie I *„Transparenter Spielanfang als kurzes Video“*, Kategorie VI *„Realitätsnahe Spiele werden bevorzugt“*, Kategorie XI *„Ziele im Spiel sollen transparent sein“*, Kategorie XIII *„Gegner im Spiel motiviert“*, Kategorie II *„Aufgabenvielfalt fördert Interesse“*, Kategorie III *„Dynamische und unvorhersehbare Spielentwicklung ist interessefördernd“* und Kategorie V *„Offene Spielwelten mit gewissen Spielregeln sind interessefördernd“*.

Im Einführungsvideo in dieser Spielsequenz wird gezeigt, dass ein Kollege des Nutzers ins Büro kommt und vorschlägt, zusammen in die Kantine zu gehen. Dem Nutzer stehen die zwei Aktionsvorschläge „Aufstehen und rausgehen“ und „Computer sperren, aufstehen und rausgehen“ sowie ein leeres Feld, wo der Spieler seinen Aktionsvorschlag eintippen soll, zur Verfügung.

Laut den Informationssicherheitsrichtlinien ist es generell vorgeschrieben, dass die Beschäftigten der Volkswagen AG nicht nur ihren Laptop sperren, sondern auch ihre PKI-Karte mitnehmen sollen, wenn sie den Arbeitsplatz verlassen. Die PKI-Karte ermöglicht nicht nur einen physischen Zugang zu den Räumlichkeiten des Werkes, sondern auch digitalen Zugang zu verschiedenen Systemen, deswegen soll die PKI-Karte, die auch eine Art Ausweis ist, auf dem Werksgelände stets mitgeführt werden.

Wenn sich der Spieler in diesem Spielabschnitt für eins der Aktionsangebote entscheidet oder nicht die „PKI-Karte“ im leeren Feld erwähnt, sollen ihm Punkte abgezogen und eine Erklärung bereitgestellt werden, warum es ist nicht den Informationssicherheitsregeln entspricht, seine PKI-Karte nicht mitzunehmen.

3.3.3 Die Spielperspektive „Hacker“

Dadurch, dass das entwickelte Spiel nicht das Ziel verfolgt, detailliertes Wissen über Hacking und Social Engineering zu vermitteln, sondern der Zielgruppe zu zeigen und sie dafür zu sensibilisieren, dass für einen Angriff kein elaboriertes technisches und IT-Know-how benötigt wird, ist es empfehlenswert, das Storytelling im Serious Game bezüglich des Hackers kürzer zu halten und sich auf die nötigsten Elemente zu konzentrieren. Die Experten haben erwähnt, dass die folgenden Themen in Bezug auf Social Engineering wichtig sind und wichtig bleiben werden: Phishing und Passwortmanagement. Im Folgenden werden Beispiele für diese zwei Themen aus der Spielperspektive „Hacker“ anhand von Ergebnissen aus den Experteninterviews und Gruppendiskussionen konsolidiert und präsentiert.

1. Phishing

Die Experten sind der Meinung, dass die Nutzer die Merkmale einer Phishing-E-Mail erkennen können sollen, um kein Opfer von Social Engineers zu werden. Außerdem kamen in den Experteninterviews zwei Arten von Phishing-E-Mails zur Sprache: Spear-Phishing (personalisierte Phishing-E-Mail) und Phishing-Welle (unpersonali-

sierter Angriff). Daher soll innerhalb des Spiels zum Thema Phishing-Angriff aus der Perspektive eines Social Engineers sensibilisiert werden.

Die folgenden Kategorien wurden bei der Entwicklung dieser Spielsequenz benutzt: Kategorie I *„Transparenter Spielanfang als kurzes Video“*, Kategorie VI *„Realitätsnahe Spiele werden bevorzugt“*, Kategorie XI *„Ziele im Spiel sollen transparent sein“*, Kategorie XIII *„Gegner im Spiel motiviert“*, Kategorie II *„Aufgabenvielfalt fördert Interesse“*, Kategorie III *„Dynamische und unvorhersehbare Spielentwicklung ist interessefördernd“*, Kategorie V *„Offene Spielwelten mit gewissen Spielregeln sind interessefördernd“*, Kategorie XIV *„Hintergrundgeschichte fördert Interesse“*, Kategorie XV *„Wenige Avatar-Auswahloptionen werden bevorzugt“*, Kategorie XVI *„Selbstidentifikation mit Avatar ist wichtig“*, Kategorie VIII *„Transparentes Belohnungssystem“*, Kategorie IX *„Das Spiel soll verschiedene Genres inkludieren“*, Kategorie X *„Quiz als Spielgenre“* und Kategorie XVII *„Zeitdruck motiviert“*.

Nachdem der Spieler sich für die Spielperspektive „Hacker“ entschieden und den Avatar personalisiert hat, wird der Spieler aufgefordert, einen Unternehmensbereich oder eine konkrete Person zu hacken. Seine erste Aufgabe ist es, eine Phishing-E-Mail zu erstellen. Zu Anfang soll es ein kurzes Video über die verschiedenen Arten des Phishings geben: Phishing-Welle und Spear-Phishing. Außerdem soll dem Spieler erklärt werden, welche Merkmale eine Phishing-E-Mail hat. Die Punktevergabe erfolgt anhand einer Wissensabfrage zum Thema Phishing (z. B. eine unpersönliche Anrede in der E-Mail, verdächtige Links etc.). Ergänzend muss der Spieler die Aufgaben unter Zeitdruck beantworten.

2. Passwortmanagement

Die Experten sind der Meinung, dass Passwortmanagement ein wichtiges Thema im Kontext des Social Engineerings ist. Nutzer sollten nicht die gleichen Passwörter für verschiedene Systeme einsetzen, um zu vermeiden, Opfer von Social Engineering zu werden. Social Engineers erhalten zudem viele private Informationen aus den sozialen Medien. Daher können diese beiden Themen in der Spielsequenz Passwortmanagement konsolidiert werden.

Die folgende Kategorien wurden für diese Spielsequenz berücksichtigt: Kategorie XI *„Ziele im Spiel sollen transparent sein“*, Kategorie XIII *„Gegner im Spiel motiviert“*, Kategorie II *„Aufgabenvielfalt fördert Interesse“*, Kategorie III *„Dynamische und unvorhersehbare Spielentwicklung ist interessefördernd“*, Kategorie V *„Offene Spielwelten mit gewissen Spielregeln sind interessefördernd“*, Kategorie XIV *„Hintergrundgeschichte fördert Interesse“*, Kategorie XV *„Wenige Avatar-Auswahloptionen werden bevorzugt“*, Kategorie XVI *„Selbstidentifikation mit Avatar ist wichtig“*, Kategorie VIII *„Transparentes Belohnungssystem“*, Kategorie IX *„Das Spiel soll verschiedene Genres inkludieren“* und Kategorie XVII *„Zeitdruck motiviert“*.

Der Spieler wird aufgefordert, einen Zugang zu drei Accounts von verschiedenen Personen zu bekommen. Dazu stehen ihm private Profile von den jeweiligen Personen aus unterschiedlichen sozialen Medien und Networking-Plattformen (Facebook,

LinkedIn) zur Verfügung, die er als Hilfestellung benutzen kann. Die Punktvergabe erfolgt anhand richtig oder falsch erratener Passwörter.

Am Ende der Spielsequenz soll es ein kurzes Video geben, was den Spieler dazu motiviert, die andere Spielperspektive auszuprobieren und zu versuchen, dem Nutzer zu helfen, nicht gehackt zu werden. Dies entspricht auch den Ergebnissen der Gruppendiskussionen (Kategorie XIX *„Spannendes Spielende"*).

3.4 Reflexion der Erhebungs- und Auswertungsmethoden

Im Rahmen dieser Arbeit wurde die Zielgruppe der jungen Erwachsenen in die Spielentwicklung in Form von Gruppendiskussion mit einbezogen. So konnten wertvolle Meinungen bezüglich der Spielcharakteristiken gesammelt werden. Die Schwerpunkte für das bei Volkswagen entwickelte Spiel wurden anhand von drei Experteninterviews zusammengestellt. In diesem Kapitel sollen die in dieser Arbeit angewendeten Erhebungsmethoden Gruppendiskussion und Experteninterviews kritisch betrachtet werden. Außerdem sollen die Auswertungsmethoden reflektiert werden.

Ein Gruppendiskussionsverfahren hat nach Kruse (2015, S. 196 in Anlehnung an Kelle, 2007; Seipel & Rieker, 2003) unterschiedliche Einsatzmöglichkeiten und kann sowohl als ein eigenständiges als auch als ein komplementäres Erhebungsverfahren dienen. Wie bereits beschrieben, ist es mit dieser Methode möglich, Einstellungen und Meinungen einer Gruppe mit ihren Gemeinsamkeiten und Unterschieden zu erheben und zu analysieren.

Der Vorteil einer Gruppendiskussion liegt nach Pfeiffer (2023) darin, dass sie eine effiziente Methode ist, um qualitative Daten zu sammeln, da hierbei alle Teilnehmenden gleichzeitig befragt werden. Außerdem gibt Pfeiffer an, dass Gruppendiskussionen sich gut für einen Einstieg in neue Themen eignen. Auch sensible Themen können besser in einer Gruppendiskussion angesprochen werden, wenn die Teilnehmer ähnliche Erfahrungen teilen.

Littig und Wallace merken trotzdem in ihrer Studie über Möglichkeiten und Grenzen von Gruppendiskussionen für die sozialwissenschaftliche Forschung an, dass bei Gruppendiskussionen keine „natürlichen" Daten generiert werden können, da die Gruppendiskussion, die zudem noch von einem Moderator geführt wird, nur „[...] Hinweise auf ‚natürliche' Unterhaltungen oder Interaktion bietet, sie aber keinesfalls nachstellen kann" (Littig & Wallace, 1997, S. 9). Zusätzlich beschreiben die Autoren in ihrer Studie, dass auch kritisch zu betrachten ist, inwiefern die Gruppendiskussionsteilnehmer ehrlich und offen antworten oder sich lieber zurückhalten (Littig & Wallace, 1997). Zudem sind auch die Interpretationen und Interaktionen des Moderators während der Gruppendiskussion zu berücksichtigen. Ein weiterer möglicher Nachteil der Gruppendiskussion ist vor allem, dass das Risiko besteht, dass sie durch einige Teilnehmer dominiert wird und somit keine Gruppendynamik aufkommt, wodurch der gewünschte Austausch nicht zustande kommt (Littig & Wallace, 1997). Die

Koordination des Gesprächsablaufes ist daher elementar, um die Diskussion richtig zu leiten (Littig & Wallace, 1997).

Die Gruppendiskussion, so Littig und Wallace (1997, S. 9 in Anlehnung an Turner, 1990; Jameson, 1991; Kumar, 1995), eignet sich trotzdem als Methode für die Aufnahme der Kommunikation „[...] in postmodernen Gesellschaften, in denen Meinungen und Einstellungen als sozial konstruiert, fragmentiert und ephemer angesehen werden". Sie gilt als eine geeignete Methode, das Zustandekommen von Meinungen oder Meinungswechsel innerhalb von Gruppen aufzunehmen und abzubilden (Littig & Wallace, 1997). Da eins der Ziele der vorliegenden Arbeit darin besteht, die Meinung einer großen heterogenen Gruppe zu einem kontroversen Thema zu erheben, wird die Methode der Gruppendiskussion den Intentionen dieser Studie gerecht.

Die Gruppendiskussionen wurden nach der qualitativen Inhaltsanalyse nach Mayring (2015) ausgewertet (siehe Kapitel 3.1.2 und 3.1.3).

Nach Kruse (2015, S. 401 ff.) stößt die Methode jedoch an ihre Grenzen. So hebt Kruse hervor, dass sich die qualitative Inhaltsanalyse zu wenig auf das, „wie etwas gesagt wurde", konzentriert, und zu viel auf das, „was gesagt wurde". Das „wie etwas gesagt wurde" zu verstehen, ist aber notwendig, um dann später die „was gesagt wurde"-Aussagen rekonstruieren zu können. Denn nur zusammen mit der Analyse der Art und Weise, wie konkrete Aussagen getätigt wurden, kann eine Interpretation des dokumentierten Bedeutungssystems formuliert werden (Kruse, 2015, S. 401). Die Auswertung nach Mayring beginnt in der Regel mit einer Paraphrasierung des Originaltextes. Allerdings weist Kruse (2015, S. 404) hier auf ein weiteres Problem der qualitativen Inhaltsanalyse hin: nämlich dass „bloßes Konstatieren des bereits Vorhandenen" vollzogen oder bereits in der Paraphrase implizit interpretiert wird. Außerdem betont Kruse (2015, S. 406), dass ein Kategoriensystem im Laufe der Analyse zu einem „dogmatischen Regelwerk" mutiert und den Analyseprozess vollständig dominiert. Die induktive Kategorienbildung ist zudem nach Kruse (2015, S. 409) auch weniger induktiv, sondern eher „tautologisch-zirkulär", da hierbei vom Forscher bereits starke Setzungen am Material vorgenommen werden. Als schwierig erweist sich darüber hinaus, dass das Material bei der Analyse auf der Äußerungsebene und nicht auf der Sinnebene rekonstruiert wird. Nichtdestotrotz kommt Kruse (2015, S. 410 in Anlehnung an Garfinkel, 1967; Cicourel, 1975; Sacks, 1992; Schegloff, 1984; Mayring, 2008, S. 29 ff., 34 ff., 51) zu dem Schluss, dass die Inhaltanalyse pragmatisch ist, da sprachkommunikative Sinnproduktion auf lexikalische Ausdrücke reduziert wird.

Nach Mayring (2015, S. 131) liegt die Stärke dieser Methode darin, eine große Menge an Daten systematisch und regelgeleitet bearbeiten zu können. Wenn jedoch diese Vorgehensweise aufgrund von Gegenstand oder Fragestellung nicht angemessen erscheint, sollte eine andere Auswertungsmethodik angewendet werden. Mayring (2015) betont auch, dass die Auswertungsmethode nicht unflexibel sein und zudem auf die konkrete Forschungsfrage ausgerichtet werden sollte.

Nach Liebold und Trinczek (2009, S. 53) bieten Experteninterviews dank ihrer Prozesshaftigkeit, Kommunikation und Flexibilität die Möglichkeit, nicht nur in weniger erforschten Bereichen Erkenntnisgewinne zu liefern, sondern auch da, wo bereits Vor-

wissen etabliert ist. Nichtdestotrotz sehen sie bei Experteninterviews gewisse Problematiken, die sowohl im Forschungsdesign als auch in einer Interviewsituation bedacht werden müssen. Liebold und Trinczek (2009, S. 54) nennen einen wichtigen Faktor für die Durchführung von Gruppendiskussionen, nämlich inhaltliche und soziale Kompetenz aufseiten des Interviewers. Nur durch sie kann sichergestellt werden, dass der Interviewer vor einem Experten als ein akzeptierter „Fragekommunikator" erscheint. Gleichzeitig soll ein „Expertenduell" in der Interviewsituation jedoch unbedingt vermieden werden, wenn der Interviewer Detailkenntnisse ins Gespräch mit einfließen lässt. Außerdem soll der Expertenstatus eines Experten nicht dazu führen, dass eine Trennung zwischen Person und Experte existiert, da eine gewisse Expertise „grundsätzlich nur über die Person und deren Erfahrungshintergrund zugänglich ist" (Liebold & Trinczek, 2009, S. 54).

Was die Leistungen und Grenzen von Experteninterviews betrifft, existiert in der Literatur die etablierte Ansicht, dass die Methode „Experteninterview" einen Überblick über die Insiderinformationen und Erfahrungen spezifischer Gruppen liefern kann und damit eine „[...] privilegierte Problemsicht" (Liebold & Trinczek, 2009, S. 53) ermöglicht. Daher wurden die Experteninterviews in dieser Arbeit durchgeführt, um wertvolle Einsichten und Erkenntnisse der speziellen internen Expertengruppe zu bekommen.

Die Experteninterviews wurden nach Meuser und Nagel (2009) ausgewertet. Nach Kruse (2015, S. 172 in Anlehnung an Bogner & Menz, 2005, S. 34 ff.) stellen Meuser und Nagel ihre Methode als ein offen-rekonstruktives Verfahren vor, bei genauerer Betrachtung ähnelt sie aber der Inhaltsanalyse nach Mayring und hat somit die gleichen Grenzen wie die Inhaltsanalyse, die bereits in diesem Kapitel reflektiert wurde.

4 Quantitative Studie

Obwohl für das Forschungsvorhaben die Entwicklung, Erprobung und empirische Evaluation der didaktischen Konzeption des Serious Games Volkswagen AG-Spiel vereinbart und genehmigt worden sind, führten die unerwartet auftretenden Einschränkungen infolge der Covid–19-Pandemie zu einer Veränderung des Vorhabens. Die tatsächliche Entwicklung des Serious Games wurde im März 2020 geplant. Allerdings wurde durch das Unternehmen später im Rahmen von Budgetveränderungen entschieden, die Entwicklung des Spiels vorerst zu stoppen. Um dennoch mit dem Forschungsdesign fortzufahren und die Forschungsfragen empirisch bearbeiten zu können, wurde in Übereinstimmung mit dem Hochschulbetreuer der Dissertation die Entscheidung getroffen, Alternativen für die Durchführung der empirischen Studie zu prüfen.

Wesentliches Ziel der folgenden Studie war die empirische Untersuchung der Frage, inwiefern eine spielerische Awareness-Maßnahme im Vergleich oder in Ergänzung zur klassischen Unterweisung die Informationssicherheits-Awareness fördert. Hierzu wurde entschieden, die empirische Studie mit der Awareness-Maßnahme „Security Arena“ fortzuführen. Daher kommt – trotz der daraus folgenden Veränderungen im Forschungsdesign und der Einschränkungen der Aussagekraft der empirischen Ergebnisse – in der im folgenden Kapitel vorgestellten quantitativen Studie ein verändertes didaktisches Konzept anstatt des in dem vorliegenden Kapitel bearbeiteten Serious Games zum Einsatz.

Die quantitative Studie zur Evaluation einer spielerischen Awareness-Sensibilisierung ist eine Vergleichsstudie zwischen dem Trainingskonzept „Security Arena“ und einer traditionellen Unterweisung. In den folgenden Kapiteln wird eine im Rahmen des Vorhabens entwickelte Konzeption vorgestellt, mit der Informationssicherheits-Awareness-Aspekte (Wissen, Einstellung und Verhalten) auf Effizienz und Nachhaltigkeit getestet werden können.

Zunächst wird die forschungsmethodische Ausgestaltung der empirischen Studie beschrieben. Dafür wird ein hypothesenprüfender Forschungsansatz eingesetzt. Dieser wird genutzt, um die zuvor im Rahmen qualitativer Forschung entwickelte Konzeption empirisch zu überprüfen und im Gesamtkontext auszuwerten. Anschließend erfolgt die Zusammenführung der Ergebnisse. Durch die Betrachtung der Gesamtheit der Daten werden Gemeinsamkeiten und Unterschiede zwischen den erhobenen Datenarten sowie Auffälligkeiten ermittelt und interpretiert.

Nach der Vorstellung des Designs sowie des für die Auswertung eingesetzten Strukturgleichungsmodells werden die Entwicklung des eingesetzten Fragebogens sowie der Erhebungszeitraum und die deskriptive Statistik des Datensets eruiert. Danach werden die Ergebnisse der Auswertung der Mess- und Strukturmodelle vorgestellt. Die quantitative Studie endet mit der Diskussion und Interpretation der Ergebnisse.

4.1 Vorgesehene und angewendete Sensibilisierungsmaßnahmen

Im Folgenden wird beschrieben, wie sich das zunächst vorgesehene Serious Game Volkswagen AG-Spiel von den bei der Volkswagen AG existierenden alternativen Maßnahmen Security Arena und klassische Unterweisung unterscheidet. Der Vergleich soll nicht nur anhand von Themen der Informationssicherheits-Awareness erfolgen, sondern auch anhand von Ergebnissen aus den Gruppendiskussionen.

Serious Game Volkswagen AG-Spiel

Das Konzept des Serious Games Volkswagen AG-Spiel bietet die Möglichkeit, eine große Zielgruppe online für Sicherheitsproblematiken zu sensibilisieren, was insbesondere in Zeiten von vermehrtem Homeoffice nützlich ist. Die Kosten pro Person hängen hier vom Einsatz des technischen und des IT-Supports ab. Ein Serious Game im Rahmen von Sicherheits-Awareness-Maßnahmen ist eine interaktive Methode, bei der die Teilnehmer nicht nur verschiedene Perspektiven (Nutzer und Hacker) ausprobieren, sondern selber Entscheidungen z. B. unter Zeitdruck treffen und die Themeninhalte von verschiedenen Blickwinkeln betrachten. Bei Volkswagen AG-Spiel werden die folgenden Themen bearbeitet: Phishing, Umgang mit (mobilen) Speicher- und Endgeräten, soziale Medien, Zutritts- und Zugriffsschutz, Passwortmanagement und der Umgang mit Informationen u. a. im Kontext mobiler Arbeit. Bei der didaktischen Spielentwicklung wurden alle Kategorien aus den Gruppendiskussionen bis auf Kategorie XII *„Multiplayer-Spiele sind interessefördernd"* implementiert. Aufgrund von begrenzten technischen Möglichkeiten ist es allerdings herausfordernd, auf der internen Volkswagen-Lernplattform ein Spiel einzusetzen, das gleichzeitig für mehrere Nutzer online zur Verfügung steht.

Security Arena

Die Security Arena bietet die Möglichkeit, parallel bis zu 80 Personen für Sicherheits-Awareness-Inhalte zu sensibilisieren. Die Kosten für diese Art der Awareness-Maßnahme resultieren aus dem Einsatz der internen Moderatoren für jedes Spiel, den Veranstaltungskosten und dergleichen. Im Gegensatz zum Volkswagen AG-Spiel ist die Security Arena eine Veranstaltung, die nicht online angeboten wird. Dennoch können den Teilnehmern im Rahmen der Security Arena ebenfalls wichtige Themen der Informationssicherheits-Awareness nähergebracht werden, da sie über die gleichen Spieleinhalte (also über die wichtigsten 5 Kontexte: E-Mail-Bearbeitung, Passwortmanagement, Umgang mit (mobilen) Speicher- und Endgeräten, Zutritts- und Zugriffsschutz und Umgang mit Informationen u. a. im Kontext mobiler Arbeit) verfügt (siehe Kapitel 2.3).

Im Vergleich zum Volkswagen AG-Spiel hat die Security Arena keine Onlinespielcharakteristiken wie Grafik, Avatar, Videospielanfang und kann damit auch nicht beispielsweise im Homeoffice bearbeitet werden. Darüber hinaus kann sie nicht die folgenden Kategorien aus der Gruppendiskussionen inkludieren: Kategorie I *„Transpa-*

renter Spielanfang als kurzes Video", Kategorie VII *„Realitätsnahe Grafik wird bevorzugt"*, Kategorie XII *„Multiplayer-Spiele sind interessefördernd"*, Kategorie XV *„Wenige Avatar-Auswahloptionen werden bevorzugt"* sowie Kategorie XVI *„Selbstidentifikation mit Avatar ist wichtig"*.

Allerdings bietet die Security Arena besondere Rahmenbedingungen: Die Spieler müssen in kleinen Gruppen von 5 bis 8 Personen verschiedene Aufgaben lösen. Dabei spielen sie zusammen gegen andere Spielergruppen und haben durch Rotation von Spielstation zu Spielstation die Möglichkeit, diverse Spielaufgaben auszuprobieren. Jedes Spiel soll in 10 bis 15 Minuten gelöst werden, dafür erhalten die Spieler eine Anweisung und eine Beschreibung des Belohnungssystems vom jeweiligen Moderator. Dies entspricht folgenden Kategorien aus der Gruppendiskussionen: Kategorie II *„Aufgabenvielfalt fördert Interesse"*, Kategorie III *„Dynamische und unvorhersehbare Spielentwicklung ist interessefördernd"*, Kategorie IV *„Entscheidungsmöglichkeiten im Spiel sind motivierend"*, Kategorie VI *„Realitätsnahe Spiele werden bevorzugt"*, Kategorie VIII *„Transparentes Belohnungssystem"*, Kategorie IX *„Das Spiel soll verschiedene Genres inkludieren"*, Kategorie X *„Quiz als Spielgenre"*, Kategorie XI *„Ziele im Spiel sollen transparent sein"*, Kategorie XIII *„Gegner im Spiel motiviert"*, Kategorie XIV *„Hintergrundgeschichte fördert Interesse"*, Kategorie XVII *„Zeitdruck motiviert"*, Kategorie XVIII *„Möglichkeit, untypische Rollen auszuprobieren"*.

Die Messung des Gelernten erfolgt anhand der Vergabe von Punkten nach dem Spiel. Die fünf Kontexte aus den Gruppendiskussionen, die für die inhaltliche Entwicklung des Volkswagen AG-Spiels vorgesehen sind (E-Mail-Bearbeitung, Passwortmanagement, Umgang mit (mobilen) Speicher- und Endgeräten, Zutritts- und Zugriffsschutz und Umgang mit Informationen u. a. im Kontext mobiler Arbeit), wiederholen sich im Kontext der Security Arena. Da im Laufe der weiteren empirischen Untersuchungen die Spielentwicklung von Volkswagen AG-Spiel noch nicht fortgeführt werden konnte, schien es sinnvoll, die fünf Kontexte in spielerischer Umgebung zu testen und eine sogenannte Pilotversion der Awareness-Messung zu überprüfen. Ziel der in diesem Kapitel folgenden empirischen Studie ist die Untersuchung, inwiefern eine spielerische Awareness-Methode die Sicherheits-Awareness bei den Nutzern fördert und inwiefern die von den Interviewten genannten Wünsche für eine spielerische Awareness-Methode neue und gewinnbringende Elemente zur Awareness-Steigerung mit einbringen.

Unterweisung

An der bislang im Unternehmen üblichen Unterweisung können parallel bis zu 60 Personen teilnehmen. Die Unterweisung kann online und offline stattfinden. Allerdings ist die Unterweisung eine reine Übertragung von Informationen an die Teilnehmer und hat nicht den spielerischen Charakter wie Volkswagen AG-Spiel oder die Security Arena.

Die Teilnehmer können im theoretischen Kontext zu denselben Themen wie im Rahmen der Security Arena und Volkswagen AG-Spiel sensibilisiert werden. Auf Grundlage der bislang vorliegenden Erkenntnisse muss jedoch davon ausgegangen

werden, dass angesichts der didaktischen Limitationen der Unterweisung nachhaltige Verhaltensänderungen nicht oder nur eingeschränkt erreicht werden.

Es steht daher im Fokus der weiteren Forschung, zu untersuchen, ob und in welchem Umfang die alternativen didaktischen Vorgehensweisen im Vergleich zu der bislang eingesetzten Unterweisung zu einer nachhaltigen Verhaltensänderung beitragen.

4.2 Forschungsmethodisches Desiderat

Wie bereits in den theoretischen Grundlagen angedeutet wurde (Kapitel 2.2), existieren in der Forschung bezüglich Informationssicherheits-Awareness theoretische Ansätze, auf deren Grundlage Informationssicherheits-Awareness erklärt bzw. gemessen werden kann. Sowohl das Messmodel von Parson et al. (2014) als auch die Modelle von Parsons et al. (2017) und Endsley (1995) sowie die Theorie des geplanten Verhaltens nach Ajzen (Graf, 2007, S. 34 in Anlehnung an Ajzen, 1985, 2005, 2006; Ajzen & Madden, 1986) beschreiben die Korrelation zwischen Wissen, Einstellung und Verhalten. Jedoch bleibt darin stets offen, inwiefern z. B. individuelle oder organisatorische Faktoren Wissen, Einstellung und Verhalten beeinflussen. Zusätzlich wurden in Kapitel 2.2 die sieben Schwerpunkte der HAIS-Q-Studie (Internetnutzung, E-Mail-Nutzung, Nutzung sozialer Netzwerke, Passwortmanagement, Zutritts- und Zugriffsschutz, Informationsverarbeitung und mobiles Arbeiten) nach Parson et al. (2014) als voneinander abgetrennte Modelle vorgestellt. Auch hier bleibt ungeklärt, ob und wie Wissen, Einstellung und Verhalten innerhalb dieser sieben Schwerpunkte einheitlich bleiben oder einander beeinflussen. Als einschränkend ist anzumerken, dass die HAIS-Q-Studie von Parsons et al. (2014) innerhalb mehreren australischen Organisationen in 2013 durchgeführt wurde, weshalb fraglich ist, inwiefern sie für weitere Branchen wie die Automobilindustrie in Deutschland in diesem Kontext aktuell noch relevant ist.

Das HAIS-Q-Studie liefert des Weiteren keine Informationen dazu, wie Informationssicherheits-Awareness gesteigert werden könnte und welche Maßnahmen eingesetzt werden sollten, um das Niveau der Informationssicherheits-Awareness der Beschäftigten nachhaltig zu verbessern. Eine Überprüfung der Wirksamkeit der theoretischen Mechanismen der Theorie im Zeitverlauf (beispielsweise im Rahmen einer Längsschnittstudie) fehlt bisher.

Aus diesem Forschungsdesiderat ergibt sich folgende Fragestellung, die Gegenstand der weiteren Untersuchung wird: Wie könnte die Informationssicherheits-Awareness gesteigert werden und welche Maßnahmen sind dazu geeignet? Außerdem bleibt die Frage der Überprüfung der Wirksamkeit der theoretischen Mechanismen bis jetzt offen. Raithel (2006, S. 24 f. in Anlehnung u. a. an Atteslander, 2003, S. 22; Baur & Fromm, 2004, S. 14; Diekmann, 2005, S. 166 f.; Schnell, Hill & Esser, 2005, S. 8; Schöneck & Voß, 2005, S. 17) beschreibt folgenden Ablauf für eine empirische Untersuchung:

1. Problemformulierung
2. Konzeptualisierung

3. Erhebungsvorbereitung und Datenerhebung
4. Datenaufbereitung
5. Datenanalyse
6. Interpretation und Dissemination

In der ersten Phase soll das Forschungsproblem klar definiert werden (Raithel, 2006, S. 26). Raithel gibt an, dass es an dieser Stelle notwendig ist, eine definierte Fragestellung auszuarbeiten, und dass die Hypothesen ausformuliert sein müssen.

In der Konzeptualisierungsphase sollen nicht nur das Erhebungsinstrument, sondern auch Stichprobe, Institutionen und der zeitliche Aspekt der Untersuchung definiert werden. Die Konzeptualisierungsphase für diese Studie wird in den weiteren Kapiteln detaillierter präsentiert und ausdiskutiert.

Im dritten Schritt „Erhebungsvorbereitung und Datenerhebung" sollen alle Vorbereitungen der Feldphase erfolgen. Dazu gehören Terminplanungen, Genehmigungen und die Einwilligungen, die dokumentiert werden sollen. Raithel (2006, S. 28) betont, dass die konkrete Durchführung in möglichst kürzester Zeit erfolgen soll „[...] um Entwicklungseffekte zu vermeiden und die Wahrscheinlichkeit einschneidender äußerer Ereignisse, deren Einfluss die Ergebnisse der Untersuchung beeinträchtigen können, möglichst gering zu halten". Vertiefende Informationen zur dritten Phase werden in den weiteren Kapiteln näher beleuchtet.

Im vierten Schritt nach Raithel (2006) sollen die Daten entsprechend für die weiterführende Analyse und die danach folgende Interpretation vorbereitet werden. In dieser Phase erfolgt auch die Fehler- und Datenbereinigung, indem die Daten auf Vollständigkeit und Plausibilität überprüft werden. Die Datenaufbereitung in dieser Studie wird zu einem späteren Zeitpunkt weiterführend erläutert.

Erst nachdem die Daten vorbereitet sind, soll nach Raithel (2006, S. 28) im fünften Schritt mit der tatsächlichen Datenanalyse begonnen werden, wobei er betont, dass es notwendig ist, die Frage der Analysemethoden schon bei der Entwicklung des Erhebungsbogens mitzudenken, um eine statistische Prüfung effizienter zu gestalten. Erst danach kommt die abschließende Disseminationsphase, wo sowohl die Ergebnisse als auch deren Interpretation vorgestellt werden. Raithel (2006, S. 29 in Anlehnung an Friedrichs, 1990, S. 120) beschreibt diese Phase als besonders intellektuell anspruchsvoll, denn die Ergebnisse werden mit den Fragestellungen und Hypothesen konfrontiert und schlussendlich basierend auf dem Vergleich interpretiert. In späteren Kapiteln soll eine Präsentation der Datenanalyse und der Interpretation der Ergebnisse erfolgen. Im weiteren Verlauf werden nun aber zunächst die Problemformulierung, die Forschungsfragen und die daraus hergeleiteten Hypothesen beschrieben.

4.3 Untersuchungsdesign

4.3.1 Untersuchungsfrage und -hypothesen

Die theoretisch hergeleiteten Hypothesen sollen empirisch überprüft werden (vgl. Pelz, 2008). Um dies zu ermöglichen, soll eine passende Forschungsmethode ausgewählt werden (vgl. Raithel, 2006). Für diese Studie wurde eine deduktive Vorgehensweise ausgewählt, was bedeutet, dass die theoretischen Hypothesen aus einem bestehenden theoretischen Desiderat abgeleitet wurden und anhand von konkreten Fällen überprüft werden sollen – mit dem Ziel, eine systematische Bestätigung oder eine Wiederlegung der ursprünglichen Theorie zu bekommen (vgl. Malzew, 2023). Um die Anforderungen einer deduktiven Vorgehensweise zu erfüllen, bietet sich nach Malzew (2023) ein quantitativer Forschungsansatz an. Quantitativ wird immer in den Forschungsbereichen geforscht, wo bereits etablierte Theorien existieren, allerdings zusätzliche statistisch relevante Erkenntnisse benötigt werden (Malzew, 2023). Eins der Ziele dieser Art der Forschung ist es, kausale Zusammenhänge möglichst präzise zu messen und dann die Ergebnisse auf eine größere Allgemeinheit hin zu interpretieren (Malzew, 2023).

Der Fokus der Kausalanalyse ist die Überprüfung der Ursache-Wirkungsbeziehung zwischen Sachverhalten (Weiber & Mühlhaus, 2014). Weiber und Mühlhaus (2014, S. 10 nach Cook & Campbell, 1979, S. 31) beschreiben, dass ein Kausalzusammenhang zwischen den Sachverhalten (zwischen einer verursachten Größe und der durch sie erzeugten Wirkung) dann gegeben ist, wenn folgende Bedingungen erfüllt sind:

1. Veränderungen in der verursachten Größe (unabhängige Variable) führen zu Veränderungen in der danach folgenden Wirkung (abhängige Variable).
2. Veränderungen in der abhängigen Variable sollen zeitlich nach den Veränderungen in der unabhängigen Variable vorliegen.
3. Eine unabhängige Variable soll die einzige plausible Erklärung für die Veränderung der abhängigen Variable darstellen (zu bedenken ist hierbei jedoch, dass sich der Einfluss aller möglichen Ursachen auf eine Wirkung in der Realität nur sehr schwer kontrollieren lässt).

Malzew (2023) beschreibt, dass bei einem quantitativen Ansatz standardisierte Umfragen oder Beobachtungen durchgeführt werden, um möglichst eine große Datenmenge zu erhalten. Folglich sollen auch im Rahmen dieser Arbeit anhand von standardisierten Umfragen die Daten gesammelt werden, die schlussendlich dazu dienen, die Forschungsfragen zu beantworten.

Ein Ziel dieser Studie ist, wie beschrieben, herauszufinden, inwiefern Awareness-Aspekte (Wissen, Einstellung und Verhalten) in Informationssicherheits-Awareness-Kontexten (E-Mail-Bearbeitung, Passwortmanagement, Umgang mit (mobilen) Speicher- und Endgeräten, Umgang mit Informationen u. a. im Kontext mobiler Arbeit, Zutritts- und Zugriffsschutz) miteinander korrelieren und eventuell voneinander ab-

hängig sind. In den weiteren Kapiteln wird das methodische Vorgehen detaillierter beschrieben.

Aus den in Kapitel 4.2 aufgeführten Punkten ergeben sich die Forschungsfragen für die quantitative Studie, um die schon bei der Volkswagen AG existierenden Awareness-Maßnahmen (Security Arena und Unterweisung) zu messen und zu überprüfen, ob die Awareness-Elemente (Wissen, Einstellung und Verhalten) sich innerhalb verschiedener Kontexte bei den Probanden nach der Unterweisung und nach der spielerischen Interaktion (Security Arena) verändern. Daraus lassen sich die nun anschließenden beiden Forschungsfragen (zu Forschungsfrage 1 s. qualitativer Teil dieser Arbeit) schlussfolgern:

2. Wie kann Informationssicherheits-Awareness gemessen werden?
Diese Forschungsfrage enthält die Zielsetzung, eine Messung der Informationssicherheits-Awareness zu entwickeln und durchzuführen. In den weiteren Kapiteln wird aufgezeigt werden, inwiefern dies anhand einer entwickelten Prüfmethode erfolgen kann.

3. Wie effektiv und nachhaltig für die Förderung von Awareness-Aspekten (Wissen, Einstellung und Verhalten) ist das Konzept „Serious Games" zusätzlich zur klassischen Unterweisung? Inwiefern korrelieren die drei Awareness-Aspekte jeweils miteinander?
Diese Forschungsfragen enthalten die Zielsetzung, das Konzept „Serious Games" und den Einsatz einer klassischen Unterweisung zu überprüfen. Hierzu sollen besagte Awareness-Maßnahmen durchgeführt und anhand eines Tests mit der Zielgruppe überprüft werden. Das Ziel ist, dass nach der Durchführung dieser Awareness-Maßnahmen die Informationssicherheits-Awareness der jungen Erwachsenen steigt. Nach den internen Richtlinien der Volkswagen AG sollen alle Beteiligten dieser Studie bei der Durchführung der Awareness-Maßnahmen die gleiche Grundsensibilisierung erhalten. Demnach wurde entschieden, dass alle Beteiligten eine Grundsensibilisierung zum Thema Informationssicherheit anhand einer Unterweisung bekommen und dass die spielerische Awareness-Maßnahme mit einer separaten Kontrollgruppe getestet wird, die schon an einer Grundsensibilisierung teilgenommen hat.

Um die Nachhaltigkeit der beiden Methoden zu testen, wurde beschlossen, die Experimente in einem Zeitverlauf (vom 17.08.2020 bis 21.10.2020) durchzuführen. Um die Forschungsfrage 3 zu beantworten, wurden die folgenden Hypothesen entwickelt:

H1 *Die Informationssicherheits-Awareness* der jungen Erwachsenen der Volkswagen AG *verbessert sich* nach der Durchführung der spielerischen Awareness-Veranstaltung zusätzlich zur klassischen Unterweisung im Zeitverlauf.

H1.1 *Das Wissen* der jungen Erwachsenen der Volkswagen AG über die Informationssicherheit *verbessert sich* nach der Durchführung der spielerischen Awareness-Veranstaltung zusätzlich zur klassischen Unterweisung im Zeitverlauf.

H1.2 *Die Einstellung* der jungen Erwachsenen der Volkswagen AG zum Thema Informationssicherheit *verbessert sich* nach der Durchführung der spielerischen

Awareness-Veranstaltung zusätzlich zur klassischen Unterweisung im Zeitverlauf.

H1.3 Nach der Durchführung der spielerischen Awareness-Maßnahme zusätzlich zur klassischen Unterweisung *verhalten sich* die jungen Erwachsenen der Volkswagen AG *bewusster* gegenüber den Anforderungen der Informationssicherheit.

Zudem ist das mit der Forschungsfrage formulierte Ziel, herauszufinden, inwiefern die drei Aspekte der Informationssicherheits-Awareness miteinander korrelieren und einander eventuell beeinflussen. Dazu wurden die folgenden Hypothesen entwickelt, welche auf den theoretischen Ansätzen der HAIS-Q-Studie (basierend auf Parsons et al., 2014; Parsons et al., 2017) und auf den dem Modell zugrunde liegenden Hypothesen basieren, die allerdings auf diesen Forschungskontext angepasst wurden:

H2 *Einzelne Awareness-Bereiche korrelieren* miteinander und *haben einen Einfluss* aufeinander.

H2.1 *Das Wissen* hinsichtlich Informationssicherheitsregeln *beeinflusst die Einstellung* zu Informationssicherheitsregeln.

H2.2 *Die Einstellung* zu den Informationssicherheitsregeln *beeinflusst das Verhalten* gegenüber der Informationssicherheit.

H2.3 *Das Wissen* hinsichtlich Informationssicherheitsregeln *beeinflusst das Verhalten* gegenüber der Informationssicherheit.

H3 *Die Informationssicherheits-Awareness* der jungen Erwachsenen der Volkswagen AG *verbessert sich* nach der Durchführung der spielerischen Awareness-Maßnahmen zusätzlich zu einer klassischen Unterweisung in einzelnen Kontexten stärker als in anderen Kontexten (E-Mail-Bearbeitung, Passwortmanagement, Umgang mit (mobilen) Speicher- und Endgeräten, Umgang mit Informationen u. a. im Kontext mobiler Arbeit, Zutritts- und Zugriffsschutz) im Vergleich zu einer ausschließlich erfolgten Unterweisung.

Aus den Ergebnissen der Experteninterviews und der Literaturrecherche ergeben sich die besagten fünf Informationssicherheits-Awareness-Kontexte (E-Mail-Bearbeitung, Passwortmanagement, Umgang mit (mobilen) Speicher- und Endgeräten, Umgang mit Informationen u. a. im Kontext mobiler Arbeit, Zutritts- und Zugriffsschutz), anhand derer die Hypothesen überprüft werden. Ergänzend dazu verfügt die Security Arena über fünf Spiele zu den oben genannten Kontexten. Im weiteren Verlauf der Arbeit sollen die besagten fünf Kontexte und die dazugehörigen Informationssicherheits-Awareness-Aspekte (Wissen, Einstellung und Verhalten) näher betrachtet und analysiert werden.

Im nächsten Kapitel steht die Methode, mit der die Arbeitshypothesen überprüft werden, im Vordergrund.

4.3.2 Strukturmodell

Wie schon beschrieben wurde, liegt der Fokus der Kausalanalyse auf der Erforschung von Sachverhalten, die sich in einer abhängigen Relation zueinander befinden (Nitzl, 2010; Weiber & Mühlhaus, 2014).

Für die Operationalisierung der Kausalanalyse soll in erster Linie ein Konstrukt definiert werden, welches die Abhängigkeit zwischen den latenten Variablen abbildet, die sich einer direkten Beobachtung entziehen (Nitzl, 2010, S. 1 in Anlehnung an Backhaus et al., 2006b, S. 339 f.). Die latenten Variablen sollen wiederum auch operationalisiert werden, um schlussendlich messbar zu sein (Nitzl, 2010, S. 1 in Anlehnung an Backhaus et al., 2006b, S. 339 f.).

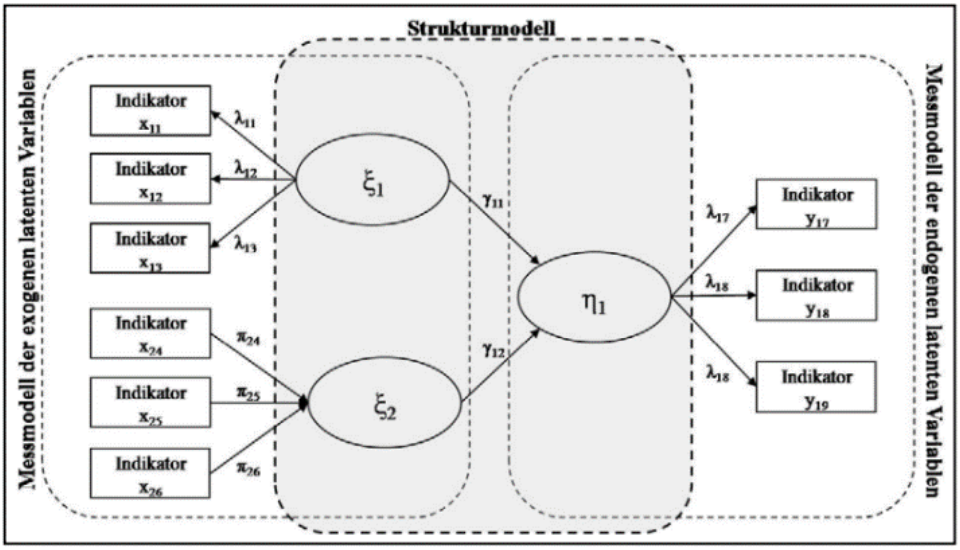


Abbildung 13: Beispielmodell mit zwei latenten Variablen (Nitzl, 2010, S. 4)

Abbildung 13 zeigt ein Beispielmodell mit Variablen. Regorz (2023) führt folgendes Beispiel für die Definition einer latenten Variable ein: Intelligenz als solches kann nicht direkt gemessen werden (und ist somit eine latente Variable), aber aus der Vielzahl der diversen Wissens-, Logik- und anderen Testergebnisse (den beobachteten Variablen) können ein oder mehrere Ergebnisse für die latente Variable „Intelligenz" extrahiert werden. Für das Forschungsdesign dieser Arbeit ergeben sich drei latente Variablen: Wissen, Einstellung und Verhalten.

Die HAIS-Q-Studie gibt vor, dass die Variable „Wissen" eine unabhängige Variable (exogene Variable) ist und die Variablen „Einstellung" und „Verhalten" abhängige (endogene) Variablen sind (Parson et al., 2014, S. 172). Gemäß den Hypothesen H2.1, H2.2 und H2.3 stehen diese drei Variablen in einem Zusammenhang zueinander und ergeben dann folgendes Strukturmodell (s. Abb. 14).

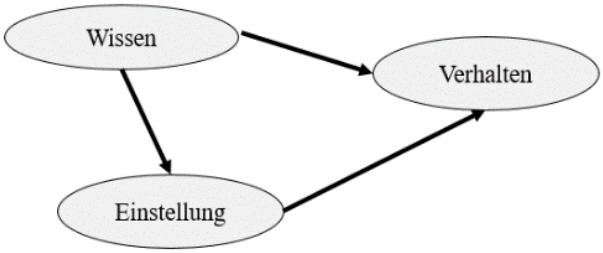


Abbildung 14: Allgemeines Strukturmodell zur Messung von Wissen/Einstellung/Verhalten bezüglich Informationssicherheits-Awareness (eigene Darstellung in Anlehnung an Parson et al., 2014, S. 169)

Das Strukturmodell lässt sich nun abschließend auf die fünf Kontexte, um die es in dieser Forschungsarbeit geht („E-Mail-Bearbeitung", „Passwortmanagement", „Umgang mit Informationen u. a. im Kontext mobiler Arbeit", „Umgang mit (mobilen) Speicher- und Endgeräten" und „Zutritts- und Zugriffsschutz"), anwenden.

4.3.3 Messmodell

Auf Basis des Strukturmodells wird nach Nitzl (2010, S. 3 in Anlehnung an Götz & Liehr-Gobbers, 2004, S. 716 ff.; Albers & Götz, 2006, S. 669) ein Messmodell entwickelt, mit dem das Strukturmodell operationalisiert wird. Für diese Studie soll das Messmodell die Indikatoren beinhalten, durch die separat das Wissen, die Einstellung und das Verhalten gemessen werden können.

Es wird zwischen formativen und reflektiven Messmodellen unterschieden (Nitzl, 2010, S. 5 in Anlehnung an Edwards & Bagozzi, 2000, S. 155; Eberl, 2004; Fassott & Eggert, 2005; Eberl, 2006; Diller, 2006, S. 613 f.; Fassott, 2006; Huber et al., 2007, S. 17; Weiber & Mühlhaus, 2010, S. 38). Die Indikatoren in einem formativen Messmodell werden als Ursprung von Veränderung in der latenten Variable interpretiert und die allgemeine Kausalrelation geht von Indikatoren zu einer latenten Variable (Nitzl, 2010, S. 7 in Anlehnung an Diamantopoulos, 1999, S. 446; Christophersen & Grape, 2007, S. 104). Darüber hinaus führen die Änderungen in den Indikatoren in einem formativen Messmodell zu Änderungen in der latenten Variable. Das heißt, dass sich Indikatoren in einem formativen Messmodell nicht unbedingt auf ein Thema beziehen und eine relativ geringe Korrelation zwischen einander haben können, im Vergleich zu einem reflektiven Messmodell und dessen Indikatoren (Nitzl, 2010, S. 9 in Anlehnung an Jarvis, MacKenzie & Podsakoff, 2003, S. 201). Außerdem kann die Elimination eines einzelnen Indikators des formativen Messmodells die Veränderungen der latenten Variable verursachen (Nitzl, 2010, S. 12 in Anlehnung an Fassott, 2006, S. 71). In einem reflektiven Messmodell führt die Kausalrelation von der latenten Variable hin zu den Indikatoren (Nitzl, 2010, S. 9 in Anlehnung an Diamantopoulos, 1999, S. 446; Christophersen & Grape, 2007, S. 104; Jarvis, MacKenzie & Podsakoff, 2003, S. 201). Die Indikatoren eines reflektiven Messmodells besitzen eine identische Ursache, sind austauschbar und verfügen somit über eine hohe Korrelation zwischen einander (Nitzl, 2010, S. 9 in Anlehnung an Jarvis, MacKenzie & Podsakoff, 2003, S. 201).

Jede latente Variable in einem Strukturmodell wird durch Indikatoren operationalisiert und besitzt somit ein eigenes Messmodell (Nitzl, 2010, S. 5 in Anlehnung an Ringle et al., 2006, S. 83). Das Auffinden der passenden Indikatoren, die das Konstrukt beschreiben, ist von großer Bedeutung, allerdings betont Nitzl (2010, S. 5 in Anlehnung an Anderson, Gerbing & Hunter, 1987, S. 432), dass die Indikatoren möglichst eindimensional sein sollten. Das bedeutet, dass ein jeweiliger Indikator nicht mit anderen Konstrukten des Modells korrelieren sollte. Die Indikatoren für diese Untersuchung basieren auf der HAIS-Q-Studie, wurden jedoch teilweise angepasst und umfassen: den richtigen Umgang mit E-Mail-Bearbeitung, das Passwortmanagement, den Umgang mit (mobilen) Speicher- und Endgeräten, den Umgang mit Informationen u. a. im Kontext mobiler Arbeit sowie Zutritts- und Zugriffsschutz. Diese Indikatoren werden dann in entsprechende Items überführt, sodass sie in der Datenerhebung von den Teilnehmenden beantwortet werden können (vgl. König, 2019, S. 111).

Im Folgenden werden die Indikatoren und die Messmodelle vorgestellt. Die dazu gehörigen Items gemäß der jeweiligen Kontexte werden in späteren Kapiteln veranschaulicht.

4.3.4 Items-Entwicklung

Nachdem das Herausarbeiten der Forschungsfragen, Hypothesen und deren Operationalisierung erfolgt sind, soll im nächsten Schritt die Konstruktion des Fragebogens stattfinden. Nach Steiner und Bensch (2021) eignet sich die Methode der schriftlichen Befragung besonders gut für die Untersuchung von großen und homogenen Gruppen. Außerdem können Fragebogen nach Steiner und Benesch (2021) als Instrumente zur Erfassung von Einstellungen und Bewertungen von diversen Sachverhalten durch die zu befragten Personen genutzt werden. Dadurch, dass es sich in dieser Forschungsarbeit um eine homogene Untersuchungsgruppe (junge Erwachsene bei der Volkswagen AG) handelt (und aufgrund des bereits skizzierten Forschungsinteresses der Forschungsarbeit), soll dieses Verfahren als Untersuchungsmethode eingesetzt werden. Die Befragung wurde aufgrund der organisatorischen Voraussetzungen der Volkswagen AG und des Mangels einer internen Plattform für interne Befragungen dieser Art in Papierform durchgeführt.

Bevor es an die konkreten weiteren Schritte der Fragenbogenkonstruktion geht, empfehlen Steiner und Bensch (2021), zu überprüfen und kritisch zu betrachten, wie und mit welchen Instrumenten das zu bearbeitende Thema bereits untersucht wurde. Der in dieser Arbeit umgesetzte Fragebogen basiert auf dem Fragebogen von Parsons et al. (2014) und Parsons et al. (2017), allerdings wurden einige Fragen für den Kontext der Volkswagen AG adaptiert.

Für die Erhebung der Daten wurde ein strukturierter Fragebogen in Papierform entwickelt. Dazu wurden die zuvor genannten Indikatoren mit sogenannten Items operationalisiert (vgl. König, 2019). Der Fragebogen besteht aus zwei Abschnitten mit insgesamt 56 Items. Im ersten Abschnitt sollten die Probanden Angaben für die deskriptive Statistik machen. Im zweiten Abschnitt wurden die Probanden hinsichtlich Wissen, Verhalten und Einstellung zu den fünf beschriebenen Informationssicher-

heitskontexten befragt. Zu jedem Konstrukt muss erst die maximale Anzahl der Items entwickelt werden, jedoch wird von Nitzl (2010, S. 13 in Anlehnung an Huber et al., 2007, S. 23; Bergkvist, & Rossiter, 2007, S. 175; Drolet & Morisson, 2001, S. 199 f.) empfohlen, auch nicht eine zu große Anzahl an Indikatoren zu generieren, um den Fragebogen nicht zu lang werden lassen, da das zu Folge hat, dass die Teilnehmende die Fragebogenbeantwortung abbrechen könnten oder die Beantwortung der Fragen nicht mehr valide ist, wenn die Teilnehmer den Fragebogen durch Ermüdung falsch beantworten. Nitzl (2010, S. 14 in Anlehnung an Churchill, 1979, S. 66; Weiber & Mühlhaus, 2010, S. 92 f.) empfiehlt jedoch, mit möglichst mehr als nur einem Indikator jedes Konstrukt zu operationalisieren, auch wenn es per se durchaus möglich ist, ein Konstrukt mit einem Indikator zu operationalisieren (Nitzl, 2010, S. 14 in Anlehnung u. a. an Fassott, 2006, S. 73 f; Fuchs & Diamantopoulos, 2009, S. 197 ff.).

In Anhang 2.2 Indikatoren/Items ist die Gesamtstruktur mit den Indikatoren und den entsprechenden Items aufgelistet.

Im Folgenden soll detaillierter erklärt werden, wie die Fragebogenfragen entwickelt wurden.

E-Mail-Bearbeitung

Wie aus dem Verizon Data Breach Investigations Report von 2019 hervorgeht, wurden über 90 % der Malware per E-Mail übermittelt (z. B. durch infizierte Links oder Anhänge in einer E-Mail). Daher ist es von besonderem Interesse, zu überprüfen, inwiefern die Teilnehmer dieser Studie zum Thema E-Mail-Bearbeitung sensibilisiert sind. Die Indikatoren und deren Items basieren auf der HAIS-Q-Studien (Parsons et al., 2014; Parsons et al., 2017) und beinhalten die wichtigsten Themen aus dem Kontext „E-Mails-Bearbeitung", die auch im Kontext der Volkswagen AG relevant sind. Aus diesem Grund ergeben sich analog zur HAIS-Q-Studien folgende Indikatoren für den Kontext E-Mail-Bearbeitung:

- Die Links in E-Mails von unbekannten Absendern anklicken (Indikator 1)
- Die Links in E-Mails von bekannten Absendern anklicken (Indikator 2)
- Die Anhänge aus den E-Mails von unbekannten Absendern öffnen (Indikator 3)

Die Indikatoren wurden anhand von Items operationalisiert, um daraus eine Befragung im Rahmen der Studie durchzuführen (vgl. König, 2019, S. 111). Die Items dienen später für jeden Indikator als Fragebogenfragen für die Messung von Wissen, Einstellung und Verhalten. Für die Messung von Wissen wurden die Fragebogenfragen in der Form einer Wissensabfrage zum Thema „E-Mail-Bearbeitung" entwickelt. Die Fragebogenfragen für die Messung von Einstellung basieren auf der Abfrage der persönlichen Einstellung von Probanden zum Thema „E-Mail-Bearbeitung". Die Fragebogenfragen zur Messung von Verhalten wurden in Form von Arbeitssituationen mit einer möglichen Lösung entwickelt, auf die der Proband eine Antwort gibt, inwiefern es wahrscheinlich ist, dass er sich so verhält. Im Folgenden sollen die Fragebogenfragen zu jedem Indikator in den Bereichen Wissen, Einstellung und Verhalten präsentiert werden:

Die Links in E-Mails von unbekannten Absendern anklicken (Indikator 1)

Wissen:

- Links in E-Mails erleichtern sehr die Arbeit, daher kann ich erst einmal draufklicken, um herauszufinden, ob die Informationen für mich wichtig sind.
- Ich darf auf Links aus E-Mails von unbekannten Absendern nur dann klicken, wenn die E-Mail von einer sehr bekannten Firma oder Organisation ist (WHO, DHL, PayPal etc.).

Einstellung:

- Grundsätzlich kann nichts Schlimmes passieren, wenn ich auf einen Link aus einer E-Mail von einem unbekannten Absender klicke.

Verhalten:

- Ich arbeite bei einem sehr großen Unternehmen und kann schließlich nicht alle Mitarbeitenden kennen. Wenn eine E-Mail von einem mir nicht bekannten Mitarbeiter eingeht, dann öffne ich schon einmal die Mail und aktiviere den dort enthaltenen Link, wenn der Inhalt für mich wichtig ist.
- Versetze dich bitte in folgende Alltagssituation am Arbeitsplatz:
  Du bist in Zeitnot und erwartest eine wichtige E-Mail vom Projektteam mit den Links zu einem Projektordner im Datenmanagementsystem.
  Auf einmal bekommst du eine E-Mail mit den erwarteten Links. Die E-Mail wurde von einer Volkswagen-E-Mail-Adresse zugeschickt, allerdings kennst du den Absender nicht.
  Die Zeit läuft und du benötigst dringend die Dokumente aus dem Projektordner.
  Beantworte bitte die folgenden Frage, als wärst du in der geschilderten Situation:
  Ich öffne die E-Mail und klicke auf die Links, weil es eine Volkswagen-interne E-Mail-Adresse ist, auch wenn ich den Absender nicht persönlich kenne.

Die Links in E-Mails von bekannten Absendern anklicken (Indikator 2)

Wissen:

- Ich darf nicht auf Links aus unbekannten E-Mails klicken, selbst wenn diese von einem Volkswagen-Account stammen.

Einstellung:

- Es ist sicher, auf Links aus E-Mails von bekannten Absendern zu klicken.

Verhalten:

- Ich klicke nicht immer die Links aus meinen E-Mails an, nur weil ich den Absender kenne.

Die Anhänge aus den E-Mails von unbekannten Absendern öffnen (Indikator 3)

Wissen:

- Es ist verboten, die Anhänge von einem unbekannten Absender zu öffnen.

Einstellung:

- Bevor ich Anhänge von einem mir unbekannten Absender öffne, vergewissere ich mich, dass diese von einem Volkswagen-Account versandt worden sind.

Verhalten:

- Ich öffne niemals Anhänge von E-Mails, wenn mir der Absender unbekannt ist.

Im Folgenden soll die Entwicklung des Fragebogens für weitere Kontexte detaillierter beschrieben werden.

Passwortmanagement

Wie schon im Theoriekapitel erwähnt wurde, sind die wichtigsten Aspekte des Passwortmanagements die Wiederverwertung von Passwörtern und gestohlene Passwörter (Sieger, 2019). Parsons et al. (2017) benennen in ihrer Studie die wichtigsten Aspekte des Passwortmanagements wie folgt: Passwortverwendung (Benutzung desselben Passworts für diverse IT-Systeme), Teilung des Passwortes sowie Benutzung eines sicheren Passworts (unter der Bezeichnung „sicheres Passwort" ist gemeint, dass das Passwort größtmöglichen Schutz bietet und verschiedene Richtlinien des Passwortmanagements inkludiert, z. B. Passwörter bestehend aus Klein- und Großbuchstaben, Sonderzeichen, Zahlen). Daraus ergeben sich folgende Indikatoren für diesen Kontext, die für die Durchführung der Befragung für jeden Bereich der Informationssicherheits-Awareness (Wissen, Einstellung und Verhalten) operationalisiert wurden:

- Sein eigenes Passwort teilen
- Ein sicheres Passwort benutzen
- Dasselbe Passwort benutzen

Umgang mit Informationen u. a. im Kontext mobiler Arbeit

Wie schon in den Experimenten „Robin Sage" und „Emily Williams" gezeigt wurde (Kapitel 2.5), kann der (öffentliche) Umgang mit Arbeitsinformationen (Veröffentlichung zur eigenen Arbeit auf nicht dazu geeigneten Plattformen sozialer Medien etc.) kritisch sein, dementsprechend wichtig erscheinen die Messung des Wissens, der Einstellung und des Verhaltens der Beschäftigten und deren Sensibilisierung zum Thema Umgang mit Arbeitsinformationen im Kontext der Informationssicherheits-Awareness. Außerdem nutzen rund 40 % der Deutschen diverse Arten des mobilen Arbeitens und die Statistiken zeigen, dass dieser Trend noch zunehmen wird (Statista Research Department, 2022). Folglich wird das Risiko eines Datendiebstahls bei der Verwendung entsprechender Endgeräte bei der mobilen Arbeit nur steigen.

Die Awareness der Teilnehmenden zu diesem Thema zu testen, um schlussendlich deren Sensibilisierung zu gewährleisten, ist entsprechend wichtig. Parsons et al.

(2017) nehmen in ihrer HAIS-Q-Studie Bezug auf Shoulder Surfing als einen Indikator im Kontext der mobilen Arbeit, was die Bedeutsamkeit der Thematik noch einmal hervorhebt. Rouse (2022) beschreibt noch eine weitere Social-Engineering-Methode, bei der ein Hacker z. B. nicht nur digitale Cyber-Attacken initiiert, sondern sich auch unautorisiert in internen Systemen anmeldet, um Daten zu stehlen oder Schadsoftware zu verbreiten. Im Kontext der Volkswagen AG ist es zum einen äußerst wichtig für die Beschäftigten, sich mit einem Arbeitsausweis (PKI-Karte) physisch zu autorisieren, und zum anderen, die notwendigen Zugänge zu den internen Volkswagen-Systemen zu erhalten, um solche Informationssicherheitsvorfälle zu vermeiden. Der Arbeitsausweis der Beschäftigten, der zum einen Informationsträger ist und zum anderen Zugänge zu internen Systemen gewährleistet, soll von den Mitarbeitern bei Volkswagen folglich stets gesichert sein. Es ergeben sich die folgenden Indikatoren für den Kontext „Umgang mit Informationen u. a. im Kontext mobiler Arbeit“:

- Über die Arbeit in sozialen Medien veröffentlichen
- Shoulder Surfing
- Arbeitsausweis sichern

Umgang mit (mobilen) Speicher- und Endgeräten

Nach Parson et al. (2017) ist der Umgang mit Endgeräten (darunter auch mobile Geräte) von großer Bedeutung. Darunter fallen sowohl die Benutzung von privaten Endgeräten als auch deren Ankopplung (z. B. von privaten Handys oder USB-Sticks) an Arbeitsgeräte. Parsons et al. (2017) nutzen in ihrer Studie Indikatoren, die nicht nur die physische Sicherheit der Endgeräte, sondern auch die Ankopplung von privaten und/oder unsicheren Geräten untersuchen.

Es ergeben sich folgende Indikatoren für den Kontext „Umgang mit (mobilen) Speicher- und Endgeräten“:

- Ankopplung des Handys an den Arbeitslaptop
- Ankopplung des privaten USB-Sticks an den Arbeitslaptop

Zutritts- und Zugriffsschutz

Beim Thema Zutritts- und Zugriffsschutz muss nicht nur die technische Absicherung betrachtet werden, auch der Aspekt des menschlichen Verhaltens darf nicht außer Acht gelassen werden. Denn wie bereits im Theoriekapitel erwähnt, stellt Fehlverhalten von Mitarbeitern die größte Ursache für erfolgreiche Cyber-Security-Angriffe dar. Um einen angemessenen Zutritts- und Zugriffsschutz z. B. auf dem Werksgelände oder direkt am Arbeitsplatz zu gewährleisten, darf ein Informationssicherheitsvorfall nicht ignoriert werden, sondern muss gemeldet werden. Informationssicherheitsvorfälle bewusst zu ignorieren, stellt bei der Volkswagen AG einen Unternehmensregelverstoß gegen Integrität und Compliance dar. Die Meldung von verdächtigem Verhalten ist dementsprechend von großer Bedeutung und findet auch bei Parsons et al. (2017) in ihrer HAIS-Q-Studie als Indikator Anwendung.

Daraus ergeben sich folgende Indikatoren zum Thema „Zutritts- und Zugriffsschutz“:
- Informationssicherheitsvorfälle ignorieren
- Informationssicherheitsvorfälle melden

Nachdem der Indikatorensatz vollständig gesammelt wurde, ist nun zu entscheiden, in welchem Zusammenhang die Indikatoren zu den jeweiligen Variablen stehen und welches Messmodell daraus resultiert: ein reflektives oder ein formatives Messmodell (vgl. Nitzl, 2010). Es ist entscheidend, welches Messmodell verwendet wird, denn davon sind die weiteren Schritte der Auswertung abhängig.

In dieser Studie handelt es sich bei den fünf Kontexten der Informationssicherheits-Awareness um ein reflektives Messmodell. Wie bereits erwähnt, zeichnen sich reflektive Messmodelle im Vergleich zu formativen Messmodellen dadurch aus, dass ihre Indikatoren gegeneinander austauschbar sind, einen gemeinsamen Ursprung (eine latente Variable) haben und untereinander eine relativ hohe Korrelation aufweisen (Nitzl, 2010 in Anlehnung an Jarvis, MacKenzie & Podsakoff, 2003).

Regorz (2023) und Miles (o. J.) nennen als Beispiel für ein reflektives Messmodell einen Intelligenztest: Je intelligenter ein Proband ist, desto höher ist die Wahrscheinlichkeit, dass er die richtigen Antworten auf die Testaufgaben gibt. Daher ist die Intelligenzstufe hier die latente Variable und Testfrage 1, Testaufgabe 2 usw. sind die Indikatoren, die mit der latenten Variable in einem reflektiven Zusammenhang stehen. Am Beispiel des Kontextes „E-Mail-Bearbeitung“ im Awareness-Bereich Wissen soll im Folgenden veranschaulicht werden, warum im Rahmen dieser Arbeit ein reflektives Modell gewählt wurde: Je größer das Informationssicherheitswissen des jeweiligen Probanden, desto größer ist die Wahrscheinlichkeit, dass der Proband weiß, dass es gewisse Informationssicherheitsrisiken birgt, die Links in E-Mails von unbekannten Absendern anzuklicken oder die Anhänge aus den E-Mails von unbekannten Absendern zu öffnen. Außerdem sind die Indikatoren in diesem Kontext gegeneinander austauschbar, jedoch repräsentativ für die Variable.

Daraus ergeben sich die Messmodelle für alle fünf Kontexte. In Abbildung 15 werden am Beispiel des Kontextes „E-Mail-Bearbeitung“ die Zusammenhänge zwischen den Awareness-Aspekten (Wissen, Einstellung und Verhalten) dargestellt. In den nächsten Kapiteln werden die Durchführung der Befragungen, die Auswertung der Daten und die Überprüfung der Hypothesen beschrieben.

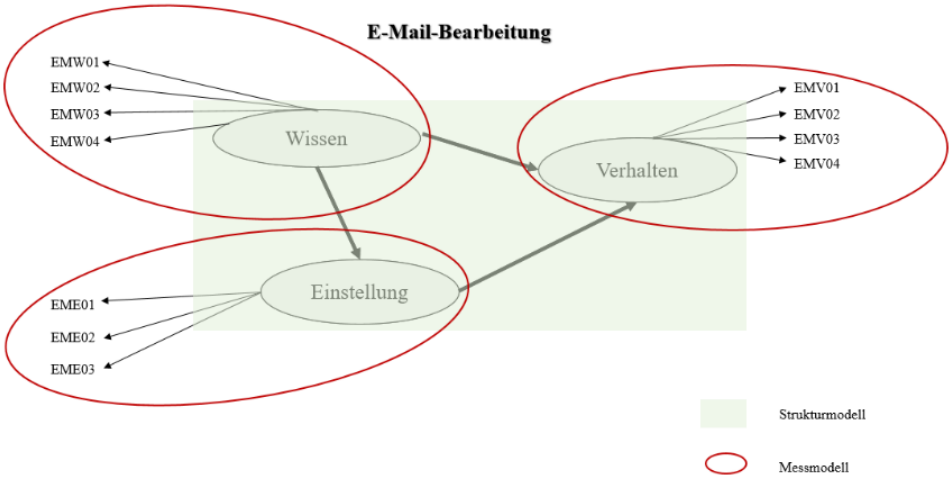


Abbildung 15: Reflektives Mess- und Strukturmodell im Kontext „E-Mail-Bearbeitung" (eigene Darstellung basierend auf Parsons et al., 2014, S. 169)

4.4 Datenerhebung

4.4.1 Fragebogenstruktur

Analog zum Fragebogen von Parsons et al. (2017, S. 47) wurden geschlossene Fragen für den Fragebogen dieser Studie ausgewählt. Der Vorteil dieser Art der Fragen liegt darin, dass sich die Antworten geschlossener Fragen im Vergleich zu den Antworten offener Fragen schneller und effizienter systematisieren und auswerten lassen (Steiner & Bensch, 2021). Außerdem sind die zu befragenden Personen motiviert, eher vorgefertigte Antworten auszuwählen, als selbst die Antworten zu generieren (Steiner & Bensch, 2021). Darüber hinaus kann davon ausgegangen werden, dass die Rückmeldungsquote bei geschlossenen Fragen im Fragebogen größer ausfällt als bei offenen Fragen.

Nachdem die Form der Fragen des Fragebogens ausgewählt wurde, soll die Einleitung des Fragebogens formuliert werden. Hier empfehlen Steiner und Bensch (2021, S. 49 f. nach Bortz & Döring, 2006, S. 254 f.) eine Darstellung der groben Richtung, wofür die Erhebung gemacht wird, und der Fragen, zudem eine kurze Erklärung, was mit den gewonnenen Daten weiter gemacht wird, eine Bitte um das vollständige und aufrichtige Beantworten der Fragen und eine Zusicherung der Anonymität. Die erste Frage in der Befragung dieser Studie bezieht sich auf das Einverständnis der Befragten bezüglich der Nutzung ihrer Daten und Antworten im Rahmen dieser Arbeit. Eins der Ziele dieser Arbeit ist der Vergleich der Ergebnisse der Befragungen zu verschiedenen Zeitpunkten. Allerdings soll die Identität der Befragten anonymisiert werden, um ihre Privatsphäre zu schützen und geltenden Datenschutzvorgaben gerecht zu werden. Damit einerseits die Anonymität der Befragten gewährleistet werden kann und die Rückvollziehbarkeit auf einzelne Personen vermieden wird, es andererseits aber dennoch

möglich ist, die Ergebnisse derselben Person zu verschiedenen Erhebungspunkten zu vergleichen und so die Effektivität der Awareness-Maßnahmen zu überprüfen, soll jeder Teilnehmer am Anfang der Befragung einen Code erhalten (vgl. Pöge, 2008). Dieser Code wird mithilfe von Antworten auf die folgenden Fragen generiert (basierend auf Pöge, 2008, S. 63):

- Der erste Anfangsbuchstabe des Namens deiner Mutter
- Der erste Anfangsbuchstabe des Namens deines Vaters
- Die ersten zwei Ziffern deines Geburtsdatums
- Der letzte Buchstabe deines Vornamens

Daraus ergibt sich eine originelle ID, die jeder Befragte bekommt. Um den Prozess der Code-Generierung für die Befragten dieser Studie leichter und unauffälliger zu gestalten, wurden in dieser Studie keine komplexen Fragen für die ID-Generierung benutzt, wie z. B. „[...] der letzte Buchstabe der Haarfarbe des Vaters" (Pöge, 2008, S. 63) oder ein Duisburg-Codeblatt, wo die befragte Person die entsprechenden Buchstaben ankreuzen soll, um einen Code zu generieren.

Nachdem die Einverständniserklärung und die Anonymisierung erfolgten, sollen die Teilnehmer die Fragebogenfragen beantworten. Steiner und Bensch (2021, S. 51 f. in Anlehnung an Bortz & Döring, 2006, S. 254 f.) beschreiben folgende Regeln für die Formulierung der Fragen: Zum einen soll sich die Sprache, die in der Befragung benutzt wird, auf die Zielgruppe richten, zum anderen soll die Länge der Befragung die Teilnehmer nicht abschrecken. Des Weiteren sollen die Teilnehmer das Gefühl bekommen, dass durch die Eingabe ihrer Meinung eine Veränderung des Sachverhaltens im befragten Thema angestoßen wird. Es muss vermieden werden, mehrere Items in einer Frage zu platzieren. Außerdem sollen solche Formulierungen wie „immer", „nie", „keiner" oder „alle" unterlassen werden. Die Fragen (Items) wurden nach den Regeln von Steiner und Bensch (2021, S. 51 f. in Anlehnung an Bortz & Döring, 2006, S. 254 f.) formuliert.

Nachdem der gesamte Fragebogen ausformuliert ist, soll entschieden werden, welche Art der Antwortmöglichkeiten die Teilnehmer im Fragebogen bekommen. Wie schon erwähnt, werden im Fragebogen dieser Arbeit geschlossene Fragen benutzt. Steiner und Bensch (2021, S. 54 f.) nennen zwei Varianten von vorgegebenen Antwortformaten für geschlossene Fragen, nämlich ein dichotomes Antwortformat („ja/nein"; „stimmt/stimmt nicht") und Antworten mit einer Ratingskala. Ein Nachteil der ersten Variante liegt darin, dass die Teilnehmer der Befragung sich für eine der zwei Möglichkeiten entscheiden müssen und keine weiteren Abstufungen ihrer Antworten treffen können (Steiner & Bensch, 2021 in Anlehnung an Karner, 1993). Daher ist es nach Steiner und Bensch (2021 in Anlehnung an Amelang & Bartussek, 2001) sinnvoll, für die Korrelationsberechnungen eine Mehrkategorienskala zu verwenden. Weil es in dieser Arbeit um eine Kausaluntersuchung geht, wurde entschieden, eine Mehrkategorienskala zu verwenden. Eine Ratingskala bietet mehr als zwei Antwortalternativen für die Befragten. Wenn die Antwortalternativen für mehrere oder alle Items eines Fragebogens gleich sind, dann handelt es sich um eine sogenannte Likert-Skala (Steiner &

Bensch, 2021 in Anlehnung an Rost, 2004, S. 64). Mithilfe dieser Likert-Skala können Fremd- und Selbstwahrnehmungen dokumentiert werden (Steiner & Bensch, 2021). Da eins der Ziele dieser Arbeit darin besteht, den Grad der Kausalität zwischen Wissen, Einstellung und Verhalten zu untersuchen, ist es von großer Bedeutung, die Selbsteinschätzung der Zielgruppe zu bestimmten Situationen in Erfahrung zu bringen. Folglich wurde in dieser Arbeit eine Befragung mit Antwortmöglichkeiten, die auf einer Likert-Skala liegen, ausgewählt.

Nachdem die Art der Antwortmöglichkeiten für den Fragebogen festgelegt wurde, soll im nächsten Schritt entschieden werden, wie viele Abstufungen die Ratingskala haben soll und welcher Art diese sein sollen. Nach Steiner und Bensch (2021) kann die Ratingskala entweder in eine Richtung verlaufen (unipolare Skala, die z. B. von keiner Ablehnung bis zu einer starken Ablehnung verläuft) oder symmetrisch (bipolare Ratingskala mit einer Abstufung von einer sehr starken Ablehnung über einen Nullpunkt (Mittelkategorie) bis hin zu einer positiven Zustimmung). In dieser Arbeit wird eine sogenannte bipolare Ratingskala verwendet, um den Befragten eine Möglichkeit zur Verfügung zu stellen, die Breite der Selbsteinschätzung möglichst präzise ausdrücken zu können. Nach Steiner und Bensch (2021, S. 55 in Anlehnung an Rost, 2004, S. 66) soll die Abstufung eine maximale Anzahl von 5 bis 7 Kategorien haben. Es wurde entschieden, in dieser Arbeit eine Anzahl von 5 Kategorien zu verwenden, um eine überschaubare Anzahl der Kategorien in der Befragung zur Verfügung zu stellen (vgl. Steiner & Bensch, 2021, S. 55).

Nachdem die Bestimmung der Fragebogenstruktur und die inhaltliche Entwicklung der Items abgeschlossen sind, soll der Fragebogen vor der tatsächlichen Erhebung erprobt werden, um die Bearbeitungsdauer und die Verständlichkeit der Fragen zu überprüfen (Steiner & Bensch, 2021). In den beiden nächsten Kapiteln werden die Pretest-Durchführung, die Stichprobenauswahl und der Erhebungsprozess detaillierter dargelegt.

4.4.2 Pretest und Stichprobenauswahl

Steiner und Bensch (2021, S. 59) empfehlen, nach einem Probedurchlauf in Form eines Vortests für die Befragung folgende Aspekte zu berücksichtigen:

- Verständlichkeit der Fragen: Sind alle Fragen und die Begrifflichkeiten, die benutzt werden, verständlich ausformuliert und ist der Fragebogen sprachlich auf die Zielgruppe abgestimmt?
- Eine ungewollte Beeinflussung der Befragten: Werden die Befragten in eine Richtung gedrängelt?
- Bearbeitungsdauer des Fragebogens: Wirkt der Fragebogen zu lange?
- Auswertung des Fragebogens: Können die Hypothesen mit den vorliegenden Fragen beantwortet werden?

Um sowohl die inhaltliche Richtigkeit der Items als auch die Verständlichkeit des Fragebogens innerhalb der Studienzielgruppe zu gewährleisten, wurde ein Pretest des Fragebogens mit fünf akademischen Experten aus dem Informationssicherheitsum-

feld durchgeführt sowie mit drei Auszubildenden. Die Erkenntnisse aus dem Pretest gaben Aufschluss hinsichtlich einiger unverständlicher Ausformulierungen bei manchen Fragen, die entsprechend bearbeitet und deren Verbesserungen dann in den Fragebogen eingepflegt wurden.

Um eine repräsentative Stichprobe aus einem bestimmten Personenkreis auswählen zu können, wurde sich im Rahmen dieser Studie auf die Befragung der spezifischen Personengruppe der jungen Erwachsenen bei der Volkswagen AG konzentriert (siehe Kapitel 1.1). Der Fokus dieser Studie liegt auf den Auszubildenden gewerblich-technischer sowie kaufmännischer Berufe im ersten Ausbildungsjahr. Die Erhebung ist in fünf verschiedene Erhebungszeitpunkte (von 17.08.2020 bis 21.10.2020) aufgeteilt, um die Nachhaltigkeit der Awareness-Maßnahmen zu testen und den Vergleich zwischen den Probanden, die nur anhand einer Unterweisung sensibilisiert wurden (Gruppe B), und denen, die eine Unterweisung mit zusätzlicher Security Arena durchlaufen haben (Gruppe A), zu ermöglichen.

4.4.3 Erhebungszeitpunkte

Die erste Erhebung (T0) wurde mit der Gesamtpersonenanzahl von 87 Auszubildenden am 17.08.2020 durchgeführt. Im Anschluss erfolgte der erste Durchlauf einer Informationssicherheits-Awareness-Maßnahme, nämlich der klassischen Unterweisung. Innerhalb dieser Unterweisung waren die in Kapitel 2.5 genannten didaktischen Elemente enthalten.

Die zweite Erhebung fand mit demselben Personenkreis direkt nach der Durchführung der klassischen Unterweisung statt (T1). Sechs Wochen nach den Erhebungen T0 und T1, am 21.09.2020, wurde mit der Kontrollgruppe A, bestehend aus 30 Auszubildenden, eine weitere Umfrage durchgeführt, um die Veränderungen im Verlauf zwischen T1 und der erneuten Erhebung T2 zu untersuchen. Im Anschluss wurde mit der Kontrollgruppe A die Informationssicherheits-Awareness-Maßnahme „Security Arena“ durchgeführt, bei der die in Kapitel 2.3 aufgeführten didaktischen Elemente enthalten waren. Direkt nach der Durchführung der Maßnahme wurde eine weitere Umfrage gemacht, um die Veränderungen durch die Maßnahme zu beobachten (T3). Die letzte Erhebung zur Überprüfung der Langzeitwirkung beider Maßnahmen und der benötigten zeitlichen Intervalle für deren effiziente Wirkung wurde 30 Tage nach der Erhebung des Zeitpunkts T3 am 21.10.2020 durchgeführt (T4). Zum Zeitpunkt T4 wurden Auszubildende aus den ersten beiden Befragungen, also aus Gruppe A und Gruppe B, befragt (jedoch konnten nur 52 Auszubildende teilnehmen). Das Vorgehensmodell ist in Tabelle 8 zusammengefasst.

Tabelle 8: Vorgehensmodell der quantitativen Studie

	Befragung T0	Unterweisung	Befragung T1	Befragung T2	Security Arena	Befragung T3	Befragung T4
Kontrollgruppe A	X	X	X	X	X	X	X
Kontrollgruppe B	X	X	X				X

4.5 Datenauswertung

4.5.1 Auswertung der Daten

4.5.1.1 Ermittelte Daten und deskriptive Statistik

Wie im vorangegangenen Teilkapitel beschrieben, wurde die Befragung in Papierform durchgeführt. Die zuvor definierte Personenanzahl bestand aus insgesamt 87 Probanden. Die Befragten wurden für jede Befragung zu einem Präsenztermin eingeladen, wo die Umfrage und das entsprechende Awareness-Verfahren durchgeführt wurden. Die Personenanzahl zu den jeweiligen Erhebungszeitpunkten ist in Tabelle 9 abgebildet. Die Werte in der Tabelle stellen die vollständigen und somit verwertbaren Rückmeldungen dar.

Tabelle 9: Probandenanzahlgröße zu den Erhebungszeitpunkten

Erhebungszeitpunkt	T0	T1	T2	T3	T4
Personenanzahl	87	87	30	30	52

Etwa 51 % der Befragten sind männlich und 49 % sind weiblich. Alle Probanden sind Berufseinsteiger und befinden sich zur Zeit der Durchführung von allen 5 Erhebungen im ersten Jahr der Berufsausbildung. Tabelle 10 zeigt eine Übersicht über die Ausbildungen, die die Probanden ausüben.

Tabelle 10: Übersicht über die Ausbildungsberufe der Probanden (Erhebungspunkt T0)

Berufsbezeichnung	**Anzahl**
Industriekauffrau/Industriekaufmann	38
Köchin/Koch	5
Fachinformatiker/-in Anwendungsentwicklung	31
Fachkraft für Lagerlogistik	13

Um die Auswertung durchzuführen, wurden die gewonnenen Ausprägungen je nach Art der Fragestellung zu einem Großteil von „stimme überhaupt nicht zu“ mit Wert 5 bis „stimme ganz zu“ mit Wert 1 codiert; bei den restlichen Fragebogenfragen wurden die gewonnenen Ausprägungen von „stimme ganz zu“ mit Wert 5 bis „stimme überhaupt nicht zu“ mit Wert 1 codiert (vgl. König, 2019). Auch jedes Item wurde entsprechend codiert, um die Möglichkeit zu haben, die Überprüfung jedes einzelnen Items durchzuführen. Die Zahlen wurden anschließend aus jedem Befragungsbogen per Hand in eine Excel-Tabelle eingetragen, um später das gesamte Datenset in das statistische Programm (SmartPLS 4, Version 4.0.9.4. nach Ringle, Wende & Becker, 2022)

hochzuladen und es auszuwerten. Darin wurde anhand der zu jedem Kontext zugehörigen Items jeweils ein Mess- und Strukturmodell entwickelt (siehe Abb. 16).

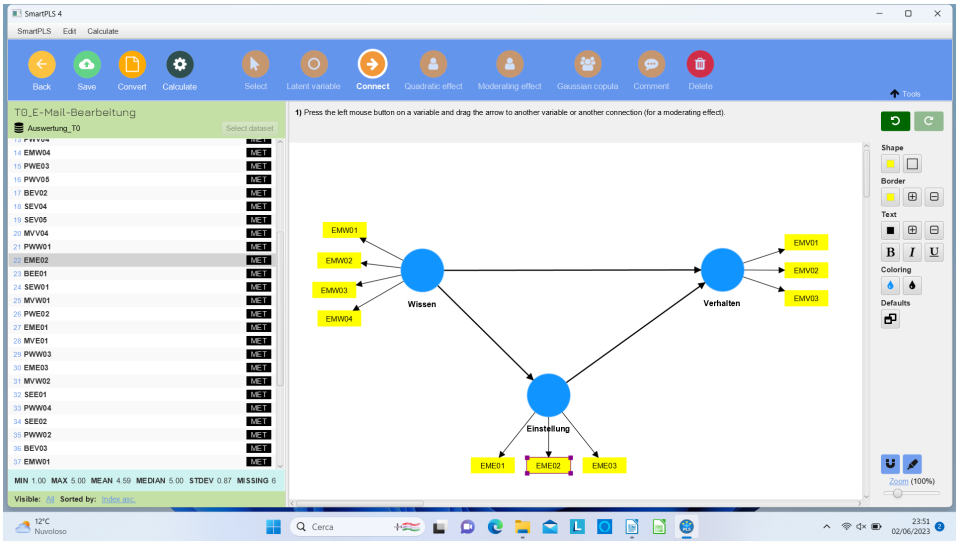


Abbildung 16: Beispielhaftes Mess- und Strukturmodell für die Auswertung der ersten Befragung T0 im statistischen Programm SmartPLS 4 (Screenshot aus dem statistischen Programm SmartPLS 4, vgl. Ringle, Wende & Becker, 2022)

Die detaillierte Beschreibung des Auswertungsprozesses erfolgt separat in weiteren Kapiteln. Die deskriptiven Statistiken der gewonnenen Daten aus der Befragung wurden nicht in den Mess- und Strukturmodellen mitberechnet, da sie keinen Mehrwert für die statistische Auswertung der Mess- und Strukturmodelle liefern können. Damit eine hohe Datenqualität sichergestellt werden kann, soll eine Fehlerkontrolle bzw. Bereinigung des erhobenen Datensets aus der Befragung hinsichtlich der Qualität vorgenommen werden (König, 2019, S. 150 in Anlehnung an Häder, 2010, S. 406). Dabei wurden inkonsistente oder fehlende Werte (z. B. fehlende Antworten) nicht in die Analyse oder die Mittelwertersetzung einbezogen (König, 2019, S. 151 in Anlehnung an Häder, 2010, S. 406). Die nächsten Kapitel geben Auskunft über die Validität der Mess- und Strukturmodelle und deren Limitationen.

4.5.1.2 Modellschätzung – Partial-Least-Square-(PLS)-Methode

Zur Schätzung und Analyse von Kausalzusammenhängen existieren zwei Ansätze, wobei zwischen der varianz- und kovarianzbasierten Methode unterschieden wird (Nitzl, 2010, S. 15 in Anlehnung an Henseler, Ringle & Sinkovics, 2009, S. 277).

Einer der Verteile der kovarianzbasierten Methode liegt darin, die Zusammenhänge in einem aufgestellten Strukturmodell mit den empirisch erfassten Zusammenhängen zu vergleichen und auf Richtigkeit zu überprüfen (Nitzl, 2010, S. 17 in Anlehnung an Lohmöller, 1989, S. 211 ff.). Im Vergleich zur kovarianzbasierten Methode

wird die varianzbasierte Methode als eine Auswertungsmethode für Studien empfohlen, die eher einen explorativen Charakter haben, in welchen die zu erforschenden Phänomene noch auf keinen fundierten Mess- oder Konstrukttheorien basieren (Nitzl, 2010, S. 17 in Anlehnung an Reinartz, Haenlein & Henseler, 2009, S. 341; Weiber & Mühlhaus, 2010, S. 253).

Nitzl (2010, S. 18 in Anlehnung an Scholderer & Balderjahn, 2005, S. 97) führt noch ein weiteres Kriterium zum Vergleich der beiden Verfahren ein, nämlich die erforderliche Stichprobengröße für die Modellschätzung. Für die kovarianzbasierte Analyse wird eine minimale Anzahl von 200 Rückmeldungen pro Stichprobe empfohlen (Nitzl, 2010, S. 19 in Anlehnung an Boomsma, 1982, S. 171; Backhaus et al., 2006b, S. 370 f.; Homburg & Klarmann, 2006, S. 733; Scholderer & Balderjahn, 2006, S. 67). Um die empfohlene Anzahl der Rückmeldungen pro Stichprobe für die varianzbasierte Analyse herauszufinden, empfiehlt Nitzl (2010, S. 18 in Anlehnung an Chin, 1998b; S. 311) die Anzahl der zu schätzenden Indikatoren in dem zu schätzenden Strukturmodell mit fünf bzw. mit zehn zu multiplizieren. Daraus ergibt sich die empfohlene Stichprobengröße, die seltener die Zahl 100 übersteigt (Nitzl, 2010, S. 18 in Anlehnung an Chin & Newsted, 1999, S. 355 f.).

Für diese Arbeit wird eine varianzbasierte Auswertungsmethode ausgewählt, da diese Studie einen explorativen Charakter hat, die aufgestellten Struktur- und Messmodelle nicht in erster Linie mit den in der Literatur existierenden Struktur- und Messmodellen verglichen werden sollen und die Stichprobengröße für diese Studie unter der Zahl 100 liegt. Als varianzbasiertes Analyseverfahren nennt Nitzl (2010, S. 16 in Anlehnung an Henseler, Ringle & Sinkovics, 2009, S. 282; Weiber & Mühlhaus, 2010, S. 253) die Partial-Least-Square-(PLS)-Methode, die in den letzten Jahren zunehmend in wissenschaftlichen Studien angewendet wurde. Nitzl (2010, S. 23 in Anlehnung an Schloderer, Ringle & Sarstedt, 2009, S. 589) schlägt das folgende Vorgehen zur Evaluierung von PLS-Modellschätzungen vor (s. Abb. 17):

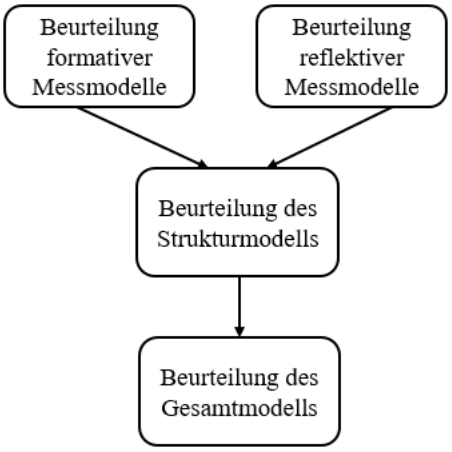


Abbildung 17: Vorgehen zur Evaluierung von PLS-Modellschätzungen (eigene Darstellung nach Nitzl, 2010, S. 23 in Anlehnung an Schloderer, Ringle & Sarstedt, 2009, S. 589)

Zuerst sollen die formativen bzw. reflektiven Messmodelle überprüft werden. An dieser Stelle ist hervorzuheben, dass sich die Gütebeurteilung zwischen reflektiven und formativen Messmodellen unterscheidet (Nitzl, 2010, S. 23 in Anlehnung an Krafft, Götz & Liehr-Gobbers, 2005, S. 72). In dieser Studie werden nur reflektive Messmodelle genutzt (siehe Kapitel 4.3.3.), daher entfällt der Schritt der Beurteilung der formativen Messmodelle. Im zweiten Schritt soll die Beurteilung der Strukturmodelle erfolgen, indem die Pfadbeziehung überprüft wird (Nitzl, 2010). Erst danach soll die Beurteilung des Gesamtmodells erfolgen. In den beiden weiteren Kapiteln wird sowohl die Gütebeurteilung der Mess- und Strukturmodelle als auch die Beurteilung des Gesamtmodells detaillierter präsentiert.

4.5.1.3 Gütekriterien des reflektiven Messmodells

Im ersten Schritt der PLS-Methode soll die Gütebeurteilung der Messmodelle erfolgen. Nitzl (2010, S. 24) beschreibt, dass die Gütebeurteilung reflektiv gemessener latenter Variablen ausgehend von beiden Gütekriterien erfolgt: Reliabilität (Zuverlässigkeit) und Validität (Gültigkeit). Dafür führt Nitzl (2010, S. 24 in Anlehnung an Ringle & Spreen, 2007, S. 212 f.) vier Kriterien ein: *Indikatorenreliabilität, Konstruktreliabilität, durchschnittlich erfasste Varianz* und *Diskriminanzvalidität*.

Die ersten drei behandelten Kriterien dienen zur Überprüfung der Konvergenzreliabilität, die besagt, dass die Indikatoren, die einem Konstrukt zugeordnet sind, miteinander stark in Beziehung stehen müssen (Nitzl, 2010, S. 24 in Anlehnung an Hair et al., 2010, S. 709 f.; Himme, 2007, S. 384 f.). Diskriminanzvalidität dient dazu, die Validität zu überprüfen (Nitzl, S. 24).

Im Folgenden werden die einzelnen Kriterien beschrieben, um die Messmodelle und schließlich die Strukturmodelle weiter zu beurteilen.

Indikatorenreliabilität

Die Indikatorenreliabilität analysiert, inwiefern sich jedes einzelne Item für die Messung einer latenten Variable eignet. Nitzl beschreibt, dass „[…] die Indikatorenreliabilität hierzu den Anteil der Varianz eines Indikators an[gibt], der durch die ihm zugeordneten latenten Variablen erklärt wird. Dabei sollte die Hälfte der Varianz eines Indikators durch den [sic!] ihm zugeordneten Konstrukt erklärt werden, was einen Mindestwert von 0,7 ($0{,}7^2 \approx 0{,}5$) für die jeweilige Faktorladung bedeutet“ (Nitzl, 2010, S. 25 in Anlehnung an Hildebrandt & Temme, 2006, S. 625).

Somit besagt der Mindestwert, dass der erklärte Varianzanteil größer als der nicht erklärte sein sollte (Nitzl, 2010, S. 25 in Anlehnung an Krafft, Götz & Liehr-Gobbers, 2005, S. 73 ff.). Drüber hinaus, dass sich die Ladungen der Größenordnung von 0,7 signifikant von Null unterscheiden, soll an dieser Stelle ein Signifikanztest durchgeführt werden (Nitzl, 2010, S. 25 in Anlehnung an Huber et al., 2007, S. 35; Schloderer, Ringle & Sarstedt, 2009, S. 590). Jedoch beschreibt Nitzl (2010, S. 25 in Anlehnung an Hulland, 1999, S. 198), dass auch geringere Ladungen als 0,7 vorkommen können.

Allgemein gilt aber, je höher die Ladung ist, desto größer ist der Zusammenhang zwischen einem Item und einer latenten Variable (Nittel-Neubert, o. J.). Allerdings gilt

nach Pelz (2008, S. 156 in Anlehnung an Agarwal & Karahanna, 2000, S. 678 ff.; Fritz, 1995, S. 131 f.) ein Wert von 0,5 als akzeptabel, was impliziert, dass mindestens 50 % der Varianz des Indikators durch das latente Konstrukt erklärt werden. Pelz (2008, S. 156 in Anlehnung an Götz & Liehr-Gobbers, 2004, S. 727; Hulland, 1999, S. 198) empfiehlt alle Indikatoren, die einen Ladungskoeffizienten mit einem Wert geringer als 0,4 aufweisen, aus dem Messmodell zu entfernen. Daher wird sich in dieser Arbeit am Mindestmesswert von ≈ 0,4 orientiert.

Die detaillierte Darstellung der Datenauswertung erfolgt in späteren Kapiteln.

Durchschnittlich erfasste Varianz

Die durchschnittlich erfasste Varianz (DEV) ist neben der Konstruktreliabilität ein Kriterium für die Überprüfung der Konvergenzvalidität (Nitzl, 2010, S. 26 in Anlehnung an Hair et al., 2010, S. 709). Die DEV setzt den Anteil der erklärten Varianz in Relation zum Messfehler einer latenten Variable (Nitzl, 2010). Nitzl (2010, S. 26) beschreibt, dass die Berechnung der DEV ähnlich zur Berechnung der Konstruktreliabilität ρ_c erfolgt, „[...] wobei jedoch die Faktorladung direkt quadriert in die Formel eingeht". Auch diese Berechnung der Ergebnisse wurde mithilfe von SmartPLS 4 (Version 4.0.9.4. nach Ringle, Wende & Becker, 2022) durchgeführt, jedoch kann die DEV auch nach oben ersichtlicher Formel berechnet werden (Abb. 18):

$$\boldsymbol{DEV} = \frac{\sum_i \lambda_i^{\,2}}{\sum_i \lambda_i^{\,2} + \sum_i var(\varepsilon_i)}$$

Abbildung 18: Formel der durchschnittlich erfassten Varianz (Nitzl, 2010, S. 26)

Der mögliche Wert der DEV liegt zwischen 0 und 1, jedoch stellt eine DEV ≥ 0,5 einen ausreichend hohen Wert dar, der definiert, dass mindestens die Hälfte der Varianz eines Konstrukts durch die ihm zugeordneten Indikatoren erklärt wird (Nitzl, 2010, S. 26 f. in Anlehnung an Huber et al., 2007, S. 36; Ringle & Spreen, 2007, S. 212).

Konstruktreliabilität

Die Konstruktreliabilität (KR) fordert, dass die Indikatoren, die einer latenten Variable zugeordnet sind, untereinander positiv stark korrelieren (Nitzl, 2010, S. 25). Die Berechnung der Ergebnisse für diese Studie wurde mithilfe von SmartPLS 4 (Version 4.0.9.4. nach Ringle, Wende & Becker, 2022) durchgeführt, jedoch kann die KR nach folgender Formel berechnet werden (Abb. 19):

$$\rho_C = \frac{(\sum_i \lambda_i)^2}{(\sum_i \lambda_i)^2 + \sum_i var(\varepsilon_i)}$$

Abbildung 19: Formel der Konstruktreliabilität (Nitzl, 2010, S. 26)

λ_i stellt die Ladung zwischen der latenten Variable und dem jeweiligen Indikator i dar (Nitzl, 2010, S. 26). Die Varianz des Messfehlers var (ε_i) wird aus der Subtraktion 1-λ_i^2 bestimmt. Die KR kann Werte zwischen 0 und 1 annehmen, jedoch gelten Werte von ≥ 0,6 als akzeptabel (Nitzl, 2010, S. 26 in Anlehnung an Ringle & Spreen, 2007, S. 212). Laut Nitzl (2010, S. 26 in Anlehnung an Chin, 1998b, S. 320; Henseler, Ringle & Sinkovics, 2009, S. 298 f.) ist dieses Gütekriterium gegenüber dem üblichen Cronbachs Alpha für die interne Konsistenz von Vorteil, da Cronbachs Alpha dazu neigt, die interne Konsistenz zu unterschätzen.

Des Weiteren wird es in dieser Studie statt Cronbachs Alpha berechnet, um die positive Korrelation der latenten Variablen zu messen. Die Konstruktreliabilität wird für diese Studie mithilfe von SmartPLS 4 (Version 4.0.9.4. nach Ringle, Wende & Becker, 2022) berechnet und die Darstellung der Ergebnisse der Konstruktreliabilität für T0, T1, T2, T3 und T4 erfolgt zu einem späteren Zeitpunkt.

Diskriminanzvalidität

Nach Nitzl (2010, S. 27 in Anlehnung an Ringle & Spreen, 2007, S. 213; Panten & Boßow-Thies, 2007, S. 322) soll eine Überprüfung der Diskriminanzvalidität erfolgen, da die Diskriminanzvalidität den methodischen Gegensatz zur Konvergenzvalidität darstellt und angibt, inwiefern sich die Indikatoren eines Konstrukts von den Indikatoren eines anderen Konstrukts unterscheiden. Nitzl (2010, S. 27) führt für die Überprüfung der Diskriminanzvalidität ein Kriterium an, nämlich das Fornell-Larcker-Kriterium. Dies besagt, dass die Diskriminanzvalidität nur dann erfüllt ist, wenn die Wurzel der DEV einer latenten Variable größer ist als jede Korrelation dieser latenten Variable mit einer anderen latenten Variable (siehe Abb. 20) (Nitzl, 2010, S. 27 in Anlehnung an Fornell & Larcker, 1981, S. 46). Nitzl (2010, S. 27) beschreibt, dass die grau markierten Kästchen aus Abbildung 20 die kritischen Größen markieren. Um das Fornell-Larcker-Kriterium zu erfüllen, soll beispielsweise $\sqrt{DEV\,\xi_1} \geq |\text{Korr}, (\xi_1\eta_1)|$ sein.

Nitzl (2010, S. 28 in Anlehnung an Chin, 1998b, S. 321) führt noch ein weiteres Kriterium für die Diskriminanzvaliditätsüberpüfung an, nämlich die sogenannte Kreuzladung. Die Kreuzladung ist eine Berechnung der Korrelation zwischen manifestierten Variablen mit anderen im Modell enthaltenen latenten Variablen (Nitzl, 2010, S. 28 in Anlehnung an Chin, 1998b, S. 321). Dabei soll jeder Indikator die stärkste Korrelation mit dem ihm zugeordneten Konstrukt haben, was bedeutet, dass die Faktorladung zwischen der manifestierten Variable und dem Konstrukt größer sein sollte als die Kreuzladungen (Nitzl, 2010, S. 28 in Anlehnung an Huber et al., 2007, S. 37). Wenn eine stärkere Beziehung zwischen einem Indikator und einem nicht zugeordneten Konstrukt existiert, soll das theoretische Modell neu überdacht werden (Nitzl, 2010, S. 28).

	ξ_1 (reflektiv)	ξ_2 (formativ)	η_1 (reflektiv)
ξ_1 (reflektiv)	$\sqrt{DEV(\xi_1)}$		
ξ_2 (formativ)	Korr. (ξ_1, ξ_2)	formativ	
η_1 (reflektiv)	Korr. (ξ_1, η_1)	Korr. (ξ_2, η_1)	$\sqrt{DEV(\eta_1)}$

Abbildung 20: Beispielhafte Darstellung der Diskriminanzvaliditätsüberpüfung für das PLS-Modell (Nitzl, 2010, S. 27)

Allerdings werden in der Literatur das Fornell-Larcker-Kriterium und die Berechnung der Kreuzladungen als ein Kriterium der Diskriminanzvalidität stark kritisiert (Henseler, Ringle & Sarstedt, 2015, S. 118 in Anlehnung an Rönkkö & Evermann, 2013). In ihrer Studie, in der die traditionellen Ansätze für die Berechnung der Diskriminanzvalidität verglichen werden, kommen Henseler, Ringle und Sarstedt (2015, S. 120) zu dem Ergebnis, dass das Fornell-Larcker-Kriterium und Kreuzladungen scheitern, Diskriminanzvaliditätsprobleme und Diskriminanzvaliditätsmängel zu identifizieren.

Henseler, Ringle und Sarstedt (2015, S. 121) führen ein alternatives Kriterium für die Bewertung der Diskriminanzvalidität an, nämlich das Kriterium heterotrait-monotrait ratio (HTMT). Der HTMT-Ansatz wird auch von Ringle, Wende und Becker (2022, S. 121) als Diskriminanzvaliditätskriterium empfohlen. Sie beschreiben, dass wenn der HTMT-Wert unter 0,90 liegt, die Diskriminanzvalidität zwischen zwei reflexiven Konstrukten gegeben ist (Ringle, Wende & Becker, 2022, S. 121 in Anlehnung an Gold et al., 2001; Teo et al., 2008).

Hingegen schlagen Römer, Schuberth und Henseler (2021, S. 2641) in ihrer Studie einen Wert von ≤ 0,945 für die HTMT-Ratio als Grenze für das Messmodell vor, wo die Diskriminanzvalidität gegeben ist.

Im Rahmen dieser Arbeit wird die Diskriminanzvalidität mithilfe von HTMT beurteilt und es wird sich dabei an einem Wert von ≤ 0,945 orientiert. Die Bewertung des HTMT-Kriteriums erfolgt in SmartPLS 4 und wird in den weiteren Kapiteln präsentiert. Im Folgenden werden die reflektiv gebildeten Messmodelle auf Reliabilität und Validität anhand der beschriebenen Gütekriterien überprüft und analysiert. Danach erfolgt die Beurteilung der Strukturmodelle.

Zusammenfassend sind die Beurteilungskriterien für die reflektiven Messmodelle in Tabelle 11 aufgeführt.

Tabelle 11: Zusammenfassung der Beurteilungskriterien für ein reflektives Messmodell

Gütemaß	Beschreibung	Empfohlener Wertebereich
Indikatorreliabilität	„Erklärungsgrad der Indikatorenvarianz durch das Konstrukt“ (Nitzl, 2010, S. 28 in Anlehnung an Krafft, Götz & Liehr-Gobbers, 2005, S. 75)	≥ 0,4 (vgl. Pelz, 2008, S. 156 in Anlehnung an Götz & Liehr-Gobbers, 2004, S. 727; Hulland, 1999, S. 198)

(Fortsetzung Tabelle 11)

Gütemaß	Beschreibung	Empfohlener Wertebereich
Konstruktreliabilität	Erklärungsgrad, wie hoch die Korrelation der Indikatoren ist, die einem Konstrukt zugeordnet sind (Nitzl, 2010, S. 28 in Anlehnung an Krafft, Götz & Liehr-Gobbers, 2005, S. 75)	≥ 0,6 (Nitzl, 2010, S. 26 in Anlehnung an Ringle & Spreen, 2007, S. 212)
Durchschnittlich erfasste Varianz	„Erklärungsgrad, wie hoch der durch die latente Variable erklärte Varianzanteil in Relation zum Messfehler ist" (Nitzl, 2010, S. 28 in Anlehnung an Krafft, Götz & Liehr-Gobbers, 2005, S. 75)	≥ 0,5 (Nitzl, 2010, S. 26 f. in Anlehnung an Huber et al., 2007, S. 36; Ringle & Spreen, 2007, S. 212)
Diskriminanzvalidität	Erklärungsgrad, wie „[...] sich die Indikatoren eines Konstrukts von denen eines anderen Konstrukts unterscheiden" (Nitzl, 2020, S. 27 in Anlehnung an Panten & Boßow-Thies, 2007, S. 322)	HTMT-Ansatz ≤ 0,945 (Römer, Schuberth & Henseler, 2021, S. 2641)

4.5.1.4 Gütekriterien des Strukturmodells

Nachdem die Beurteilung der reflektiv gemessenen Messmodelle erfolgte, ist es im zweiten Schritt möglich, die Beurteilung der Strukturmodelle durchzuführen. Nitzl (2010, S. 33 ff.) legt folgende Gütekriterien zur Beurteilung eines Strukturmodells dar:

Bestimmtheitsmaß

Bevor auf das Strukturmodell selbst eingegangen wird, wird dessen Erklärungskraft beurteilt. Dafür wurde für jedes latente endogene Konstrukt (Einstellung und Verhalten) das Bestimmtheitsmaß (R^2-Wert) definiert.

Das Bestimmtheitsmaß R^2 ist ein wichtiges Kriterium zur Beurteilung eines Strukturmodells, das den Anteil der erklärten Varianz im Verhältnis zur Gesamtvarianz darstellt (Nitzl, 2010, S. 33 in Anlehnung an Chin & Newsted, 1999, S. 316; Backhaus et al., 2006b, S. 66 f.). Nitzl (2010, S. 33) hebt hervor, dass an dieser Stelle der Varianzanteil einer endogenen Variable gemeint ist, der über die ihr zugeordneten latenten Variablen erklärt wird.

Der R^2-Wert ist auf einen standardisierten Wertebereich zwischen 0 und 1 festgelegt und gibt an, wie viel Prozent der Varianz einer latenten endogenen Variable über die ihr zugeordneten unabhängigen (exogenen) Variablen erklärt wird (Nitzl, 2010, S. 33). Ein Mindestwert ist aber von der zugrunde liegenden Forschungsfrage abhängig (Nitzl, 2010, S. 33 in Anlehnung an Harhoff & Wagner, 2009, S. 483). Nach Nitzl (2010, S. 33 in Anlehnung an Chin, 1998b, S. 323) gelten Werte für R^2 ab 0,67 als substanziell, ab 0,33 als moderat und ab 0,19 als schwach.

Das standardisierte Bestimmtheitsmaß für die Strukturmodelle in dieser Studie wurde mithilfe des PLS-Algorithmus geschätzt (SmartPLS 4, Version 4.0.9.4. nach Ringle, Wende & Becker, 2022). Die Ergebnisse werden an späterer Stelle entsprechend den Erhebungszeitpunkten präsentiert und diskutiert.

Pfadkoeffizientenanalyse

Bei der Pfadkoeffizientenanalyse handelt es sich um die Form einer multiplen Regressionsanalyse, die an Kausalzusammenhängen orientiert ist und in der nur einzelne Indikatoren für die jeweiligen Variablen des Kausalmodells eingesetzt werden (Nitzl, 2010, S. 34 in Anlehnung an Krafft, Götz & Liehr-Gobbers, 2005, S. 83). Standardisierte Pfadkoeffizienten können Werte zwischen 1 und –1 annehmen (Nitzl, 2010, S. 34 in Anlehnung an Ringle & Spreen, 2007, S. 214). Angaben zur Mindestgröße bei der Berechnung der Pfadkoeffizienten existieren nicht, jedoch führt Nitzl (2010 in Anlehnung an Ringle & Spreen, 2007) an, dass Werte nahe 0 eine schwache und Werte nahe 1 bzw. –1 eine starke Korrelation einer latenten Variable mit ihrem kausalen Nachfolger bedeuten. Nitzl (2010, S. 34 in Anlehnung an Chin, 1998a, S. 11) beschreibt zudem, dass Werte größer als 0,2 und unter -0,2 als bedeutsam angesehen werden.

Die Pfadkoeffizientenanalyse in den Strukturmodellen wurde mithilfe des PLS-Algorithmus geschätzt (SmartPLS 4, Version 4.0.9.4. nach Ringle, Wende & Becker, 2022). Die Ergebnisse der Pfadkoeffizientenanalyse werden in den weiteren Kapiteln entsprechend den Erhebungszeitpunkten vorgestellt.

Effektstärke

Nitzl (2010, S. 35 in Anlehnung an Chin, 1998b, S. 316) führt ein weiteres Gütekriterium für die Beurteilung des Strukturmodells, nämlich die Effektgröße f^2, an, die angibt, inwiefern und ob eine exogene Variable eine endogene latente Variable beeinflusst. Nitzl (2010, S. 35 in Anlehnung an Cohen, 1988, S. 410 ff.) präsentiert die folgende Formel zur Berechnung der Effektgröße (siehe Abb. 21):

$$f^2 = \frac{R^2_{eingeschlossen} - R^2_{ausgeschlossen}}{1 - R^2_{eingschlossen}}$$

Abbildung 21: Formel zur Berechnung der Effektgröße (Nitzl, 2010, S. 35 in Anlehnung an Cohen, 1988, S. 410 ff.)

Das Einflussergebnis einer exogenen auf eine endogene Variable basiert auf Änderungen des Bestimmtheitsmaßes R^2 der endogenen latenten Variable (Nitzl, 2010). Um die Änderungen des Bestimmtheitsmaßes R^2 zu berechnen, soll nach Nitzl (2010) ein Strukturmodell einmal mit der betrachteten exogenen Variable ($R^2_{eingeschlossen}$) und einmal ohne sie ($R^2_{ausgeschlossen}$) berechnet werden. Dabei entspricht ein f^2-Wert ab 0,02 einem geringen, ab 0,15 einem mittleren und ab 0,35 einem großen Einfluss von einer exogenen Variable auf eine endogene Variable (Nitzl, 2010, S. 35 in Anlehnung an Cohen, 1988, S. 413; Chin, 1998b, S. 46).

Dieses Gütekriterium ermöglicht es, durch Berücksichtigung zusätzlicher Pfade im Modell, auch bisher nicht hypothetisierte Strukturen zu überprüfen (Nitzl, 2010, S. 35 in Anlehnung an Huber et al., 2007, S. 46).

Die Berechnung der Effektstärke wurde in SmartPLS 4 (Version 4.0.9.4. nach Ringle, Wende & Becker, 2022) durchgeführt und wird zu einem späteren Zeitpunkt konkreter dargelegt.

Prognoserelevanz

Die Prognoserelevanz ist ein weiteres Beurteilungskriterium des Strukturmodells, die beschreibt, wie gut das aufgestellte Modell empirische Daten rekonstruieren kann (Nitzl, 2010, S. 36 in Anlehnung an Fornell & Cha, 1994, S. 72). Um einen relativen Prognoseeinfluss einer Variable auf eine endogene Variable zu untersuchen, nennt Nitzl (2010, S. 36) in Anlehnung an die Effektgröße f^2 folgende Formel:

$$Q^2 = 1 - \frac{\sum_D E_D}{\sum_D O_D}$$

Abbildung 22: Formel zur Berechnung der Effektgröße (Nitzl, 2010, S. 36)

Nach Nitzl (2010, S. 36) gibtE_D „[...] die quantitierten Fehler der geschätzten Werte und O_D die quadrierten Fehler der übrigen Originalwerte an".

Nitzl (2010, S. 37 in Anlehnung an Krafft, Götz & Liehr-Gobbers, 2005, S. 85) hebt hervor, dass ein Prognoserelevanzwert > 0 bedeutet, dass eine entsprechend Prognoserelevanz vorliegt. Eine negative Prognoserelevanz kann vorkommen und bedeutet, dass „[...] das verwendete Modell die Rohdaten nicht besser vorhersagen kann als eine einfache Schätzung mithilfe des Mittelwertes" (Nitzl, 2010, S. 37 in Anlehnung an Krafft, Götz & Liehr-Gobbers, 2005, S. 85).

Q^2 wurde mithilfe von SmartPLS 4 (Version 4.0.9.4. nach Ringle, Wende & Becker, 2022) berechnet, die Ergebnisse werden in den weiteren Kapiteln präsentiert.

Beurteilung des Gesamtmodells

Nach der Beurteilung des Messmodells und Strukturmodells soll die Beurteilung des Gesamtmodells im Rahmen der PLS-Methode erfolgen (Nitzl, 2010, S. 23 in Anlehnung an Schloderer, Ringle & Sarstedt, 2009, S. 589). Nitzl (2010, S. 39 in Anlehnung an Ringle, 2004, S. 26 f.; Huber et al., 2007, S. 43; Weiber & Mühlhaus, 2010, S. 259) legt dar, dass für PLS kein allgemein anerkanntes globales Gütemaß existiert, sind die zuvor genannten Gütekriterien jedoch erfüllt, wird von einer zuverlässigen Schätzung ausgegangen. Des Weiteren gilt, dass die Schätzung des Bestimmtheitsmaßes R^2 der Variablen angibt, wie gut das gesamte Modell ist. Allerdings kann laut Nitzl (2010, S. 39) selbst für ein Modell mit statistisch signifikanten Beziehungen und hohem R^2 ein besseres Modell mit einem noch höheren Erklärungswert zur Erklärung einer Zielvariable existieren. Nitzl (2010, S. 39 in Anlehnung an Diller, 2006, S. 612) weist jedoch auch darauf hin, dass Modelle mit einer hohen Anzahl von berücksichtigten Variablen und Beziehungen nicht immer die besten Modelle sind, da deren Aussagekraft und Praktikabilität durch zu viele Variablen, die berücksichtigt werden sollten, konterkariert werden kann.

Eins der wichtigsten Gütekriterien ist eine valide Schätzung der Pfade (Nitzl, 2010, S. 39), denn sie repräsentieren die vorab entwickelten hypothetischen Zusammenhänge und geben die Einflussstärke eines Konstruktes auf dessen kausalen Nachfolger an. Es ist im Interesse dieser Arbeit, die Pfade und den Einflussgrad zu überprüfen und herauszufinden, inwiefern die kausalen Nachfolger vom Konstrukt beeinflusst werden.

Der Forscher steht also vor der Entwicklung eines Modells vor der Herausforderung, ein effizientes Forschungsdesign zu erstellen, indem wesentliche von unwesentlichen Einflussvariablen getrennt werden (Nitzl, 2010, S. 40). Jedoch kann der Forscher den explorativen Charakter dieser methodischen Vorgehensweise nutzen, um eine Anzahl der möglichen Einflussvariablen und -indikatoren zu erheben und dann später auf Relevanz zu prüfen, indem man die Validität und Reliabilität der Ergebnisse nach den zuvor genannten Regeln überprüft (Nitzl, 2010, S. 40 in Anlehnung an Wold, 1980, S. 70).

Es erfolgen nun im weiteren Verlauf die Überprüfung und Analyse der Messmodelle und Strukturmodelle zu jedem Erhebungspunkt anhand der zuvor genannten Gütekriterien.

4.5.2 Beurteilung der Ergebnisse der ersten Erhebung T0 nach Gütekriterien

4.5.2.1 T0-Ergebnisse der Messmodelle

In diesem Kapitel sollen die Ergebnisse aller Messmodelle (inklusive E-Mail-Bearbeitung) präsentiert werden. Dadurch, dass die Vorgehensweise und die Berechnung mit dem statistischen Programm SmartPLS 4 (Version 4.0.9.4. nach Ringle, Wende & Becker, 2022) dargelegt wurden, werden die Ergebnisse in tabellarischer Form vorgestellt.

Wie schon erwähnt wurde, sollen die Messmodelle den Mindestanforderungen der folgenden Gütekriterien entsprechen, um Konvergenzreliabilität nachzuweisen (siehe Kapitel 4.5.1.3):

- Indikatorenreliabilität: Die Indikatoren sollen einen Wert größer als 0,4 aufweisen
- Das DEV-Wert soll größer als 0,5 sein
- KR soll einen Wert von über 0,6 aufweisen
- Die Messmodelle sollen die Mindestanforderungen des Gütekriteriums Diskriminanzvalidität (HTMT ≤ 0,945) erfüllen, um die Validität nachweisen zu können

Zuerst soll die Indikatorenreliabilität aller fünf Kontexte vorgestellt werden. Die Faktorladungen der Indikatoren aller fünf Kontexte können in Tabelle 12 eingesehen werden. Dabei wurden einige Indikatoren aus den Messmodellen eliminiert und in die finale Ergebnisdarstellung nicht inkludiert. Obwohl einige der eliminierten Indikatoren das oben genannte Kriterium einer Minimumladung von 0,4 erfüllten, können sie nicht für die Berechnung der Messmodelle verwendet werden, da sie nicht zur Gewährleistung einer guten Datenqualität (Erfüllung von Reliabilitäts- und Validitätsanforderungen) beitragen.

Tabelle 12: Faktorladungen der genutzten Items aus Erhebungszeitpunkt T0

Kontext	Indikator	Faktorladung
E-Mail-Bearbeitung	EMW03	0,879
	EMW04	0,703
	EME01	0,837
	EME03	0,724
	EMV01	0,513
	EMV03	0,951
Passwortmanagement	PWW02	0,970
	PWW03	0,943
	PWE01	0,935
	PWE03	0,611
	PWV01	0,533
	PWV04	0,914
Umgang mit Informationen u. a. im Kontext mobiler Arbeit	SEW04	0,715
	SEW03	0,851
	SEE02	0,888
	SEE03	0,659
	SEV04	0,821
	SEV05	0,771
Umgang mit (mobilen) Speicher- und Endgeräten	BEW03	1,000
	BEE01	0,950
	BEE02	0,885
	BEV01	0,778
	BEV02	0,872
Zutritts- und Zugriffsschutz	MVW01	0,760
	MVW03	0,786
	MVE01	1,000
	MVV01	0,824
	MVV02	0,804
	MVV03	0,724

Parallel konnten die DEV und die KR jedes Modells aus SmartPLS 4 entnommen werden (nach Ringle, Wende & Becker, 2022), die in Tabelle 13 aufgelistet sind. Die DEV und die KR konnten für das Konstrukt „Wissen" im Kontext „Umgang mit (mobilen) Speicher- und Endgeräten" und das Konstrukt „Einstellung" im Kontext „Zutritts- und Zugriffschutz" nicht berechnet werden, da diese Konstrukte durch ein sogenanntes Single-Item erklärt werden. Wie die weiteren DEV-Ergebnisse zeigen, hat die DEV aller Messmodelle einen ausreichend hohen Wert (≥ 0,5), was impliziert, dass mindestens die Hälfte der Varianz eines Konstrukts durch die ihm zugeordneten Indikatoren erklärt wird. Laut den KR-Ergebnissen korrelieren die Indikatoren, die einer latenten Variable zugeordnet sind, untereinander stark und zeigen Werte von ≥ 0,6 in allen Messmodellen. Das heißt, dass die KR für alle fünf Messmodelle der T0-Erhebung erfüllt ist. Wie die Ergebnisse zeigen, sind die Gütekriterien damit gewährleistet.

Tabelle 13: DEV und KR der Messmodelle aus dem Erhebungszeitpunkt T0

Kontext	Konstrukt	DEV	KR
E-Mail-Bearbeitung	Wissen	0,633	0,773
	Einstellung	0,612	0,758
	Verhalten	0,584	0,721
Passwortmanagement	Wissen	0,915	0,956
	Einstellung	0,624	0,760
	Verhalten	0,560	0,704
Umgang mit Informationen u. a. im Kontext mobiler Arbeit	Wissen	0,618	0,763
	Einstellung	0,612	0,755
	Verhalten	0,634	0,766
Umgang mit (mobilen) Speicher- und Endgeräten	Einstellung	0,842	0,914
	Verhalten	0,683	0,811
Zutritts- und Zugriffsschutz	Wissen	0,597	0,748
	Verhalten	0,617	0,828

Des Weiteren soll die Diskriminanzvalidität der Messmodelle berechnet werden, um deren Validität zu gewährleisten. Wie schon erwähnt wurde, wird in dieser Arbeit die Diskriminanzvalidität mithilfe der HTMT-Methode beurteilt (siehe Kapitel 4.5.1.3), wobei sich in dieser Arbeit an einem Wert ≤ 0,945 orientiert wird (vgl. Römer, Schuberth & Henseler, 2021, S. 2641). Die Ergebnisse der HTMT-Analyse können aus Tabelle 14 entnommen werden. Wie die Ergebnisse zeigen, kann die Diskriminanzvalidität zwischen allen reflektiven Konstrukten in den Messmodellen festgestellt werden, bis auf den Kontext „Zutritts- und Zugriffsschutz" (Konstruktpfad „Wissen auf Einstel-

lung“). Es wurde jedoch entschieden, das Konstrukt nicht aus der Beurteilung der Messmodelle zu eliminieren, da die restlichen Gütekriterien erfüllt sind.

Tabelle 14: HTMT-Ratio für die Messmodelle aus dem Erhebungszeitpunkt T0

	E-Mail-Bearbeitung	Passwort-management	Umgang mit Informationen u. a. im Kontext mobiler Arbeit	Umgang mit (mobilen) Speicher- und Endgeräten	Zutritts- und Zugriffsschutz
Wissen ↔ Einstellung	0,377	0,611	0,258	0,434	1,032
Wissen ↔ Verhalten	0,306	0,194	0,482	0,713	0,835
Einstellung ↔ Verhalten	0,720	0,522	0,522	0,886	0,380

Nach der Beurteilung der Validität und Reliabilität der Konstrukte in den Messmodellen kann die Analyse der Strukturmodelle beginnen. Im nächsten Kapitel werden die Ergebnisse der Strukturmodelle präsentiert.

4.5.2.2 T0-Ergebnisse der Strukturmodelle

Wie bereits erwähnt, führt Nitzl (2010, S. 33 in Anlehnung an Chin & Newsted, 1999, S. 316) ein Kriterium für die Bewertung der Strukturmodelle ein, und zwar das Bestimmtheitsmaß. Für jedes latente endogene Konstrukt (Einstellung und Verhalten) soll das Bestimmtheitsmaß (R^2-Wert) eingeschätzt und bestimmt werden. Die Ergebnisse des Bestimmtheitsmaßes R^2 für die Strukturmodelle sind in Tabelle 15 dargestellt.

Tabelle 15: Übersicht über das Bestimmtheitsmaß R^2 für T0

	E-Mail-Bearbeitung	Passwort-management	Umgang mit Informationen u. a. im Kontext mobiler Arbeit	Umgang mit (mobilen) Speicher- und Endgeräten	Zutritts- und Zugriffsschutz
Einstellung R^2	0,024	0,187	0,013	0,174	0,342
Verhalten R^2	0,099	0,022	0,095	0,460	0,178

Daraus ergibt sich, dass ein eher schwacher R^2-Wert für die Einstellung für alle Kontexte vorliegt. Im Kontext „Zutritts- und Zugriffsschutz“ ist der R^2-Wert im Konstrukt „Einstellung“ am höchsten und weist einen moderaten Wert auf. Im Konstrukt „Verhalten“ weisen die R^2-Werte niedrige Wert auf, bis auf den Kontext „Umgang mit (mobilen) Speicher- und Endgeräten“, wo dieser Wert moderat ist.

Im Folgenden soll die Berechnung der Signifikanz der Pfadkoeffizienten erfolgen. Diese wurde mit SmartPLS 4 (Version 4.0.9.4. nach Ringle, Wende & Becker, 2022) durchgeführt. Die Ergebnisse können Tabelle 16 entnommen werden. Nitzl

(2010, S. 34 in Anlehnung an Chin, 1998a, S. 11) beschreibt, dass Werte der Pfadkoeffizienten größer als 0,2 und unter -0,2 als bedeutsam angesehen werden.

Für die meisten Kontexte wurde eine starke Korrelation zwischen der Variable „Wissen" mit ihrem kausalen Nachfolger „Einstellung" identifiziert, außer in den Kontexten „E-Mail-Bearbeitung" und „Umgang mit Informationen u. a. im Kontext mobiler Arbeit", wo die Korrelation niedrig ist.

Tabelle 16: Ergebnisse der Pfadkoeffizienten der Strukturmodelle für T0

Pfad	E-Mail-Bearbeitung	Passwort-management	Umgang mit Informationen u. a. im Kontext mobiler Arbeit	Umgang mit (mobilen) Speicher- und Endgeräten	Zutritts- und Zugriffsschutz
Wissen → Einstellung	0,154	0,432	0,112	0,418	0,585
Einstellung → Verhalten	0,318	0,132	0,235	0,436	0,128
Wissen → Verhalten	–0,052	0,032	–0,227	0,368	0,335

Im Pfad „Einstellung auf Verhalten" korreliert die latente Variable „Einstellung" wenig mit deren kausalem Nachfolger „Verhalten" in den Kontexten „Passwortmanagement" und „Zutritts- und Zugriffsschutz". Die Korrelation von Einstellung mit Verhalten ist in den anderen Kontexten stark, allerdings im Kontext „Umgang mit (mobilen) Speicher- und Endgeräten" am signifikantesten.

Auf dem Pfad „Wissen auf Verhalten" findet sich eine starke Korrelation von Wissen mit Verhalten in den Kontexten „Umgang mit Informationen u. a. im Kontext mobiler Arbeit", „Umgang mit (mobilen) Speicher- und Endgeräten" sowie „Zutritts- und Zugriffsschutz". In den anderen beiden Kontexten konnte hingegen festgestellt werden, dass die Korrelation zwischen Wissen und Verhalten eher geringer ist.

Die Effektstärke ist ein weiteres Gütekriterium für die Beurteilung von Strukturmodellen. Nach Nitzl (2010, S. 35 in Anlehnung an Chin, 1998b, S. 316) stellt die Effektgröße f^2 dar, wie groß der Einfluss einer exogenen Variable auf eine endogene latente Variable ist. In Tabelle 17 sind die Ergebnisse für die Effektstärke aller fünf Kontexte zum Zeitpunkt T0 aufgelistet.

Daraus ergibt sich, dass der Einfluss der exogenen Variable „Wissen" auf die endogene Variable „Einstellung" am stärksten im Kontext „Zutritts- und Zugriffsschutz" und am geringsten im Kontext „Umgang mit Informationen u. a. im Kontext mobiler Arbeit" ist. Im Kontext „E-Mail-Bearbeitung" ist der Einfluss der exogenen Variable „Wissen" auf die endogene Variable „Einstellung" auch niedrig und in den übrigen Kontexten ist dieser Einfluss moderat.

Der Einfluss der Variable „Einstellung" auf die Variable „Verhalten" ist in allen Kontexten insignifikant, bis auf den Kontext „Umgang mit (mobilen) Speicher- und Endgeräten", wo dieser Einfluss moderat ist.

Der Einfluss der exogenen Variable „Wissen“ auf die endogene Variable „Verhalten“ ist im Kontext „Umgang mit (mobilen) Speicher- und Endgeräten“ moderat und in den anderen Kontexten eher gering.

Tabelle 17: Ergebnisse der Effektstärke (f^2) in den Strukturmodellen für Erhebungszeitpunkt T0

	E-Mail-Bearbeitung	Passwort-management	Umgang mit Informationen u. a. im Kontext mobiler Arbeit	Umgang mit (mobilen) Speicher- und Endgeräten	Zutritts- und Zugriffsschutz
Wissen → Einstellung	0,024	0,230	0,013	0,211	0,520
Einstellung → Verhalten	0,109	0,015	0,060	0,291	0,013
Wissen → Verhalten	0,003	0,001	0,056	0,207	0,090

Die Prognoserelevanz ist das letzte Gütekriterium nach Nitzl (2010) und beschreibt, wie gut das Modell die Daten rekonstruieren kann (siehe Kapitel 4.5.1.4). Die Berechnungen Q^2 für den Erhebungszeitpunkt T0 für alle Kontexte außer „E-Mail-Bearbeitung“ (Konstrukt Einstellung und Verhalten), „Passwortmanagement“ (Konstrukt Verhalten) und „Umgang mit Informationen u. a. im Kontext mobiler Arbeit (Konstrukt Verhalten) weisen einen positiven Wert auf, was impliziert, dass eine Prognoserelevanz vorhanden ist. Wie schon erwähnt wurde, kann das verwendete Modell einen negativen Wert aufweisen, was nach Nitzl (2010, S. 37 in Anlehnung an Krafft, Götz, & Liehr-Gobbers, 2005, S. 85) bedeutet, dass die Prognoseschätzung des verwendeten Modells genauso anwendbar wie eine einfache Schätzung mithilfe des Mittelwertes ist (siehe Tabelle 18).

Tabelle 18: Ergebnisse der Prognoserelevanz der Strukturmodelle für Erhebungszeitpunkt T0

	E-Mail-Bearbeitung	Passwort-management	Umgang mit Informationen u. a. im Kontext mobiler Arbeit	Umgang mit (mobilen) Speicher- und Endgeräten	Zutritts- und Zugriffsschutz
Q^2 Einstellung	–0,041	0,140	–0,030	0,150	0,315
Q^2 Verhalten	–0,050	–0,034	–0,026	0,275	0,118

Folglich konnte nachgewiesen werden, dass die Messmodelle sowie die Strukturmodelle für alle fünf Kontexte zum Erhebungszeitpunkt T0 zuverlässig sind.

In den folgenden Kapiteln werden die Ergebnisse aus den Erhebungen T1, T2, T3 und T4 diskutiert. Auf eine Zusammenfassung der Ergebnisse hinsichtlich der gestellten Hypothesen und eine Darstellung im Zeitverlauf wird in den einzelnen Unterkapiteln verzichtet. Eine diesbezügliche zusammenfassende Darstellung erfolgt abschließend nach der Beschreibung der T4-Erhebungsergebnisse.

4.5.3 Beurteilung der Ergebnisse der zweiten Erhebung T1 nach Gütekriterien

4.5.3.1 T1-Ergebnisse der Messmodelle

Die weiteren Erhebungszeitpunkte folgen derselben Auswertungsstruktur wie zuvor im Kapitel für die Auswertung der Messmodelle zum Zeitpunkt T0 vorgestellt. Für die T1-Erhebung kann gezeigt werden, dass die Faktorladungen der genutzten Indikatoren im Modell größer als 0,4 sind. Diese werden in Tabelle 19 dargestellt. Einige Indikatoren mussten allerdings aus den Messmodellen entfernt werden, damit die restlichen Gütekriterien erfüllt werden können.

Tabelle 19: Faktorladungen der genutzten Items aus Erhebungszeitpunkt T1

Kontext	Indikator	Ladung
E-Mail-Bearbeitung	EMW01	0,590
	EMW02	0,841
	EMW03	0,779
	EME02	1,000
	EMV02	0,777
	EMV04	0,879
Passwortmanagement	PWW01	0,522
	PWW02	0,965
	PWE01	0,840
	PWE04	0,655
	PWV02	0,826
	PWV04	0,913
Umgang mit Informationen u. a. im Kontext mobiler Arbeit	SEW01	0,540
	SEW02	0,992
	SEE03	0,853
	SEE02	0,606
	SEV04	0,425
	SEV05	0,981
Umgang mit (mobilen) Speicher- und Endgeräten	BEW02	0,598
	BEW03	0,832
	BEE03	0,946
	BEE01	0,884
	BEV01	1,000

(Fortsetzung Tabelle 19)

Kontext	Indikator	Ladung
Zutritts- und Zugriffsschutz	MVW01	0,666
	MVW02	0,705
	MVW03	0,811
	MVE01	0,820
	MVE02	0,798
	MVV01	0,866
	MVV02	0,906
	MVV03	0,846

Parallel können in SmartPLS 4 (Version 4.0.9.4. nach Ringle, Wende & Becker, 2022) die DEV und KR entnommen werden. Die DEV und die KR konnten für das Konstrukt „Einstellung" im Kontext „E-Mail-Bearbeitung" und das Konstrukt „Verhalten" nicht berechnet werden, da diese Konstrukte durch ein sogenanntes Single-Item erklärt werden. Wie Tabelle 20 zeigt, sind die DEV-Werte für alle weiteren Kontexte größer als 0,5 und somit kann davon ausgegangen werden, dass die Konvergenzvalidität erfüllt ist. Auch die KR-Werte der anderen Konstrukten sind größer als 0,6. Daher ist gewährleistet, dass das Konstruktreliabilitätskriterium erfüllt ist.

Tabelle 20: DEV und KR der Messmodelle aus dem Erhebungszeitpunkt T1

Kontext	Konstrukt	DEV	KR
E-Mail-Bearbeitung	Wissen	0,554	0,815
	Verhalten	0,688	0,785
Passwortmanagement	Wissen	0,601	0,735
	Einstellung	0,574	0,727
	Verhalten	0,757	0,862
Umgang mit Informationen u. a. im Kontext mobiler Arbeit	Wissen	0,637	0,764
	Einstellung	0,547	0,701
	Verhalten	0,572	0,698
Umgang mit (mobilen) Speicher- und Endgeräten	Wissen	0,525	0,683
	Einstellung	0,838	0,912
Zutritts- und Zugriffsschutz	Wissen	0,533	0,773
	Einstellung	0,655	0,791
	Verhalten	0,763	0,906

Im nächsten Schritt soll die Diskriminanzvalidität anhand der HTMT-Ratio analysiert werden. Wie Tabelle 21 zeigt, können alle Messmodelle bis auf die Kontexte „Umgang mit (mobilen) Speicher- und Endgeräten“ (Konstruktpfad „Wissen auf Verhalten“) und „Zutritts- und Zugriffsschutz“ (Konstruktpfad „Wissen auf Einstellung“ und „Wissen auf Verhalten“) eine Diskriminanzvalidität nachweisen. Auch im Kontext „E-Mail-Bearbeitung“ (Konstruktpfad „Wissen auf Verhalten“) ist die Diskriminanzvalidität leicht erhöht. Es wurde jedoch entschieden, die Konstrukte nicht aus der Beurteilung der Messmodelle zu eliminieren, da die restlichen Gütekriterien erfüllt sind.

Tabelle 21: HTMT-Ratio für die Messmodelle aus dem Erhebungszeitpunkt T1

	E-Mail-Bearbeitung	Passwort-management	Umgang mit Informationen u. a. im Kontext mobiler Arbeit	Umgang mit (mobilen) Speicher- und Endgeräten	Zutritts- und Zugriffsschutz
Wissen ↔ Einstellung	0,185	0,427	0,217	0,625	1,140
Wissen ↔ Verhalten	0,947	0,831	0,286	1,053	0,980
Einstellung ↔ Verhalten	0,040	0,156	0,696	0,048	0,917

Als Ergebnis lässt sich festhalten, dass die Analyse der Messmodelle eine Basis bildet, um die Strukturmodelle zu beurteilen. Im nächsten Kapitel wird die Analyse der Strukturmodelle für den Erhebungszeitpunkt T1 dargelegt.

4.5.3.2 T1-Ergebnisse der Strukturmodelle

Zuerst soll das Bestimmtheitsmaß R^2 für jedes latente endogene Konstrukt (Einstellung und Verhalten) im Strukturmodell berechnet werden (Nitzl, 2010, S. 33 in Anlehnung an Chin & Newsted, 1999, S. 316). Die Berechnung wurde in SmartPLS 4 (Version 4.0.9.4. nach Ringle, Wende & Becker, 2022) durchgeführt und die Ergebnisse können aus Tabelle 22 entnommen werden.

Tabelle 22: Übersicht über das Bestimmtheitsmaß R^2 für T1

	E-Mail- Bearbeitung	Passwort-management	Umgang mit Informationen u. a. im Kontext mobiler Arbeit	Umgang mit (mobilen) Speicher- und Endgeräten	Zutritts- und Zugriffsschutz
Einstellung R^2	0,021	0,020	0,001	0,034	0,343
Verhalten R^2	0,320	0,319	0,076	0,119	0,564

Basierend auf den Gütekriterien für Strukturmodelle kann für alle Konstrukte in allen Kontexten ein Bestimmtheitsmaß nachgewiesen werden, allerdings ist das Bestimmtheitsmaß nur im Kontext „Zutritts- und Zugriffsschutz“ moderat.

Die Ergebnisse der Berechnung der Pfadkoeffizienten (s. Tabelle 23) zeigen, dass der Pfad „Wissen auf Einstellung“ in allen Kontexten eine relativ geringe Korrelation zwischen der latenten Variable „Wissen“ und ihrem kausalen Nachfolger „Einstellung“ hat, bis auf den Kontext „Zutritts- und Zugriffsschutz“, wo die Variable „Wissen“ stark mit der Variable „Einstellung“ korreliert.

Der Pfad „Einstellung auf Verhalten“ zeigt nur in den Kontexten „Umgang mit Informationen u. a. im Kontext mobiler Arbeit“ und „Zutritts- und Zugriffsschutz“ eine stärkere Korrelation zwischen der Variable „Einstellung“ und ihrem kausalen Nachfolger „Verhalten“, in allen anderen Kontexten ist dieser Zusammenhang weniger signifikant.

Betrachtet man den Pfad „Wissen auf Verhalten“, hat die latente Variable „Wissen“ ein signifikantes Korrelationsniveau mit ihrem Nachfolger „Verhalten“, bis auf den Kontext „Umgang mit Informationen u. a. im Kontext mobiler Arbeit“, wo die Korrelation gering ist.

Tabelle 23: Ergebnisse der Pfadkoeffizienten der Strukturmodelle für T1

Pfad	E-Mail- Bearbeitung	Passwort-management	Umgang mit Informationen u. a. im Kontext mobiler Arbeit	Umgang mit (mobilen) Speicher- und Endgeräten	Zutritts- und Zugriffsschutz
Wissen → Einstellung	0,145	–0,142	–0,028	0,185	0,585
Einstellung → Verhalten	–0,050	0,108	0,213	–0,016	0,238
Wissen → Verhalten	0,571	0,570	0,182	0,348	0,587

Im nächsten Schritt soll die Effektstärke (f^2) der Konstrukte in den Strukturmodellen berechnet werden (siehe Tabelle 24). Laut den Gütekriterien für die Effektstärke (f^2) sind die Ergebnisse des Pfades „Wissen auf Einstellung“ in allen Kontexten insignifikant, außer im Kontext „Zutritts- und Zugriffsschutz“.

Der Einfluss der Variable „Einstellung“ auf die Variable „Verhalten“ ist in allen Kontexten gering.

Die Ergebnisse der Effektstärke (f^2) zeigen, dass der Einfluss der Variable „Wissen“ auf die Variable „Verhalten“ in den Kontexten „E-Mail-Bearbeitung“, „Passwortmanagement“ und „Zutritts- und Zugriffsschutz“ signifikant ist, während der Einfluss in den Kontexten „Umgang mit Informationen u. a. im Kontext mobiler Arbeit“ und „Umgang mit (mobilen) Speicher- und Endgeräten“ gering ist.

Tabelle 24: Ergebnisse der Effektstärke (f^2) der Strukturmodelle für Erhebungszeitpunkt T1

	E-Mail-Bearbeitung	Passwort-management	Umgang mit Informationen u. a. im Kontext mobiler Arbeit	Umgang mit (mobilen) Speicher- und Endgeräten	Zutritts- und Zugriffsschutz
Wissen → Einstellung	0,022	0,021	0,001	0,035	0,521
Einstellung → Verhalten	0,004	0,017	0,049	0,0002	0,085
Wissen → Verhalten	0,470	0,468	0,036	0,132	0,519

Das letzte Prüfkriterium, was die Strukturmodelle erfüllen sollen, ist die Prognoserelevanz. Die Ergebnisse der Prognoserelevanz können aus Tabelle 25 entnommen werden. Generell kann in allen Kontexten im Konstrukt Verhalten eine positive Prognoserelevanz nachgewiesen werden. Für das Konstrukt „Einstellung" kann nur eine positive Q^2 in den Kontexten „Umgang mit (mobilen) Speicher- und Endgeräten" und „Zutritts- und Zugriffsschutz" identifiziert werden. Wie schon erwähnt, kann der Q^2-Wert eine negative Prognoserelevanz aufweisen. Dies bedeutet, dass der Vorhersagefehler der PLS-Ergebnisse größer ist als der Vorhersagefehler bei der einfachen Verwendung der Mittelwerte (Nitzl, 2010, S. 37 in Anlehnung an Krafft, Götz & Liehr-Gobbers, 2005, S. 85).

Tabelle 25: Ergebnisse der Prognoserelevanz der Strukturmodelle für Erhebungszeitpunkt T1

	E-Mail-Bearbeitung	Passwort-management	Umgang mit Informationen u. a. im Kontext mobiler Arbeit	Umgang mit (mobilen) Speicher- und Endgeräten	Zutritts- und Zugriffsschutz
Q^2 Einstellung	–0,031	–0,014	–0,025	0,003	0,264
Q^2 Verhalten	0,259	0,235	0,002	0,076	0,477

Somit kann die Schlussfolgerung gezogen werden, dass alle Konstrukte in allen Kontexten, bis auf den Konstruktpfad „Einstellung auf Verhalten" im Kontext „Umgang mit (mobilen) Speicher- und Endgeräten", alle Gütekriterien erfüllen. Dadurch, dass der Konstruktpfad die restlichen Anforderungen sowohl im Mess- als auch im Strukturmodell erfüllt, wurde entschieden, das Konstrukt nicht zu eliminieren, sondern in die Gesamtbeurteilung zu inkludieren.

4.5.4 Beurteilung der Ergebnisse der dritten Erhebung T2 nach Gütekriterien

4.5.4.1 T2-Ergebnisse der Messmodelle

Auch die Erhebungszeitpunkte der Kontrollgruppe folgen derselben Auswertungsstruktur wie zuvor in Kapitel 4.5.1 vorgestellt. Für die T2-Erhebung kann gezeigt wer-

den, dass die Faktorladungen der genutzten Indikatoren im Modell größer als 0,4 sind und eine signifikante Ladung aufweisen (Tabelle 26). Diese werden in der nachfolgenden Tabelle aufgeführt. Jedoch wurden einige Indikatoren aus den Messmodellen eliminiert, um die restlichen Gütekriterien zu erfüllen.

Tabelle 26: Faktorladungen der genutzten Items aus Erhebungszeitpunkt T2

Kontext	Indikator	Ladung
E-Mail-Bearbeitung	EMW01	0,858
	EMW03	0,859
	EME01	0,516
	EME02	0,966
	EMV02	0,838
	EMV03	0,754
	EMV04	0,792
Passwortmanagement	PWW02	0,963
	PWW04	0,427
	PWE02	0,953
	PWE04	0,553
	PWV01	0,796
	PWV02	0,699
	PWV04	0,880
Umgang mit Informationen u. a. im Kontext mobiler Arbeit	SEW03	0,727
	SEW04	0,905
	SEE02	0,928
	SEE03	0,531
	SEV04	0,463
	SEV05	0,975
Umgang mit (mobilen) Speicher- und Endgeräten	BEW01	0,485
	BEW02	0,969
	BEE01	0,826
	BEE02	0,849
	BEE03	0,801
	BEV01	0,698
	BEV02	0,895

(Fortsetzung Tabelle 26)

Kontext	Indikator	Ladung
Zutritts- und Zugriffsschutz	MVW01	0,767
	MVW03	0,884
	MVE01	0,843
	MVE03	0,768
	MVV02	0,839
	MVV03	0,785
	MVV04	0,792

Weiter sollen die DEV und die KR jedes Messmodells berechnet werden. Die Berechnung ist in SmartPLS 4 (Version 4.0.9.4. nach Ringle, Wende & Becker, 2022) erfolgt. Die Ergebnisse der DEV- und KR-Berechnungen der Messmodelle für alle fünf Kontexte können aus Tabelle 27 entnommen werden. Generell weist die DEV einen ausreichenden Wert (> 0,5) auf und somit erfüllen alle Messmodelle dieses Kriterium. Außerdem zeigen die Ergebnisse der Messmodelle, dass die KR in allen Kontexten > 0,6 liegt, sodass alle Messmodelle die Anforderungen dieses Kriteriums erfüllen.

Tabelle 27: DEV und KR der Messmodelle aus dem Erhebungszeitpunkt T2

Kontext	Konstrukt	DEV	KR
E-Mail-Bearbeitung	Wissen	0,737	0,849
	Einstellung	0,600	0,733
	Verhalten	0,633	0,838
Passwortmanagement	Wissen	0,555	0,684
	Einstellung	0,607	0,743
	Verhalten	0,632	0,836
Umgang mit Informationen u. a. im Kontext mobiler Arbeit	Wissen	0,674	0,803
	Einstellung	0,571	0,713
	Verhalten	0,580	0,710
Umgang mit (mobilen) Speicher- und Endgeräten	Wissen	0,587	0,719
	Einstellung	0,682	0,865
	Verhalten	0,644	0,781
Zutritts- und Zugriffsschutz	Wissen	0,685	0,812
	Einstellung	0,650	0,788
	Verhalten	0,649	0,847

Das letzte Gütekriterium, was die Messmodelle erfüllen sollen, ist die Diskriminanzvalidität (siehe Kapitel 4.5.1.3). Die Ergebnisse der Messmodelle belegen die Validität der Messmodelle des Erhebungszeitpunkts T2. Eine Ausnahme bildet nur der Kontext „Umgang mit (mobilen) Speicher- und Endgeräten“ (Konstruktpfad „Wissen auf Einstellung“), wo die HTMT-Ratio leicht erhöht ist. Es wurde jedoch entschieden, das Konstrukt nicht aus der Beurteilung der Messmodelle zu eliminieren, da die restlichen Gütekriterien erfüllt sind.

Nach der Bewertung der Daten der Messmodelle für den Erhebungszeitpunkt T2 anhand von Gütekriterien kann die Schlussfolgerung gezogen werden, dass die Daten valide und qualitativ ausreichend sind und für die Analyse der Strukturmodelle verwendet werden können.

Tabelle 28: HTMT-Ratio für die Messmodelle aus dem Erhebungszeitpunkt T2

	E-Mail-Bearbeitung	Passwort-management	Umgang mit Informationen u. a. im Kontext mobiler Arbeit	Umgang mit (mobilen) Speicher- und Endgeräten	Zutritts- und Zugriffsschutz
Wissen ↔ Einstellung	0,583	0,903	0,874	1,282	0,942
Wissen ↔ Verhalten	0,944	0,790	0,437	0,711	0,442
Einstellung ↔ Verhalten	0,503	0,421	0,226	0,933	0,749

4.5.4.2 T2-Ergebnisse der Strukturmodelle

Zuerst soll das Bestimmtheitsmaß R^2 für jedes latente endogene Konstrukt (Einstellung und Verhalten) in den Strukturmodellen berechnet werden. Die Ergebnisse können Tabelle 29 entnommen werden. Generell zeigen die Ergebnisse, dass das Bestimmtheitsmaß R^2 im Konstrukt „Einstellung“ im Kontext „Umgang mit (mobilen) Speicher- und Endgeräten“ moderat ist, in allen anderen Kontexten des Konstruktes „Einstellung“ fällt es gering aus. Im Konstrukt „Verhalten“ weisen die Kontexte einen moderaten Bestimmtheitsmaßwert auf. Ausgenommen sind die Kontexte „Passwortmanagement“ und „Umgang mit Informationen u. a. im Kontext mobiler Arbeit“, wo das Bestimmtheitsmaß R^2 gering ist.

Tabelle 29: Übersicht über das Bestimmtheitsmaß R^2 für T2

	E-Mail-Bearbeitung	Passwort-management	Umgang mit Informationen u. a. im Kontext mobiler Arbeit	Umgang mit (mobilen) Speicher- und Endgeräten	Zutritts- und Zugriffsschutz
Einstellung R^2	0,120	0,016	0,148	0,575	0,038
Verhalten R^2	0,426	0,245	0,098	0,410	0,522

Danach wurde die Pfadkoeffizientenanalyse durchgeführt. Die Ergebnisse der Pfadkoeffizientenanalyse können Tabelle 30 entnommen werden.

Wie die Ergebnisse zeigen, ist die Korrelation im Pfad „Wissen auf Einstellung" in allen Kontexten stark, wobei die die Korrelation zwischen Wissen und Einstellung in den Kontexten „Passwortmanagement" und „Zutritts- und Zugriffsschutz" niedrig ist.

Im Pfad „Einstellung auf Verhalten" können die meisten Pfadkoeffizienten als stark erachtet werden, wobei diese in den Kontexten „E-Mail-Bearbeitung" und „Umgang mit Informationen u. a. im Kontext mobiler Arbeit" gering sind.

Beim Pfad „Wissen auf Verhalten" sind die Pfadkoeffizienten in allen Kontexten stark, was belegt, dass die Variable „Wissen" mit der Variable „Verhalten" stark korreliert.

Tabelle 30: Ergebnisse der Pfadkoeffizienten in den Strukturmodellen für T2

Pfad	E-Mail- Bearbeitung	Passwortmanagement	Umgang mit Informationen u. a. im Kontext mobiler Arbeit	Umgang mit (mobilen) Speicher- und Endgeräten	Zutritts- und Zugriffsschutz
Wissen → Einstellung	0,347	0,126	0,385	0,759	0,195
Einstellung → Verhalten	0,134	0,254	0,147	0,873	0,340
Wissen → Verhalten	0,594	0,394	–0,339	–0,369	0,574

Im Weiteren soll die Effektstärke (f^2) der Strukturmodelle für den Erhebungszeitpunkt T2 betrachtet werden. Die Berechnung wurde mit SmartPLS 4 (Version 4.0.9.4. nach Ringle, Wende & Becker, 2022) durchgeführt. Die Ergebnisse sind in Tabelle 31 präsentiert.

Wie die Ergebnisse der Strukturmodellbeurteilung zeigen, ist die Effektstärke des Pfades „Wissen auf Einstellung" im Kontext „Umgang mit (mobilen) Speicher- und Endgeräten" am größten, was besagt, dass in diesen Fällen die exogene Variable „Wissen" einen großen Einfluss auf die endogene Variable „Einstellung" hat. In den anderen Kontexten ist dieser Einfluss gering oder moderat.

Die Ergebnisse des Pfades „Einstellung auf Verhalten" zeigen, dass die Effektstärke im Kontext „Umgang mit (mobilen) Speicher- und Endgeräten" am größten ist, hier ist die Effektstärke der Variable „Einstellung" signifikant. In den restlichen Kontexten („E-Mail-Bearbeitung", „Umgang mit Informationen u. a. im Kontext mobiler Arbeit" und „Passwortmanagement") hat die Effektstärke einen geringen Wert, was bedeutet, dass der Einfluss der Variable „Einstellung" in diesen Kontexten gering ist. Im Kontext „Zutritts- und Zugriffsschutz" ist der Einfluss der Variable „Wissen" auf die Variable „Einstellung" wiederum moderat.

Der Pfad „Wissen auf Verhalten" zeigt eine große Effektstärke in den Kontexten „E-Mail-Bearbeitung" und „Zutritts- und Zugriffsschutz", da der Wert, der die Effekt-

stärke nachweist, hier größer als 0,35 ist (vgl. Nitzl, 2010 in Anlehnung an Cohen, 1988; Chin, 1998b). Folglich ist der Einfluss der exogenen Variable „Wissen" auf die endogene Variable „Verhalten" in diesen Kontexten groß. In den Kontexten „Umgang mit Informationen u. a. im Kontext mobiler Arbeit" und „Umgang mit (mobilen) Speicher- und Endgeräten" weist die Effektstärke jeweils einen geringen Wert auf, entsprechend gering ist also auch der Einfluss der exogenen Variable „Wissen" auf die endogene Variable „Verhalten". Im Kontext „Passwortmanagement" ist dieser Einfluss moderat.

Tabelle 31: Ergebnisse der Effektstärke (f^2) in den Strukturmodellen für den Erhebungszeitpunkt T2

	E-Mail-Bearbeitung	Passwort-management	Umgang mit Informationen u. a. im Kontext mobiler Arbeit	Umgang mit (mobilen) Speicher- und Endgeräten	Zutritts- und Zugriffsschutz
Wissen → Einstellung	0,137	0,016	0,174	1,356	0,039
Einstellung → Verhalten	0,028	0,084	0,021	0,548	0,233
Wissen → Verhalten	0,541	0,202	0,109	0,097	0,664

Das letzte Prüfkriterium für die Strukturmodellbewertung ist die Prognoserelevanz eines Strukturmodells. Die Ergebnisse der Prognoserelevanzprüfung sind in Tabelle 32 aufgeführt.

Tabelle 32: Ergebnisse der Prognoserelevanz der Strukturmodelle für den Erhebungszeitpunkt T2

	E-Mail-Bearbeitung	Passwort-management	Umgang mit Informationen u. a. im Kontext mobiler Arbeit	Umgang mit (mobilen) Speicher- und Endgeräten	Zutritts- und Zugriffsschutz
Q^2 Einstellung	–0,002	–0,259	–0,119	0,519	–0,046
Q^2 Verhalten	0,366	–0,329	–0,285	–0,052	0,314

Wie die Ergebnisse zeigen, ist die Prognoserelevanz nur im Konstrukt „Einstellung" im Kontext „Umgang mit (mobilen) Speicher- und Endgeräten" positiv, was impliziert, dass das Modell nur in diesem Kontext eine große Vorhersageleistung hat, während in den anderen Kontexten dieses Konstruktes die restlichen Modelle eine niedrige Vorhersageleistung haben. Im Konstrukt „Verhalten" hat die Prognoserelevanz der Modelle der Kontexte „E-Mail-Bearbeitung" und „Zutritts- und Zugriffsschutz" einen positiven Wert, was besagt, dass die Vorhersageleistung der Modelle groß ist. Die Modelle der Kontexte „Passwortmanagement", „Umgang mit Informationen u. a. im Kontext mobiler Arbeit" und „Umgang mit (mobilen) Speicher- und Endgeräten" im Konstrukt „Verhalten" weisen einen negativen Q^2-Wert auf. Dies impliziert, dass der

Vorhersagefehler der Schätzung mittels PLS größer ist als der Vorhersagefehler bei der einfachen Verwendung der Mittelwerteschätzung.

Nachdem die Bewertung der Mess- und Strukturmodelle erfolgt ist, kann die Gesamtbeurteilung des Modells stattfinden. Generell sind die Ergebnisse der Mess- und Strukturmodelle valide und erfüllen die Anforderungen der Gütekriterien. Die Interpretation der Ergebnisse findet zu einem späteren Zeitpunkt statt, nachdem die Ergebnisse der Mess- und Strukturmodelle für die restlichen Erhebungszeitpunkte präsentiert wurden.

4.5.5 Beurteilung der Ergebnisse der vierten Erhebung T3

4.5.5.1 T3-Ergebnisse der Messmodelle

Die Faktorladungen der Indikatoren zum Erhebungszeitpunkt T3 zeigen generell einen Wert über dem Mindestwert 0,4. Jedoch wurden einige Indikatoren aus dem Messmodell eliminiert, da sie einen Wert unter 0,4 und somit zu geringe Ladungen aufweisen, die eine gute Datenqualität für die weitere Analyse nicht gewährleisten können. Außerdem wurden die Indikatoren entfernt, die einen Wert über 0,4 aufweisen, jedoch dazu führen, dass die Messmodelle nicht alle Gütekriterien erfüllen. In der Tabelle 33 sind die Indikatoren dargestellt, die in den Messmodellen benutzt wurden.

Tabelle 33: Faktorladungen der genutzten Items aus Erhebungszeitpunkt T3

Kontext	Indikator	Ladung
E-Mail-Bearbeitung	EMW02	0,859
	EMW03	0,558
	EMW04	0,761
	EME01	0,773
	EME02	0,931
	EMV02	0,878
	EMV04	0,916
Passwortmanagement	PWW02	0,997
	PWW04	0,408
	PWE01	0,783
	PWE02	0,424
	PWE03	0,693
	PWV02	0,911
	PWV04	0,937

(Fortsetzung Tabelle 33)

Kontext	Indikator	Ladung
Umgang mit Informationen u. a. im Kontext mobiler Arbeit	SEW03	0,930
	SEW04	0,659
	SEE02	0,612
	SEE03	0,953
	SEV01	0,985
	SEV02	0,693
Umgang mit (mobilen) Speicher- und Endgeräten	BEW01	0,722
	BEW02	0,896
	BEW03	0,544
	BEE01	0,858
	BEE02	0,529
	BEE03	0,904
	BEV01	0,690
	BEV02	0,938
Zutritts- und Zugriffsschutz	MVW02	0,862
	MVW04	0,717
	MVE01	0,824
	MVE02	0,883
	MVV02	0,862
	MVV03	0,859
	MVV04	0,669

Parallel können aus dem statistischen Programm SmartPLS 4 die DEV und die KR der Messmodelle entnommen werden (vgl. Ringle, Wende & Becker, 2022). Die Ergebnisse werden in Tabelle 34 aufgelistet. Nach der Elimination der oben genannten Indikatoren stellte sich heraus, dass alle Messmodelle einen ausreichend hohen DEV-Wert (über 0,5) besitzen. Daher wird davon ausgegangen, dass mindestens die Hälfte der Varianz eines Konstrukts durch die ihm zugeordneten Indikatoren erklärt wird. Auch die KR-Werte erfüllen die Mindestanforderungen des Gütekriteriums und zeigen einen Wert über 0,6, was impliziert, dass alle Indikatoren, die einem Konstrukt zugeordnet sind, eine starke Korrelation zwischeneinander haben. Obwohl die DEV des Konstrukts „Einstellung“ im Kontext „Passwortmanagement“ leicht gesenkt ist, entspricht die KR des Konstruktes den Anforderungen des Kriteriums. Auch die andere

Kriterien des Konstruktes sind erfüllt, daher soll das Konstrukt dennoch in die weitere Auswertung einbezogen werden.

Tabelle 34: DEV und KR der Messmodelle aus dem Erhebungszeitpunkt T3

Kontext	Konstrukt	DEV	KR
E-Mail-Bearbeitung	Wissen	0,543	0,776
	Einstellung	0,732	0,844
	Verhalten	0,805	0,892
Passwortmanagement	Wissen	0,580	0,701
	Einstellung	0,425	0,677
	Verhalten	0,854	0,921
Umgang mit Informationen u. a. im Kontext mobiler Arbeit	Wissen	0,650	0,783
	Einstellung	0,642	0,774
	Verhalten	0,725	0,836
Umgang mit (mobilen) Speicher- und Endgeräten	Wissen	0,540	0,772
	Einstellung	0,611	0,818
	Verhalten	0,678	0,805
Zutritts- und Zugriffsschutz	Wissen	0,629	0,771
	Einstellung	0,729	0,843
	Verhalten	0,643	0,842

Im nächsten Schritt muss die Diskriminanzvalidität der Konstrukte in allen Kontexten berechnet werden. Dies wurde anhand der Berechnung der HTMT-Ratio erfüllt. Diese soll, wie bereits erwähnt, einen Wert ≤ 0,945 nachweisen, um eine Diskriminanzvalidität zu gewährleisten. Die Ergebnisse der Berechnung der Diskriminanzvalidität für den Erhebungszeitpunkt T3 können Tabelle 35 entnommen werden. Wie die Ergebnisse veranschaulichen, können alle Konstrukte des Messmodells in allen erwähnten Kontexten eine Diskriminanzvalidität nachweisen, da die HTMT-Ratio unter 0,945 liegt – bis auf den Kontext „E-Mail-Bearbeitung“ im Konstrukt „Wissen ↔ Verhalten“ und den Kontext „Passwortmanagement“ im Konstrukt „Einstellung ↔ Verhalten“. Im Kontext „Zutritt- und Zugriffsschutz“ liegt der Wert auch um 0,003 über den HTMT-Ratio. Da die Diskriminanzvalidität hier jedoch nur leicht erhöht ist und alle anderen Kriterien erfüllt sind, wurde entschieden, die Konstrukte weiter in die Strukturmodellanalyse einzubeziehen.

Tabelle 35: HTMT-Ratio für die Messmodelle aus dem Erhebungszeitpunkt T3

	E-Mail-Bearbeitung	Passwort-management	Umgang mit Informationen u. a. im Kontext mobiler Arbeit	Umgang mit (mobilen) Speicher- und Endgeräten	Zutritts- und Zugriffsschutz
Wissen ↔ Einstellung	0,238	0,630	0,778	0,771	0,937
Wissen ↔ Verhalten	0,978	0,428	0,430	0,363	0,897
Einstellung ↔ Verhalten	0,420	0,996	0,575	0,665	0,948

Folglich ist belegt, dass die Messmodelle Reliabilität und Validität aufweisen und für die weitere Analyse auf dem Niveau des Strukturmodells geeignet sind.

4.5.5.2 T3-Ergebnisse der Strukturmodelle

Zuerst soll das Bestimmtheitsmaß (R^2) eines Strukturmodells berechnet werden (siehe Kapitel 4.5.1.3). Die Ergebnisse der Berechnung des Bestimmtheitsmaßes (R^2) für die Strukturmodelle aus dem Erhebungszeitpunkt T3 sind in Tabelle 36 dargestellt.

Das Bestimmtheitsmaß (R^2) für „Einstellung" ist in dem Kontext „Passwort-management" moderat. Dies impliziert, dass die Varianz der latenten endogenen Variable (Einstellung) über die ihr zugeordnete exogene Variable (Wissen) in diesem Fall mäßig erklärt wird. In anderen Kontexten ist der Bestimmtheitsmaßwert gering. Daher wird die Variable „Einstellung" über die Variable „Wissen" prozentual schwach erklärt.

Das Bestimmtheitsmaß (R^2) für „Verhalten" für Kontexte „E-Mail-Bearbeitung" und „Zutritts- und Zugriffsschutz" weist einen moderaten Wert auf. Für andere Kontexte ist der Bestimmtheitsmaßwert schwach. Dies impliziert, dass die Variable „Verhalten" über die Variable „Wissen" prozentual moderat bis schwach erklärt wird.

Tabelle 36: Übersicht über das Bestimmtheitsmaß R^2 für T3

	E-Mail-Bearbeitung	Passwort-management	Umgang mit Informationen u. a. im Kontext mobiler Arbeit	Umgang mit (mobilen) Speicher- und Endgeräten	Zutritts- und Zugriffsschutz
Einstellung R^2	0,002	0,503	0,152	0,308	0,242
Verhalten R^2	0,516	0,171	0,300	0,207	0,493

Im nächsten Schritt soll die Pfadkoeffizientenanalyse evaluiert werden (siehe Tabelle 37).

Die Pfadkoeffizienten des Pfades „Wissen auf Einstellung" sind bedeutsam, bis auf den Kontext „E-Mail-Bearbeitung", wo der Pfadkoeffizient einen geringeren Wert

hat, entsprechend korrelieren hier die Variablen „Wissen“ und „Einstellung“ stark miteinander, bis auf den Kontext „E-Mail-Bearbeitung“, wo diese Korrelation gering ist.

Bei den Pfadkoeffizienten des Pfades „Einstellung auf Verhalten“ ist die Korrelation zwischen der Variable „Einstellung“ und der Variable „Verhalten“ signifikant, da die Werte der Pfadkoeffizienten größer als 0,2 sind.

Die Pfadkoeffizienten des Pfades „Wissen auf Verhalten“ sind in allen Kontexten stark, bis auf den Kontext „Umgang mit (mobilen) Speicher- und Endgeräten“, wo die Variablen eine geringere Korrelation haben.

Tabelle 37: Ergebnisse der Pfadkoeffizienten in den Strukturmodellen für T3

Pfad	E-Mail- Bear-bei-tung	Passwort-management	Umgang mit Informationen u. a. im Kontext mobiler Arbeit	Umgang mit (mobilen) Speicher- und Endgeräten	Zutritts- und Zugriffsschutz
Wissen → Einstellung	0,040	–0,222	0,390	0,555	0,492
Einstellung → Verhalten	0,287	0,771	0,372	0,423	0,533
Wissen → Verhalten	0,648	0,413	0,283	0,052	0,265

Nachdem die Pfadkoeffizientenanalyse erfolgte, soll die Effektstärke (f^2) der Strukturmodelle berechnet werden. Die Ergebnisse können aus Tabelle 38 entnommen werden.

Wie die Ergebnisse zeigen, kann nur im Kontext „Umgang mit (mobilen) Speicher- und Endgeräten“ ein größerer Einfluss von Wissen auf Einstellung beobachtet werden. In den Kontexten „Umgang mit Informationen u. a. im Kontext mobiler Arbeit“ und „Zutritts- und Zugriffsschutz“ ist dieser Einfluss mittelmäßig und in den Kontexten „E-Mail-Bearbeitung“ und „Passwortmanagement“ gering.

Tabelle 38: Ergebnisse der Effektstärke (f^2) in den Strukturmodellen für Erhebungszeitpunkt T3

	E-Mail-Bearbeitung	Passwort-management	Umgang mit Informationen u. a. im Kontext mobiler Arbeit	Umgang mit (mobilen) Speicher- und Endgeräten	Zutritts- und Zugriffsschutz
Wissen → Einstellung	0,002	0,089	0,179	0,444	0,320
Einstellung → Verhalten	0,170	0,993	0,167	0,156	0,425
Wissen → Verhalten	0,868	0,206	0,097	0,002	0,105

In den Kontexten „E-Mail-Bearbeitung“, „Umgang mit (mobilen) Speicher- und Endgeräten“ und „Umgang mit Informationen u. a. im Kontext mobiler Arbeit“ ist der Einfluss von Einstellung auf Verhalten moderat, in den Kontexten „Passwortmanagement“ und „Zutritts- und Zugriffsschutz“ wiederum zeigt sich ein großer Einfluss.

Die Effektstärke im Kontext „E-Mail-Bearbeitung“ auf dem Pfad „Wissen auf Verhalten“ ist bedeutsam, folglich kann davon ausgegangen werden, dass der Einfluss von Wissen auf Verhalten hier auch entsprechend groß ist. Im Kontext „Passwortmanagement“ fällt der Einfluss von Wissen auf Verhalten moderat aus. Die niedrigen f^2-Werte aller anderen Kontexte auf diesem Pfad führen zu der Schlussfolgerung, dass der Einfluss von Wissen auf Verhalten ansonsten eher gering ist.

Die Prognoserelevanz ist das letzte Kriterium, das die Strukturmodelle erfüllen sollen. Sie kann sowohl positiv als auch negativ sein. Die Ergebnisse der Prognoserelevanz für den Erhebungszeitpunkt T3 sind in Tabelle 39 dargestellt. Eine positive Prognoserelevanz, wie in den Kontexten „Umgang mit (mobilen) Speicher- und Endgeräten“ und „Zutritts- und Zugriffsschutz“ im Konstrukt „Einstellung“ weist nach, dass die Strukturmodelle der Kontexte empirische Daten gut rekonstruieren können (vgl. Nitzl, 2010 in Anlehnung an Fornell & Cha, 1994). Eine negative Prognoserelevanz des Modells (wie in den Kontexten „E-Mail-Bearbeitung“, „Passwortmanagement“ und „Umgang mit Informationen u. a. im Kontext mobiler Arbeit“ im Konstrukt „Einstellung“) gibt Informationen darüber, dass die Modelle die empirischen Daten nicht besser rekonstruieren können als z. B. eine Mittelwertanalyse (nach Nitzl, 2010 in Anlehnung an Krafft, Götz & Liehr-Gobbers, 2005). Die Prognoserelevanz des Konstruktes „Verhalten“ ist in allen Kontexten positiv bis auf die Kontexte „Passwortmanagement“, „Umgang mit Informationen u. a. im Kontext mobiler Arbeit“ und „Umgang mit (mobilen) Speicher- und Endgeräten“ (im Konstrukt „Verhalten“). Dies bedeutet, dass die Modelle aller Kontexte bis auf „Passwortmanagement“, „Umgang mit Informationen u. a. im Kontext mobiler Arbeit“ und „Umgang mit (mobilen) Speicher- und Endgeräten“ (Konstrukt „Verhalten“) die Rohdaten gut rekonstruieren können.

Tabelle 39: Ergebnisse der Prognoserelevanz der Strukturmodelle für den Erhebungszeitpunkt T3

	E-Mail-Bearbeitung	Passwort-management	Umgang mit Informationen u. a. im Kontext mobiler Arbeit	Umgang mit (mobilen) Speicher- und Endgeräten	Zutritts- und Zugriffsschutz
Q^2 Einstellung	–0,060	–0,195	–0,133	0,142	0,173
Q^2 Verhalten	0,338	–0,235	–0,143	–0,061	0,220

Abschließend kann die Schlussfolgerung gezogen werden, dass sowohl die Mess- als auch die Strukturmodelle alle Gütekriterien erfüllen und somit zuverlässig und valide sind. Dementsprechend können die Ergebnisse der Erhebung T3 in die finale Interpretation der Ergebnisse einbezogen werden. Dies erfolgt in weiteren Kapiteln. Zuerst sollen die Ergebnisse der restlichen Erhebung analysiert und auf Gültigkeit und Zuverlässigkeit mittels Anforderungen der Gütekriterien überprüft werden.

4.5.6 Beurteilung der Ergebnisse der fünften Erhebung T4

4.5.6.1 T4-Ergebnisse der Messmodelle

Die Faktorladungen der Indikatoren des Erhebungszeitpunktes T4 weisen generell eine hohe Ladung über 0,4 auf, allerdings mussten einige Indikatoren aus den Messmodellen eliminiert werden, um eine hohe Datenqualität für die weitere Analyse der Messmodelle gewährleisten zu können. Die Ergebnisse der Faktorladung können Tabelle 40 entnommen werden. Generell kann die Schlussfolgerung gezogen werden, dass die Indikatorenreliabilität der gebliebenen Indikatoren gewährleistet ist.

Tabelle 40: Faktorladungen der genutzten Items aus Erhebungszeitpunkt T4

Kontext	Faktor	Ladung
E-Mail-Bearbeitung	EMW02	0,918
	EMW03	0,900
	EME01	0,834
	EME02	0,858
	EMV02	0,811
	EMV04	0,934
Passwortmanagement	PWW02	0,909
	PWW04	0,933
	PWE01	0,952
	PWE02	0,760
	PWE03	0,792
	PWV03	0,919
	PWV05	0,320
Umgang mit Informationen u. a. im Kontext mobiler Arbeit	SEW03	0,656
	SEW04	0,970
	SEE01	0,841
	SEE03	0,835
	SEV02	0,855
	SEV03	0,857
	SEV04	0,794

(Fortsetzung Tabelle 40)

Kontext	Faktor	Ladung
Umgang mit (mobilen) Speicher- und Endgeräten	BEW02	0,791
	BEW03	0,886
	BEE02	0,961
	BEE03	0,964
	BEV02	0,938
	BEV03	0,944
Zutritts- und Zugriffsschutz	MVW03	0,767
	MVW02	0,870
	MVE01	0,926
	MVE03	0,944
	MVV01	0,866
	MVV02	0,979

Nachdem die Indikatoren aus den Messmodellen eliminiert wurden, können die DEV und die KR der Messmodelle aus dem statistischen Programm SmartPLS 4 (Version 4.0.9.4. nach Ringle, Wende & Becker, 2022) entnommen werden. Die Ergebnisse sind in Tabelle 41 präsentiert. Wie die Ergebnisse zeigen, ist die DEV in jedem Konstrukt in allen fünf Kontexten größer als 0,5. Auch die KR ist in jedem Konstrukt in allen fünf Kontexten größer als 0,6. Somit kann davon ausgegangen werden, dass die Erfüllung der Mindestanforderungen der beiden Gütekriterien gewährleistet ist.

Tabelle 41: DEV und KR der Messmodelle aus dem Erhebungszeitpunkt T4

Kontext	Konstrukt	DEV	KR
E-Mail-Bearbeitung	Wissen	0,827	0,905
	Einstellung	0,715	0,834
	Verhalten	0,774	0,872
Passwortmanagement	Wissen	0,848	0,918
	Einstellung	0,703	0,876
	Verhalten	0,474	0,594
Umgang mit Informationen u. a. im Kontext mobiler Arbeit	Wissen	0,686	0,808
	Einstellung	0,702	0,825
	Verhalten	0,699	0,874

(Fortsetzung Tabelle 41)

Kontext	Konstrukt	DEV	KR
Umgang mit (mobilen) Speicher- und Endgeräten	Wissen	0,706	0,827
	Einstellung	0,927	0,962
	Verhalten	0,886	0,940
Zutritts- und Zugriffsschutz	Wissen	0,673	0,804
	Einstellung	0,874	0,933
	Verhalten	0,872	0,931

Im nächsten Schritt soll die Diskriminanzvalidität berechnet werden, um die Validität der Messmodelle zu überprüfen (siehe Kapitel 4.5.1.3).

Generell weisen alle Konstrukte bis auf den Pfad „Wissen ↔ Einstellung“ in den Kontexten „E-Mail-Bearbeitung“, „Passwortmanagement“ und „Umgang mit (mobilen) Speicher- und Endgeräten“ einen niedrigeren Wert als 0,945 auf (siehe Tabelle 42).

Somit lässt sich schlussfolgern, dass bis auf die genannte Ausnahmen Diskriminanzvalidität zwischen den reflektiven Konstrukten in den Messmodellen gewährleistet ist. Da die restlichen Gütekriterien dieser Kontexte jedoch erfüllt sind, sollen die Strukturmodelle dieser Kontexte dennoch in die allgemeine Beurteilung einbezogen werden.

Tabelle 42: HTMT-Ratio für die Messmodelle aus dem Erhebungszeitpunkt T4

	E-Mail-Bearbeitung	Passwort-management	Umgang mit Informationen u. a. im Kontext mobiler Arbeit	Umgang mit (mobilen) Speicher- und Endgeräten	Zutritts- und Zugriffsschutz
Wissen ↔ Einstellung	1,163	1,052	0,750	0,965	0,870
Wissen ↔ Verhalten	0,649	0,636	0,854	0,701	0,359
Einstellung ↔ Verhalten	0,757	0,917	0,787	0,922	0,129

Im nächsten Kapitel erfolgt die Beurteilung der Strukturmodelle.

4.5.6.2 T4-Ergebnisse der Strukturmodelle

Zuerst soll das Bestimmtheitsmaß der endogenen Konstrukte geprüft werden. Wie die Ergebnisse der Überprüfung zeigen, ist das Bestimmtheitsmaß des endogenen Konstrukts „Einstellung“ im Konstrukt „Passwortmanagement“ am höchsten. In den Kontexten „E-Mail-Bearbeitung“, „Umgang mit (mobilen) Speicher- und Endgeräten“ und „Zutritts- und Zugriffsschutz“ ist der Bestimmtheitsmaßwert moderat und im Kontext

„Umgang mit Informationen u. a. im Kontext mobiler Arbeit“ eher niedrig, was impliziert, dass die Variable „Einstellung“ durch die Variable „Wissen“ prozentual schwach bis moderat in den entsprechenden Kontexten erklärt werden kann.

Die Ergebnisse der Bestimmtheitsmaßeüberprüfung für die endogene Variable „Verhalten“ veranschaulichen, dass der Bestimmtheitsmaßwert für den Kontext „Umgang mit (mobilen) Speicher- und Endgeräten“ groß ist. Folglich kann die Variable „Verhalten“ entsprechend gut über die Variable „Wissen“ erklärt werden. Der Kontext „Umgang mit Informationen u. a. im Kontext mobiler Arbeit“ weist einen moderaten Wert auf, in den Kontexten „E-Mail-Bearbeitung“, „Passwortmanagement“ und „Zutritts- und Zugriffsschutz“ fallen die Werte eher niedrig aus. Schlussfolgernd kann davon ausgegangen werden, dass die Variable „Verhalten“ hier moderat bis gering über die Variable „Wissen“ erklärt werden kann.

Tabelle 43: Übersicht über das Bestimmtheitsmaß R^2 für T4

	E-Mail-Bearbeitung	Passwort-management	Umgang mit Informationen u. a. im Kontext mobiler Arbeit	Umgang mit (mobilen) Speicher- und Endgeräten	Zutritts- und Zugriffsschutz
Einstellung R^2	0,639	0,738	0,253	0,516	0,360
Verhalten R^2	0,317	0,119	0,487	0,696	0,080

Im nächsten Schritt muss die Pfadkoeffizientenanalyse durchgeführt werden. Die Ergebnisse können Tabelle 44 entnommen werden. Die Pfadkoeffizienten des Pfades „Wissen auf Einstellung“ sind in allen Kontexten bedeutsam, was impliziert, dass die Variable „Wissen“ stark mit der Variable „Einstellung“ korreliert.

Die Pfadkoeffizienten des Pfades „Einstellung auf Verhalten“ sind in allen Kontexten auch stark, was bedeutet, dass die Variable „Einstellung“ stark mit der Variable „Verhalten“ korreliert.

Auf dem Pfad „Wissen auf Verhalten“ weisen die Pfadkoeffizienten in den meisten Kontexten einen starken Wert auf. Eine Ausnahme stellen die Kontexte „Passwortmanagement“ und „Umgang mit (mobilen) Speicher- und Endgeräten“ dar, wo die Werte niedrig ausfallen. Folglich korrelieren die Variable „Wissen“ und die Variable „Verhalten“ entsprechend stark in allen Kontexten außer Kontexte „Passwortmanagement“ und „Umgang mit (mobilen) Speicher- und Endgeräten“ miteinander.

Tabelle 44: Ergebnisse der Pfadkoeffizienten in den Strukturmodellen für T4

Pfad	E-Mail-Bearbeitung	Passwort-management	Umgang mit Informationen u. a. im Kontext mobiler Arbeit	Umgang mit (mobilen) Speicher- und Endgeräten	Zutritts- und Zugriffsschutz
Wissen → Einstellung	0,800	0,859	0,503	0,718	0,600

(Fortsetzung Tabelle 44)

Pfad	E-Mail-Bearbeitung	Passwort-management	Umgang mit Informationen u. a. im Kontext mobiler Arbeit	Umgang mit (mobilen) Speicher- und Endgeräten	Zutritts- und Zugriffsschutz
Einstellung → Verhalten	0,291	–0,463	0,265	0,942	–0,213
Wissen → Verhalten	0,303	0,147	0,526	–0,161	0,353

Im Folgenden werden die Ergebnisse für die Effektstärke (f^2) dargestellt (siehe Tabelle 45). Die Effektstärke des Pfades „Wissen auf Einstellung" ist in allen Kontexten bedeutsam, bis auf den Kontext „Umgang mit Informationen u. a. im Kontext mobiler Arbeit". Dies impliziert, dass die exogene Variable „Wissen" einen großen Einfluss auf die endogene Variable „Einstellung" hat, im Kontext „Umgang mit Informationen u. a. im Kontext mobiler Arbeit" fällt dieser jedoch nur moderat aus. Im Kontext „Passwortmanagement" sticht ein besonders hoher f^2-Wert heraus, folglich beeinflusst die Variable „Wissen" in diesem Kontext die Variable „Einstellung" am meisten.

Die Effektstärke des Pfades „Einstellung auf Verhalten" ist nur im Kontext „Umgang mit (mobilen) Speicher- und Endgeräten" sehr groß, in den restlichen Kontexten hingegen gering. Dies bedeutet, dass der Einfluss der Variable „Einstellung" auf die Variable „Verhalten" nur im Kontext „Umgang mit (mobilen) Speicher- und Endgeräten" signifikant ist.

Auf dem Pfad „Wissen auf Verhalten" ist die Effektstärke im Kontext „Umgang mit Informationen u. a. im Kontext mobiler Arbeit" signifikant. In den restlichen Kontexten ist die Effektstärke gering. Das heißt, dass die Variable „Wissen" nur im Kontext „Umgang mit Informationen u. a. im Kontext mobiler Arbeit" bedeutsam auf die Variable „Verhalten" einwirkt.

Tabelle 45: Ergebnisse der Effektstärke (f^2) in den Strukturmodellen für den Erhebungszeitpunkt T4

	E-Mail-Bearbeitung	Passwort-management	Umgang mit Informationen u. a. im Kontext mobiler Arbeit	Umgang mit (mobilen) Speicher- und Endgeräten	Zutritts- und Zugriffsschutz
Wissen → Einstellung	1,773	2,811	0,339	1,067	0,563
Einstellung → Verhalten	0,045	0,064	0,102	1,412	0,032
Wissen → Verhalten	0,048	0,006	0,402	0,031	0,087

Das letzte Gütekriterium, was die Strukturmodelle erfüllen müssen, ist die Prognoserelevanz (siehe Tabelle 46). Die Prognoserelevanz des Konstruktes „Einstellung" ist in

allen Kontexten positiv, was impliziert, dass das Strukturmodell gut die empirischen Daten rekonstruieren kann (siehe Kapitel 4.5.1.4).

Die Prognoserelevanz des Konstruktes „Verhalten“ ist fast auch in allen Kontexten positiv, bis auf die Kontexte „Passwortmanagement“ und „Zutritts- und Zugriffsschutz“. In diesen Fällen kann das Konstrukt „Verhalten“ des Messmodells die Daten nicht ausreichend rekonstruieren.

Tabelle 46: Ergebnisse der Prognoserelevanz der Strukturmodelle für den Erhebungszeitpunkt T4

	E-Mail-Bearbeitung	Passwort-management	Umgang mit Informationen u. a. im Kontext mobiler Arbeit	Umgang mit (mobilen) Speicher- und Endgeräten	Zutritts- und Zugriffsschutz
Q^2 Einstellung	0,627	0,736	0,137	0,486	0,298
Q^2 Verhalten	0,271	–0,059	0,384	0,220	–0,139

Somit kann die Schlussfolgerung gezogen werden, dass alle Konstrukte in allen Kontexten, bis auf den Konstruktpfad „Wissen ↔ Einstellung“ in den Kontexten „E-Mail-Bearbeitung“, „Passwortmanagement“ und „Umgang mit (mobilen) Speicher- und Endgeräten“ (HTMT-Ratio), alle Gütekriterien erfüllen. Dadurch, dass die Konstruktpfade aber die restlichen Anforderungen sowohl in den Mess- als auch in den Strukturmodellen erfüllen, wurde entschieden, die Konstrukte nicht zu eliminieren, sondern in die Gesamtbeurteilung zu inkludieren.

4.5.7 Mittelwertanalyse

Um herauszufinden, wie effektiv und nachhaltig das Konzept der Security Arena zusätzlich zur klassischen Unterweisung für die Förderung von Awareness-Aspekten (Wissen, Einstellung und Verhalten) ist, soll eine Mittelwertanalyse durchgeführt werden. So werden die Ergebnisse entlang der Erhebungszeitpunkte analysiert, um die Veränderungen im arithmetischen Mittel (auch Mittelwert) hinsichtlich des Wissens der Probanden bezüglich der abgefragten Kontexte zu analysieren und die Veränderung hinsichtlich der positiven oder negativen Einstellung und des informationssicherheitskonformen Verhaltens im Zeitverlauf zu beobachten. Um die Nachhaltigkeit der Sicherheits-Awareness-Maßnahmen Unterweisung sowie Unterweisung mit zusätzlich durchgeführter Security Arena zu messen, werden die entsprechenden Mittelwerte berechnet.

Um Mittelwerte zu berechnen, müssen alle Messwerte aufaddiert werden, woraufhin das Ergebnis durch die Anzahl der Messwerte geteilt wird (vgl. Benning, 2020). Die Formel des arithmetischen Mittels sieht wie folgt aus (vgl. Benning, 2020):

$$\bar{x} = \frac{1}{n} \sum_{i=1}^{n} x_i = \frac{X_1 + X_2 + X_n}{n}$$

Die Mittelwerte für alle Kontexte in Bezug zu Wissen, Einstellung und Verhalten wurden für alle Erhebungszeitpunkte mittels Microsoft Excel für Gruppe A und für Gruppe B separat berechnet.

Die Ergebnisse der Mittelwertanalyse sind in Tabelle 47 dargestellt. Die Tabelle zeigt den Mittelwert der Antworten hinsichtlich Wissen, Einstellung und Verhalten für die jeweils betrachteten Kontexte sowie ihre Ausprägung zu den jeweiligen Erhebungszeitpunkten. Dabei stellt der Wert 1 den niedrigsten und der Wert 5 den höchstmöglichen Wert gemäß der im Rahmen der quantitativen Studie verwendeten 5er-Likert-Skala dar (siehe Kapitel 4.4.1).

Die Berechnungen werden im Folgenden separat jeweils für Gruppe A und Gruppe B dargestellt. In Tabelle 47 sind die Ergebnisse der Mittelwertanalyse für die Gruppe A, die mit einer Unterweisung und der Security Arena sensibilisiert wurde, ersichtlich.

Tabelle 47: Ergebnisse der Mittelwertanalyse für die Gruppe A vom Erhebungszeitpunkt T0 bis zum Erhebungszeitpunkt T4

Kontext	Konstrukt	$\bar{x}$ in T0	$\bar{x}$ in T1	$\bar{x}$ in T2	$\bar{x}$ in T3	$\bar{x}$ in T4
E-Mail-Bearbeitung	Wissen	3,69	4,41	4,03	4,26	4,35
	Einstellung	3,81	4,02	3,86	4,17	4,02
	Verhalten	3,45	4,31	3,96	4,18	3,88
Passwortmanagement	Wissen	3,87	4,71	3,87	4,09	4,04
	Einstellung	3,65	4,38	4,66	4,63	4,08
	Verhalten	3,57	4,32	3,82	3,84	3,71
Umgang mit Informationen u. a. im Kontext mobiler Arbeit	Wissen	4,28	4,38	4,61	4,63	4,03
	Einstellung	3,67	4,23	4,56	4,52	4,16
	Verhalten	3,34	3,72	4,16	4,66	4,43
Umgang mit (mobilen) Speicher- und Endgeräten	Wissen	3,81	4,26	4,47	4,62	4,27
	Einstellung	4,02	4,61	4,63	4,72	4,36
	Verhalten	3,94	4,54	4,55	4,70	4,25
Zutritts- und Zugriffsschutz	Wissen	3,75	4,21	4,15	4,25	4,1
	Einstellung	4,21	4,41	4,40	4,50	4,08
	Verhalten	3,83	4,42	4,21	4,37	4,30

Nachdem die Mittelwertanalyse durchgeführt wurde, ist es sinnvoll, zu evaluieren, inwiefern sich die Einzelwerte zu den bestimmten Erhebungszeitpunkten verändert haben. Generell kann festgestellt werden, dass die Gruppe A schon eine relativ hohe Grundsensibilisierung und eine gewisse Affinität zu dem Thema „Informationssicher-

heit“ mitbringt (obwohl die erste offizielle Sensibilisierung zum Thema Informationssicherheit direkt nach dem Erhebungszeitpunkt T0 im Rahmen dieser Studie durchgeführt wurde), denn die Werte der Mittelwertanalyse im Erhebungszeitpunkt T0 sind für alle Kontexte nicht niedriger als 3,3 von möglichen 5.

Wie die Ergebnisse belegen, kann generell ein Zuwachs des Mittelwertes nach der Durchführung der Unterweisung festgestellt werden. Am signifikantesten ist dieser Zuwachs im Kontext „E-Mail-Bearbeitung“ (in den Konstrukten „Wissen“ und „Verhalten“), im Kontext „Passwortmanagement“ (in den Konstrukten „Wissen“, „Einstellung“ und „Verhalten“), im Kontext „Umgang mit Informationen u. a. im Kontext mobiler Arbeit“ (in den Konstrukten „Einstellung“ und „Verhalten“), im Kontext „Umgang mit (mobilen) Speicher- und Endgeräten“ (in den Konstrukten „Wissen“, „Einstellung“ und „Verhalten“) und im Kontext „Zutritts- und Zugriffsschutz“ (in den Konstrukten „Wissen“ und „Verhalten“). Im Kontext „Umgang mit Informationen u. a. im Kontext mobiler Arbeit“ im Konstrukt „Wissen“ und im Kontext „Zutritts- und Zugriffsschutz“ im Konstrukt „Einstellung“ ist der Zuwachs des Mittelwerte zwar vorhanden, jedoch nicht signifikant. Was zu dem Schluss führt, dass die Unterweisung generell eine relativ effektive Methode der Sensibilisierung für kurzfristige Effekte in fast allen Bereichen und in allen Konstrukten ist.

Die Befragung T2 wurde mit der Gruppe A einige Wochen nach dem Erhebungszeitpunkt T1 durchgeführt. Wie die Ergebnisse der Befragung T2 zeigen, ergab sich nur in wenigen Kontexten eine leichte Steigerung der Mittelwerte vom T1-Befragungszeitpunkt bis zum T2-Befragungszeitpunkt, z. B. in den Kontexten „Umgang mit Informationen u. a. im Kontext mobiler Arbeit“ (Konstrukte „Wissen“, „Einstellung“ und „Verhalten“), Passwortmanagement („Konstrukt „Einstellung“) und „Umgang mit (mobilen) Speicher- und Endgeräten (Konstrukte „Wissen“, „Einstellung“ und „Verhalten“). Die Gründe dafür könnten u. a. sein, dass die Teilnehmer in den Wochen nach dem Erhebungszeitpunkt T1 z. B. im Berufsalltag neue Impulse zum Thema „Umgang mit Informationen u. a. im Kontext mobiler Arbeit“ im Rahmen ihrer Einarbeitung erhalten haben.

Generell sind die Mittelwerte aus dem Zeitpunkt T2 niedriger als die Ergebnisse der Mittelwerte aus dem Zeitpunkt T1 (außer in den Kontexten „Passwortmanagement“ (im Konstrukt „Einstellung“), „Umgang mit (mobilen) Speicher- und Endgeräten“ (Konstrukte „Wissen“, „Einstellung“ und „Verhalten“) und „Umgang mit Informationen u. a. im Kontext mobiler Arbeit“ (Konstrukte „Wissen“, „Einstellung“ und „Verhalten“), aber dennoch höher als die Mittelwerte aus dem Erhebungszeitpunkt T0. Dies impliziert, dass die Unterweisung kurzfristige Effekte bringt und als eine Lösung für die kurzfristige Sensibilisierung eingesetzt werden kann.

Direkt nach der Erhebung zum Zeitpunkt T2 wurde die Security Arena als eine zusätzliche Sensibilisierungsmaßnahme für die Gruppe A durchgeführt. Nach der Durchführung der Security Arena wurden die Teilnehmer im Anschluss erneut befragt, um die kurzfristigen Effekte der Security Arena zu überprüfen. Wie die Ergebnisse der Befragung T3 zeigen, haben sich die Mittelwerte in fast allen Kontexten und Konstrukten stark verbessert – bis auf die folgende Kontexte, wo die Mittelwerte leicht

gesunken sind: „Passwortmanagement“ im Konstrukt „Einstellung“ und „Umgang mit Informationen u. a. im Kontext mobiler Arbeit“ im Konstrukt „Einstellung“. Dass diese Werte dennoch höher als die Ergebnisse aus dem Erhebungszeitpunkt T0 sind, könnte daran liegen, dass die Teilnehmer den Befragungsbogen, der dieselben Fragen in T0, T1 und T2 beinhaltet, (zu) rasch bearbeiteten und somit den Sinn der Fragen nicht richtig aufnahmen und reflektierten. Dieser Effekt der unerwünschten Verfälschung der Antworten von Teilnehmern wurde auch von Steiner und Bensch (2011, S. 59 in Anlehnung an Mummendey, 2003) beschrieben.

Die Erhebung T4 wurde erst nach einem Monat nach der Durchführung von Erhebung T3 durchgeführt. Wie die Ergebnisse der Mittelwertanalyse zeigen, haben sich die Werte in fast allen Kontexten im Vergleich zum Erhebungszeitpunkt T3 verschlechtert – bis auf den Kontext E-Mail-Bearbeitung (Konstrukt „Wissen“). Dies könnte daran liegen, dass die Teilnehmer im Berufsalltag eine weitere Sensibilisierung zu letzterem Thema erfahren haben. Die Begründung für die leichte Verringerung der Mittelwerteergebnisse aus dem Erhebungszeitpunkt T4 im Vergleich zu den Mittelwerteergebnissen aus dem Erhebungszeitpunkt T3 besteht möglicherweise darin, dass die Unterweisung zusammen mit der Security Arena nur kurzfristige Sensibilisierungseffekte liefert. Allerdings zeigt der Vergleich der Ergebnisse der Mittelwerte von T0 und T4, dass eine Unterweisung zusammen mit einer zusätzlich durchgeführten Security Arena generell eine effektive Sensibilisierungslösung ist. Ausgenommen sind allerdings die Kontexte „Umgang mit Informationen u. a. im Kontext mobiler Arbeit“ (Konstrukt „Wissen“) und „Zutritts- und Zugriffsschutz“ (Konstrukt „Einstellung“). In diesen Kontexten sind die Mittelwerte zum Erhebungszeitpunkt T4 niedriger als die Mittelwerte zum Erhebungszeitpunkt T0.

Im weiteren Verlauf sollen die Ergebnisse der Mittelwertanalyse für Gruppe B, die Gruppe, die nur mit der Unterweisung sensibilisiert wurde, präsentiert und diskutiert werden (siehe Tabelle 48).

Die Gruppe B hat zusammen mit der Gruppe A an der ersten Erhebung zum Zeitpunkt T0 teilgenommen und wurde danach zusammen mit der Gruppe A sensibilisiert. Im Anschluss haben die beiden Gruppen wie bereits beschrieben an der Erhebung T1 teilgenommen. Die Ergebnisse der Mittelwertanalyse für die Zeitpunkte T0 und T1 der Gruppe B sind identisch mit den Mittelwertergebnissen der Zeitpunkte T0 und T1 der Gruppe A. Die mäßige Steigerung der Mittelwerte der T1-Erhebung in allen Kotexten und allen Konstrukten bei Gruppe B bestätigt die Ergebnisse der Gruppe A, dass die Unterweisung eine geeignete Informationssicherheits-Awareness-Methode ist.

Gruppe B wurde nicht mit der Security Arena sensibilisiert, deswegen existieren keine Ergebnisse für die Erhebungen T2 und T3, die vor und nach der Security Arena durchgeführt wurden. Allerdings hat sowohl Gruppe A als auch Gruppe B an der letzten Erhebung T4 teilgenommen, deswegen können die Mittelwerte der T4-Erhebung der Gruppe A zum einen mit den Ergebnissen von der ersten Erhebung T0 und der zweiten Erhebung T1 verglichen werden, um herauszufinden, wie nachhaltig die Unterweisung als eine Sensibilisierungsmaßnahme ist. Zum anderen können die Ergebnisse von Erhebung T4 der Gruppe A mit denen der Gruppe B verglichen werden, um festzu-

stellen, inwiefern sich die Sensibilisierungsmethoden Unterweisung und Unterweisung mit zusätzlicher Security Arena in Bezug auf die Nachhaltigkeit unterscheiden.

Für den Kontext „E-Mail-Bearbeitung“ (in den Konstrukten „Wissen“ und „Einstellung“) zeigen die Ergebnisse, dass sich die Unterweisung als eine relativ nachhaltige Sensibilisierungsmaßnahme eignet, denn obwohl die Mittelwertanalysewerte vom Erhebungszeitpunkt T4 niedriger als die Ergebnisse der Mittelwertanalysewerte T1 sind, sind sie trotzdem höher als die vom Erhebungszeitpunkt T0, was impliziert, dass die Teilnehmenden ein relativ höheres Sensibilisierungsniveau erreicht haben. Dasselbe Phänomen konnte im Kontext „Passwortmanagement“ in den Konstrukten „Wissen“ und „Einstellung“ festgestellt werden, allerdings nicht im Konstrukt „Verhalten“, denn die Mittelwertanalysewerte im Konstrukt „Verhalten“ vom Erhebungszeitpunkt T4 fallen niedriger aus als die Mittelwertanalysewerte aus den Erhebungszeitpunkten T1 und T0. Daraus ergibt sich, dass die Unterweisung als alleinige Sensibilisierungsmaßnahme nicht ausreichend ist, um sicherheitskonformes Verhalten der Teilnehmenden nachhaltig im Kontext „Passwortmanagement“ zu fördern.

Die Resultate der Mittelwertanalyse für den Kontext „Umgang mit Informationen u. a. im Kontext mobiler Arbeit“ bestätigen, dass die Unterweisung die Einstellung und das Verhalten in Bezug auf die Informationssicherheit nachhaltig fördern kann, da die Ergebnisse des Erhebungszeitpunkts T4 in diesen beiden Konstrukten höher sind als die der Erhebungszeitpunkte T0. Allerdings kann sich die Unterweisung nicht als eine nachhaltige Maßnahme für das Konstrukt „Wissen“ beweisen, da das Ergebnis der Mittelwertanalyse für den Erhebungszeitpunkt T4 im Konstrukt „Wissen“ niedriger ist als das aus dem Erhebungszeitpunkt T0.

Im Kontext „Umgang mit (mobilen) Speicher- und Endgeräten“ zeigen die Ergebnisse der Mittelwertanalyse eine nachhaltige Förderung der Informationssicherheits-Awareness des Konstrukts „Wissen“, weil die Resultate der Erhebung T4 höher sind als die der Erhebungen T1 und T0, allerdings sind in den Konstrukten „Einstellung“ und „Verhalten“ die Mittelwertergebnisse zwar höher als die Ergebnisse der T0-Erhebung, jedoch niedriger als die Ergebnisse der T1-Erhebung.

Im Kontext „Zutritts- und Zugriffsschutz“ ist der Mittelwert der T4-Erhebung im Konstrukt „Wissen“ höher als der Mittelwert der T0-Erhebung. Dies trifft auch für das Konstrukt „Verhalten“ zu. Im Konstrukt „Einstellung“ hingegen ist der Mittelwert der T4-Erhebung etwas niedriger als der der T0-Erhebung.

Tabelle 48: Ergebnisse der Mittelwertanalyse für die Gruppe B vom Erhebungszeitpunkt T0 bis zum Erhebungszeitpunkt T4

Kontext	Konstrukt	$\bar{x}$ in T0	$\bar{x}$ in T1	$\bar{x}$ in T2	$\bar{x}$ in T3	$\bar{x}$ in T4
E-Mail-Bearbeitung	Wissen	3,83	4,31	x	x	4,07
	Einstellung	3,88	4,21	x	x	4,09
	Verhalten	3,84	4,14	x	x	3,54

(Fortsetzung Tabelle 48)

Kontext	Konstrukt	x̄ in T0	x̄ in T1	x̄ in T2	x̄ in T3	x̄ in T4
Passwortmanagement	Wissen	3,87	4,62	x	x	3,99
	Einstellung	3,76	4,21	x	x	4,02
	Verhalten	3,58	4,38	x	x	3,56
Umgang mit Informationen u. a. im Kontext mobiler Arbeit	Wissen	4,30	4,57	x	x	4,14
	Einstellung	3,59	4,31	x	x	4,17
	Verhalten	2,99	3,87	x	x	3,51
Umgang mit (mobilen) Speicher- und Endgeräten	Wissen	3,89	4,12	x	x	4,24
	Einstellung	4,23	4,48	x	x	4,34
	Verhalten	3,91	4,28	x	x	4,15
Zutritts- und Zugriffsschutz	Wissen	3,90	4,21	x	x	4,19
	Einstellung	4,19	4,25	x	x	4,13
	Verhalten	4,01	4,29	x	x	4,17

Im Folgenden sollen die Ergebnisse der Erhebung T4 von Gruppe A und Gruppe B verglichen werden. Grundsätzlich zeigt die Mittelwertanalyse, dass die Security Arena als zusätzliche Awareness-Maßnahme effektiv bei der Förderung von Wissen in den Awareness-Kontexten „E-Mail-Bearbeitung“ und „Passwortmanagement“ ist. Im Kontext „Umgang mit (mobilen) Speicher- und Endgeräten“ ist die Security Arena fast genauso effektiv bei der Förderung von Wissen wie eine klassische Unterweisung. Im Kontext „Umgang mit Informationen u. a. im Kontext mobiler Arbeit“ und „Zutritts- und Zugriffsschutz“ fördert eine klassische Unterweisung das Wissen besser als die Security Arena.

Was die Förderung der Einstellung angeht, sind die Ergebnisse der beiden Gruppen A und B fast identisch, jedoch hat sich die Security Arena als eine effektive Informationssicherheitsmaßnahme in den folgenden Kontexten erwiesen: „Passwortmanagement“ und „Umgang mit (mobilen) Speicher- und Endgeräten“. Wie die Ergebnisse der Mittelwertanalyse zeigen, ist die Security Arena in den Kontexten „E-Mail-Bearbeitung“, „Umgang mit Informationen u. a. im Kontext mobiler Arbeit“ und „Zutritts- und Zugriffsschutz“ fast genauso effektiv wie eine klassische Unterweisung. In diesen Kontexten kann eine klassische Unterweisung die Einstellung zu entsprechenden Sicherheits-Awareness-Maßnahmen also sogar etwas besser fördern als die Security Arena. Das Verhalten hinsichtlich Sicherheits-Awareness wird wiederum in allen Kontexten besser durch die Durchführung der zusätzlichen Security Arena gefördert.

4.6 Diskussion der Forschungsergebnisse

In diesem Kapitel werden die Einzelbeurteilungen der Ergebnisse in einer finalen Diskussion miteinbezogen. Zunächst sollen die Hypothesen überprüft werden, danach folgt die Beantwortung der Forschungsfragen. Am Ende des Kapitels werden die Limitationen der quantitativen Studie präsentiert.

4.6.1 Hypothesenüberprüfung und Forschungsfragenbeantwortung

Zusammenfassend müssen die der quantitativen Studie zugrunde liegenden Hypothesen überprüft werden. Es wird analysiert, ob und inwiefern die Ergebnisse der Studie die Hypothesen bestätigen oder widerlegen. Dafür werden alle in dieser Studie aufgelisteten Hypothesen nacheinander geprüft. Darauf basierend werden die Forschungsfragen der quantitativen Studie beantwortet.

H1 Die Informationssicherheits-Awareness der jungen Erwachsenen der Volkswagen AG verbessert sich nach der Durchführung der spielerischen Awareness-Veranstaltung zusätzlich zur klassischen Unterweisung im Zeitverlauf.

Diese Arbeitshypothese besagt, dass sich die Informationssicherheits-Awareness der Probanden dieser Studie im Zeitverlauf der Durchführung von Sensibilisierungsmaßnahmen signifikant verbessert, wie entsprechende Erhebungen zu verschiedenen Zeitpunkten zeigen sollen. Zur Überprüfung dieser Arbeitshypothese werden sowohl theoretische als auch empirische Erkenntnisse miteinander verglichen. In dieser Arbeitshypothese wird die Informationssicherheits-Awareness als eine Kombination von Wissen, Einstellung und Verhalten interpretiert (Kapitel 2.1). Das heißt, dass die drei Aspekte der Informationssicherheits-Awareness in einer Korrelation zueinander stehen und sich gegenseitig beeinflussen können. Dazu, inwiefern spielerische Awareness-Maßnahmen die Informationssicherheits-Awareness von Menschen tatsächlich fördern, herrscht in der dazugehörigen Forschung kein eindeutiger Konsens (siehe Kapitel 2.3). Allerdings beschreibt Scholl (2018a, S. 7 in Anlehnung u. a. an Albrechtsen, 2007; Straub & Welke, 1998; San Nicolas-Rocca, Schooley & Spears, 2014) in ihrer Studie, dass klassische Awareness-Maßnahmen, wie z. B. eine Präsentation, deren Hauptziel nur Wissenstransfer ist, keine dauerhafte Informationssicherheits-Awareness fördern – spielerische Maßnahmen wie die Security Arena bei verschiedenen Aspekten hingegen schon. Dies gilt als der erste theoretische Hinweis darauf, dass spielerische Maßnahmen in Kombination mit einer klassischen Unterweisung die Informationssicherheits-Awareness nachhaltig fördern können.

Zur Überprüfung wird die Auswertung der Mittelwerte in die Analyse einbezogen, mit deren Hilfe an dieser Stelle die Schritte der weiteren Hypothesenprüfung dargestellt werden.

Zuerst sollen die Mittelwerte der Zeitpunkte T0 und T4 für Gruppe A und Gruppe B gegenübergestellt werden, um die Hypothese H1 zu überprüfen und zu analysieren, ob alle Konstrukte der Informationssicherheits-Awareness der jungen Erwach-

senen der Volkswagen AG sich nach der Durchführung der spielerischen Awareness-Veranstaltung zusätzlich zur klassischen Unterweisung im Zeitverlauf verbessern.

Dabei zeigen die Mittelwerte von T0 das Awareness-Niveau von Wissen, Einstellung und Verhalten der Gruppe A und Gruppe B vor der Durchführung aller Awareness- bzw. Trainingsmaßnahmen. Die Mittelwerte von T4 veranschaulichen das Awareness-Niveau von Wissen, Einstellung und Verhalten von Gruppe A (die mit einer Unterweisung und Security Arena sensibilisiert wurde) und Gruppe B (die nur mit einer Unterweisung sensibilisiert wurde) nach der Durchführung der jeweiligen Awareness-Maßnahmen. Mithilfe der Veränderung dieser Werte im zeitlichen Verlauf der durchgeführten Awareness-Maßnahmen lassen sich die nachhaltigen Effekte der jeweils zu verzeichnenden Entwicklungen erfassen. Hierzu werden im Folgenden die Mittelwerte aller Kontexte für die beiden Gruppen separat und im Vergleich diskutiert.

Um die Informationssicherheits-Awareness an sich statistisch vergleichbar zu veranschaulichen, werden zuerst alle Konstrukte der Sicherheits-Awareness (Wissen, Einstellung und Verhalten) für jeden Kontext separat, sowohl für Gruppe A als auch für Gruppe B, dargestellt und mathematisch zusammengefasst. Im Ergebnis wird ein Durchschnittswert pro Kontext ausgewiesen.

Danach werden die Gruppen A und B vergleichend gegenübergestellt, um zu interpretieren, inwiefern sich die Informationssicherheits-Awareness der jungen Erwachsenen der Volkswagen AG nach der Durchführung der spielerischen Awareness-Veranstaltung zusätzlich zur klassischen Unterweisung im Zeitverlauf unterscheidet.

Auf Grundlage dieser Analysen können Schlussfolgerungen gezogen und es kann geprüft werden, ob Hypothese 1 bestätigt oder widerlegt werden kann.

Tabelle 49 stellt zunächst die ausgewählten Mittelwerte für Gruppe A für die Erhebungszeitpunkte T0 und T4 gegenüber und weist aus, wie sich diese Werte über den Zeitverlauf verändert haben (Spalte $\bar{x}$ T4-T0).

Tabelle 49: Mittelwerte für T0 und T4 (siehe. Tab. 47) im Vergleich beider Erhebungszeitpunkte – Gruppe A

Kontext	Konstrukt	$\bar{x}$ in T0	$\bar{x}$ in T4	$\bar{x}$ T4-T0
E-Mail-Bearbeitung	Wissen	3,69	4,35	0,66
	Einstellung	3,81	4,02	0,21
	Verhalten	3,45	3,88	0,43
Passwortmanagement	Wissen	3,87	4,04	0,17
	Einstellung	3,65	4,08	0,43
	Verhalten	3,57	3,71	0,14
Umgang mit Informationen u. a. im Kontext mobiler Arbeit	Wissen	4,28	4,03	–0,25
	Einstellung	3,67	4,16	0,49
	Verhalten	3,34	4,43	1,09

(Fortsetzung Tabelle 49)

Kontext	Konstrukt	$\bar{x}$ in T0	$\bar{x}$ in T4	$\bar{x}$ T4-T0
Umgang mit (mobilen) Speicher- und Endgeräten	Wissen	3,81	4,27	0,46
	Einstellung	4,02	4,36	0,34
	Verhalten	3,94	4,25	0,31
Zutritts- und Zugriffsschutz	Wissen	3,75	4,1	0,35
	Einstellung	4,21	4,08	–0,13
	Verhalten	3,83	4,30	0,47

Im Kontext „E-Mail-Bearbeitung" weisen alle Konstrukte eine positive Veränderung auf. Im Konstrukt „Wissen" ist diese Veränderung am größten. Dies führt zur Schlussfolgerung, dass die Security Arena und die Unterweisung generell effektiv für die nachhaltige Förderung des Kontextes „E-Mail-Bearbeitung" sind, beide Awareness-Maßnahmen das Konstrukt „Wissen" diesbezüglich aber am meisten fördern. Also kann im Kontext „E-Mail-Bearbeitung" beobachtet werden, dass das steigende Wissen mit Verbesserungen in der Einstellung und im Verhalten einhergeht.

Im Kontext „Passwortmanagement" können auch positive Veränderungen in allen Konstrukten beobachtet werden, die größte Veränderung allerdings im Konstrukt „Einstellung". Daraus folgt, dass Unterweisung und Security Arena eine allgemein positive Veränderung im Kontext „Passwortmanagement" fördern, am effektivsten aber auf das Konstrukt „Einstellung" einwirken. Im Kontext „Passwortmanagement" kann folglich auch eine Beobachtung der positiven Entwicklung von Einstellung und Verhalten festgestellt werden.

Im Kontext „Umgang mit Informationen u. a. im Kontext mobiler Arbeit" sind positive Veränderungen in den Konstrukten „Einstellung" und „Verhalten" zu verzeichnen, im Konstrukt „Wissen" sind diese Veränderungen hingegen negativ. Die stärkste positive Veränderung zeigt sich in diesem Kontext im Verhalten, während gleichzeitig das Wissen abnimmt. Folglich lässt sich festhalten, dass die Security Arena und die Unterweisung im Konstrukt „Wissen" weniger effektiv wirken, aber deutlich effektiv in den Konstrukten „Einstellung" und „Verhalten". Damit ist für den Kontext „Umgang mit Informationen u. a. im Kontext mobiler Arbeit" festzustellen, dass positive Veränderungen in den Kontexten Einstellung und Verhalten nicht mit ansteigendem Wissen erklärt werden können; somit steht mit dieser Beobachtung die Annahme eines Kausalzusammenhangs infrage. Demgegenüber könnte die positive Veränderung im Konstrukt „Verhalten" durch die gleichzeitige Veränderung der „Einstellung" teilweise erklärt werden.

Was den Kontext „Umgang mit (mobilen) Speicher- und Endgeräten" betrifft, sind die Veränderungen des Wissens, der Einstellung und des Verhaltens insgesamt positiv, am größten jedoch im Konstrukt „Wissen". Daraus resultiert, dass die Security Arena und die Unterweisung einen positiven Effekt im Zeitverlauf auf alle Konstrukte des Kontextes „Umgang mit (mobilen) Speicher- und Endgeräten" haben. Auch hier

ist festzustellen, dass eine positive Veränderung im Wissen mit positiven Veränderungen in der Einstellung und im Verhalten einhergeht.

Im Kontext „Zutritts- und Zugriffsschutz“ weisen das Wissen und das Verhalten positive Veränderungen auf, im Konstrukt „Einstellung“ wird hingegen im Zeitverlauf eine negative Veränderung nachgewiesen. Es ist festzustellen, dass sich die stärkste positive Veränderung in diesem Kontext im Verhalten zeigt, während gleichzeitig die Einstellung abnimmt. Auch mit dieser Beobachtung ist die Annahme eines Kausalzusammenhangs zwischen positiven Veränderungen des Wissens mit entsprechenden Veränderungen der Einstellung und des Verhaltens zu hinterfragen.

Somit kann lediglich für das Konstrukt „Verhalten“ eine positive Veränderung in allen Kontexten der Gruppe A festgestellt werden.

Im zweiten Schritt sollen die Mittelwerte der Gruppe B für die Zeitpunkte T0 und T4 gegenübergestellt und deren Entwicklung über den Zeitverlauf (Spalte $\bar{x}$ T4-T0) diskutiert werden. Allgemein kann festgestellt werden, dass die Konstrukte in vielen Kontexten eine relativ geringe oder sogar negative Entwicklung aufweisen. Die Ergebnisse sind in Tabelle 50 präsentiert.

Tabelle 50: Mittelwerte für T0 und T4 (vgl. Tabelle. 48) im Vergleich beider Erhebungszeitpunkte – Gruppe B

Kontext	Konstrukt	$\bar{x}$ in T0	$\bar{x}$ in T4	$\bar{x}$ T4-T0
E-Mail-Bearbeitung	Wissen	3,83	4,07	0,24
	Einstellung	3,88	4,09	0,21
	Verhalten	3,84	3,54	–0,3
Passwortmanagement	Wissen	3,87	3,99	0,12
	Einstellung	3,76	4,02	0,26
	Verhalten	3,58	3,56	–0,02
Umgang mit Informationen u. a. im Kontext mobiler Arbeit	Wissen	4,3	4,14	–0,16
	Einstellung	3,59	4,17	0,58
	Verhalten	2,99	3,51	0,52
Umgang mit (mobilen) Speicher- und Endgeräten	Wissen	3,89	4,24	0,35
	Einstellung	4,23	4,34	0,11
	Verhalten	3,91	4,15	0,24
Zutritts- und Zugriffsschutz	Wissen	3,9	4,19	0,29
	Einstellung	4,19	4,13	–0,06
	Verhalten	4,01	4,17	0,16

Im Kontext „E-Mail-Bearbeitung“ kann eine positive Veränderung in den Kontexten „Wissen“ und „Einstellung“ festgestellt werden. Im Kontext „Verhalten“ ist diese Ver-

änderung allerdings negativ, was zur Schlussfolgerung führt, dass sich eine Unterweisung zwar positiv auf das Wissen und die Einstellung im Kontext „E-Mail-Bearbeitung“ auswirkt, sich aber nicht in einer nachhaltigen Verbesserung für das Konstrukt „Verhalten“ niederschlägt. Zwischen den Entwicklungen der beiden Gruppen zeigt sich hier ein ausgeprägter Unterschied.

Im Kontext „Passwortmanagement“ können ähnliche Veränderungen festgestellt werden. Das Wissen und die Einstellung des Kontextes „Passwortmanagement“ haben positive Veränderungen und das Verhalten verändert sich ebenfalls negativ. Die Unterweisung als alleinige Maßnahme ist hier ebenfalls effektiv für Veränderungen des Wissens und der Einstellung, allerdings nicht für das Konstrukt „Verhalten“.

Im Kontext „Umgang mit Informationen u. a im Kontext mobiler Arbeit“ ist dies umgekehrt: Positive Veränderungen in den Konstrukten „Einstellung“ und „Verhalten“ gehen mit einer negativen Veränderung im Konstrukt „Wissen“ einher. Zu bemerken ist, dass sich in diesem Kontext die stärkste positive Veränderung in der Einstellung und im Verhalten zeigt, während gleichzeitig das Wissen abnimmt, genauso wie in Gruppe A.

Lediglich im Kontext „Umgang mit (mobilen) Speicher- und Endgeräten“ hat die Unterweisung positive Effekte für alle Konstrukte, deren Werte sich positiv im Zeitverlauf verändern. Wiederum sind widersprüchliche Ergebnisse für den Kontext „Zutritts- und Zugriffsschutz“ festzuhalten. Hier hat die Unterweisung zwar einen positiven Effekt auf das Wissen, allerdings geringe, leicht negative Effekte auf die Einstellung und positive Effekte auf das Verhalten.

Vor dem Hintergrund dieser Beobachtungen ist die aus der Theoriearbeit entwickelte Annahme kausaler Zusammenhänge zwischen den Veränderungen im Wissen, in der Einstellung und im Verhalten zu hinterfragen (vgl. hierzu auch Hypothese 2). Generell kann für Gruppe B festgestellt werden, dass gerade für das in der beruflichen Praxis wichtige Konstrukt „Verhalten“ nachhaltige Entwicklungen in zwei von fünf Kontexten negativ ausfallen. Folglich erscheint die alleinige Unterweisung als Trainingskonzept hinsichtlich ihrer Wirksamkeit nicht zweckmäßig.

Tabelle 51: Durchschnittliche Entwicklung in den jeweiligen Kontextgruppen im Vergleich

Kontext	je Kontext (Gruppe A)	je Kontext (Gruppe B)	Differenz zwischen beiden Gruppen
E-Mail-Bearbeitung	0,43	0,05	0,38
Passwortmanagement	0,25	0,12	0,13
Umgang mit Informationen u. a. im Kontext mobiler Arbeit	0,44	0,31	0,13
Umgang mit (mobilen) Speicher- und Endgeräten	0,37	0,23	0,14
Zutritts- und Zugriffsschutz	0,23	0,13	0,10
Durchschnittliche Entwicklung	*0,34*	*0,16*	*0,17*

Für die vergleichende Gegenüberstellung der Untersuchungs- und Vergleichsgruppe ist es hilfreich, deren Entwicklung in den einzelnen Awareness-Kontexten anschaulich zu illustrieren. Hierzu wurden für die Zeiträume T0 und T4 zuerst die arithmetischen Mittelwerte der drei Konstruktkategorien (Wissen, Einstellung und Verhalten) gebildet und anschließend wurde die Differenz zwischen den beiden Gruppen ausgewiesen (Tab. 51). Zur weiteren Illustration enthält die Tabelle auch die durchschnittliche Entwicklung in Form des arithmetischen Mittelwerts über alle Kontexte.

Generell ist zunächst zu erkennen, dass die Entwicklung der Gruppe A deutlich positiver ausgeprägt ist und deren Mittelwert um 0,17 höher ausfällt als bei Gruppe B. Bei der Analyse der einzelnen Kategorien ist erkennbar, dass die Mittelwerte für jeden Kontext für Gruppe A deutlich höher ausfallen als für Gruppe B. Dies ist besonders gravierend für den Kontext „E-Mail-Bearbeitung" der Fall. Hier ist die Differenz zwischen der Gruppe A und der Gruppe B mit 0,38 am größten. Offensichtlich kommt der zusätzlichen Security Arena ein durchweg positiver Effekt für die nachhaltige Förderung der Informationssicherheits-Awareness zu.

Die anderen Kontexte zeigen auch eine deutliche Differenz zwischen den Awareness-Werten von Gruppe A und Gruppe B. Dies führt zur Schlussfolgerung, dass die Ergänzung einer klassischen Unterweisung um ein Training mittels Security Arena eine effektive Sensibilisierung für Wissen, Einstellungen und Verhaltensänderungen im Bereich der Informationssicherheits-Awareness gewährleistet und das Ergebnis für dieses Trainingskonzept im Vergleich zu einer klassischen Unterweisung deutliche Verbesserungen erbringt.

Damit kann die Grundannahme der Hypothese H1 bestätigt werden; es wurde festgestellt, dass die Informationssicherheits-Awareness der jungen Erwachsenen der Volkswagen AG sich nach der Durchführung der spielerischen Awareness-Veranstaltung zusätzlich zur klassischen Unterweisung im Zeitverlauf verbessert. Diese Aussage soll im Folgenden hinsichtlich der Teilhypothesen durch eine verlaufsbezogene Betrachtung der drei Konstrukte der Informationssicherheits-Awareness differenziert werden.

H1.1 Das Wissen der jungen Erwachsenen der Volkswagen AG über die Informationssicherheit verbessert sich nach der Durchführung der spielerischen Awareness-Veranstaltung zusätzlich zur klassischen Unterweisung im Zeitverlauf.

Diese Arbeitshypothese geht davon aus, dass die Teilnehmer dieser Studie nach der Durchführung der spielerischen Awareness-Veranstaltung zusätzlich zur klassischen Unterweisung über ein besseres Wissen hinsichtlich Informationssicherheitsaspekten verfügen. Zuerst wurden zur Überprüfung dieser Arbeitshypothese theoretische Analysen durchgeführt (siehe Kapitel 2.3). In der Forschung existieren Studien, die besagen, dass das Wissen über Informationssicherheit besser mit klassischen Sensibilisierungsmaßnahmen gefördert wird (vgl. Khan, et al., 2011). Khan, et al. (2011) geben zudem in ihrer Studie an, dass spielbasierte Informationssicherheits-Awareness-Methoden ungeeignete Sensibilisierungsmaßnahmen seien, weil diese Methoden keine

Komponente des Wissenstransfers beinhalten würden, die das Wissen hinsichtlich Informationssicherheit fördern könnte. Allerdings wurde in der Forschung bis jetzt noch nicht betrachtet, inwiefern eine klassische Unterweisung in Kombination mit einer spielerischen Methode Beschäftigten erfolgreich für das Thema Informationssicherheit sensibilisiert.

Um diese Arbeitshypothese zu überprüfen, soll die Analyse der Mittelwerte der Erhebungsergebnisse von T0 bis T4 durchgeführt werden. Danach soll der Vergleich zwischen den Mittelwertergebnissen der Gruppen A und B zum Zeitpunkt T4 stattfinden, um daraus interpretieren zu können, inwiefern sich das Wissen der Probanden zum Thema Informationssicherheits-Awareness im Zeitverlauf verändert hat.

Wie die Tabelle 52 veranschaulicht, existiert eine positive Veränderung der Mittelwerte direkt nach der Durchführung der jeweiligen Intervention bei beiden Gruppen bei folgenden Erhebungszeitpunkten: T1 (nach der klassischen Unterweisung) und T3 (nach der spielerischen Awareness-Veranstaltung); wobei für Gruppe B keine Erhebungsdaten für T2 und T3 vorliegen, im Vergleich zu den Mittelwerten T0 und T1.

Tabelle 52: Mittelwerte des Awareness-Bereiches „Wissen" von T0 bis T4 für die Gruppe A und die Gruppe B

Kontext	Konstrukt	Gruppe	$\bar{x}$ in T0	$\bar{x}$ in T1	$\bar{x}$ in T2	$\bar{x}$ in T3	$\bar{x}$ in T4
E-Mail-Bearbeitung	Wissen	Gruppe A	3,69	4,41	4,03	4,26	4,35
		Gruppe B	3,83	4,31	x	x	4,07
Passwort-management	Wissen	Gruppe A	3,87	4,71	3,87	4,09	4,04
		Gruppe B	3,87	4,62	x	x	3,99
Umgang mit Informationen u. a. im Kontext mobiler Arbeit	Wissen	Gruppe A	4,28	4,38	4,61	4,63	4,03
		Gruppe B	4,3	4,57	x	x	4,14
Umgang mit (mobilen) Speicher- und Endgeräten	Wissen	Gruppe A	3,81	4,26	4,47	4,62	4,27
		Gruppe B	3,89	4,12	x	x	4,24
Zutritts- und Zugriffsschutz	Wissen	Gruppe A	3,75	4,21	4,15	4,25	4,1
		Gruppe B	3,9	4,21	x	x	4,19

Die beiden Gruppen zeigen relativ ähnliche Mittelwerte bei der Erhebung T0. Die Aufteilung der Teilnehmer in die zwei Gruppen im Studienverlauf erfolgte nach dem Zufallsprinzip. Nach der Durchführung der ersten Awareness-Maßnahme bleiben die Mittelwerte relativ gleich. Die Ergebnisse der T1-Befragung zeigen, dass sich das Wissen sowohl bei Gruppe A als auch bei Gruppe B nach der Durchführung der Unterweisung deutlich verbessert hat.

Wie schon erwähnt wurde, wurde die Erhebung T2 nur mit der Gruppe A durchgeführt. Diese Erhebung wurde nach 6 Wochen (am 21.09.2020) nach der Erhebung T1

durchgeführt. Wie die Ergebnisse der Erhebung T2 zeigen, sind die Werte in den Kontexten „E-Mail-Bearbeitung“, „Passwortmanagement“ und „Zutritts- und Zugriffsschutz“ zwar im Vergleich zu den Ergebnissen der T1-Erhebung zurückgegangen, jedoch entsprechen den Werten der T0-Erhebung der Gruppe A oder sind sogar höher. Dies könnte dadurch erklärt werden, dass die Unterweisung einen relativ kurzfristigen Awareness-Effekt erzeugt. Die Ergebnisse der Kontexte „Umgang mit Informationen u. a. im Kontext mobiler Arbeit“ und „Umgang mit (mobilen) Speicher- und Endgeräten“ sind höher als die Ergebnisse der T1-Erhebung. Dies könnte dadurch erklärt werden, dass die Teilnehmer in der Zeit zwischen den Erhebungen T1 und T2 eine zusätzliche Sensibilisierung genau zu den Themen erhalten haben.

Die Gruppe A absolvierte unmittelbar im Anschluss an die Erhebung T2 eine zusätzliche Sensibilisierungsmaßnahme in Form der Security Arena. Direkt nach der Security Arena wurde mit der Gruppe A die Erhebung T3 durchgeführt. Die Ergebnisse der Erhebung T3 zeigen, dass die Security Arena einen positiven Effekt auf die Veränderung der Wissenswerte hat, wenn auch einen nicht so großen.

Um die Nachhaltigkeit der Unterweisung mit Security Arena im Gegensatz zum ausschließlichen Erhalt einer Unterweisung zu überprüfen, wurde entschieden, die Erhebung T4 mit Gruppe A und Gruppe B durchzuführen. Folgend sollen die Differenzen zwischen den Ergebnissen der T0- und T4-Erhebung hinsichtlich der Wissensveränderung erörtert werden. Die Ergebnisse sind in Tabelle 53 veranschaulicht.

Tabelle 53: Mittelwerte des Awareness-Bereiches „Wissen“ für T0 und T4 für die Gruppe A und die Gruppe B

Kontext	Konstrukt	Gruppe A			Gruppe B		
		$\bar{x}$ in T0	$\bar{x}$ in T4	$\bar{x}$ T4-T0	$\bar{x}$ in T0	$\bar{x}$ in T4	$\bar{x}$ T4-T0
E-Mail-Bearbeitung	Wissen	3,69	4,35	0,66	3,83	4,07	0,24
Passwortmanagement	Wissen	3,87	4,04	0,17	3,87	3,99	0,12
Umgang mit Informationen u. a. im Kontext mobiler Arbeit	Wissen	4,28	4,03	–0,25	4,3	4,14	–0,16
Umgang mit (mobilen) Speicher- und Endgeräten	Wissen	3,81	4,27	0,46	3,89	4,24	0,35
Zutritts- und Zugriffsschutz	Wissen	3,75	4,1	0,35	3,9	4,19	0,29

Im Kontext „E-Mail-Bearbeitung“ verweisen die Werte auf eine große Differenz zwischen Gruppe A und Gruppe B. Die Ergebnisse der Gruppe A sind höher als die Ergebnisse der Gruppe B, was bedeutet, dass die Sensibilisierung mit einer Unterweisung und zusätzlichen Security Arena im Zeitverlauf effektiver als die Sensibilisierung

mit nur einer Unterweisung war. Auch die Ergebnisse nur T4-Erhebung weisen darauf hin, dass Gruppe A effektiver sensibilisiert wurde als Gruppe B.

Ähnliche Ergebnisse finden sich im Kontext „Passwortmanagement". Die Differenz zwischen T0 und T4 bei der Gruppe A ist höher als die Differenz zwischen T0 und T4 bei der Gruppe B. Ergänzend dazu sind die Resultate der T4-Erhebung bei Gruppe A auch größer als bei Gruppe B. Daraus kann die Schlussfolgerung gezogen werden, dass die Sensibilisierung mit einer Unterweisung und zusätzlichen Security Arena im Kontext „Passwortmanagement" effektiver ist als die Sensibilisierung mit ausschließlich einer Unterweisung.

Im Kontext „Umgang mit Informationen u. a. im Kontext mobiler Arbeit" weist die Gruppe B deutlich bessere Ergebnisse als die Gruppe A auf, da die Resultate der T4-Erhebung bei Gruppe B größer sind. Einschränkend ist allerdings zu vermerken, dass diese dennoch niedriger als die Resultate der T0-Erhebung bei beiden Gruppen sind. Dies belegt, dass die Sensibilisierung mit einer Unterweisung und der zusätzlichen Security Arena im Kontext „Umgang mit Informationen u. a. im Kontext mobiler Arbeit" im Zeitverlauf weniger effektiv ist als die Sensibilisierung mit nur einer Unterweisung.

Im Kontext „Umgang mit (mobilen) Speicher- und Endgeräten" hat Gruppe A bessere Ergebnisse bei der Erhebung T4 und eine größere Differenz zwischen T4 und T0 als Gruppe B. Daher kann die Schlussfolgerung gezogen werden, dass die Sensibilisierung mit einer Unterweisung und zusätzlichen Security Arena effektiver im Zeitverlauf ist als die Sensibilisierung mit ausschließlich einer Unterweisung.

Im Kontext „Zutritts- und Zugriffsschutz" zeigen Gruppe A und Gruppe B ähnliche Resultate bei der Erhebung T4, jedoch ist die Differenz zwischen T4 und T0 bei Gruppe A größer. Folglich kann die größere Effektivität der Sensibilisierung mit einer Unterweisung und der zusätzlichen Security Arena im Vergleich zur Sensibilisierung mit nur einer Unterweisung festgestellt werden.

Die deutlich höheren Ergebnisse von Gruppe A im Vergleich zu Gruppe B in den Kontexten „E-Mail-Bearbeitung" und „Passwortmanagement" im Konstrukt „Wissen" können dadurch erklärt werden, dass die Security Arena Spielstationen zu beiden Kontexten anbietet, wo eine interaktive Teilnahme der Probanden gefördert wird. In der Spielstation zum Thema „E-Mail-Bearbeitung" können die Teilnehmer z. B. ausgedruckte E-Mails aus dem improvisierten Kartonpool rausfischen und entscheiden, ob die ausgewählte E-Mail die Kriterien einer Phishing-E-Mail erfüllt. In der Spielstation zum Thema „Passwortmanagement" haben die Teilnehmer die Möglichkeit, sich in die Rolle eines „Hackers" zu versetzen und eine vorprogrammierte Webseite anhand von zur Verfügung gestellten Informationen zu hacken. So lernen die Teilnehmer aktiv z. B. die Wichtigkeit, ein sicheres Passwort zu haben.

Somit kann die Arbeitshypothese H1.1, dass sich das Wissen der jungen Erwachsenen der Volkswagen AG über die Informationssicherheit nach der Durchführung der spielerischen Awareness-Veranstaltung zusätzlich zur klassischen Unterweisung im Zeitverlauf verbessert, teilweise bestätigt werden.

H1.2 Die Einstellung der jungen Erwachsenen der Volkswagen AG zum Thema Informationssicherheit verbessert sich nach der Durchführung der spielerischen Awareness-Veranstaltung zusätzlich zur klassischen Unterweisung im Zeitverlauf.

Die vorliegende Arbeitshypothese besagt, dass die jungen Mitarbeiter bei Volkswagen nach der Durchführung der Security Arena zusätzlich zur klassischen Unterweisung im Zeitverlauf aufmerksamer in Bezug auf Informationssicherheitslücken werden. Generell existiert in der Forschung die einheitliche Meinung, dass eine Informationssicherheits-Awareness-Maßnahme nur dann effektiv ist, wenn diese die Einstellung der Beteiligten ändert und diese auf der emotionalen Eben anspricht, wie dies z. B. die spielerische Maßnahme „Security Arena" vermag (Scholl, 2018a S. 17 in Anlehnung u. a. an Albrechtsen, 2007). Allerdings beschreiben Khan et al. (2011), dass die reine Unterweisung („educational presentation", siehe Kapitel 2.3) auch Komponenten der Einstellungsänderung beinhaltet. Hieraus ergaben sich die Frage, welche der Maßnahme letzten Endes die effektivere ist, und mögliche Hinweise, dass sich die Einstellung der jungen Erwachsenen der Volkswagen AG zum Thema Informationssicherheit nach der Durchführung der spielerischen Awareness-Veranstaltung zusätzlich zur klassischen Unterweisung verbessern könnte.

Im Folgenden werden auch für diese Hypothese die Ergebnisse der Mittelwerte von T0 bis T4 für beide Gruppen miteinander verglichen, um zu erfahren, inwiefern sich die Einstellung der Probanden zum Thema Informationssicherheits-Awareness im Zeitverlauf verändert hat. Die Ergebnisse sind in Tabelle 54 dargestellt.

Vor der jeweiligen Sensibilisierung zeigen beide Gruppen laut Mittelwertanalyse der T0-Erhebung relativ ähnliche Ergebnisse in allen Kontexten, bis auf den Kontext „Umgang mit (mobilen) Speicher- und Endgeräten", wo der Unterschied zwischen Gruppe A und Gruppe B > 0,20 beträgt. Die Ergebnisse der T1-Befragung verdeutlichen, dass beide Gruppen teilweise signifikante positive Veränderungen in der Einstellung nach der Durchführung der Unterweisung aufweisen.

Tabelle 54: Mittelwerte des Awareness-Bereiches „Einstellung" von T0 bis T4 für die Gruppe A und die Gruppe B

Kontext	Konstrukt	Gruppe	$\bar{x}$ in T0	$\bar{x}$ in T1	$\bar{x}$ in T2	$\bar{x}$ in T3	$\bar{x}$ in T4
E-Mail-Bearbeitung	Einstellung	Gruppe A	3,81	4,02	3,86	4,17	4,02
		Gruppe B	3,88	4,21	x	x	4,09
Passwort-management	Einstellung	Gruppe A	3,65	4,38	4,66	4,63	4,08
		Gruppe B	3,76	4,21	x	x	4,02
Umgang mit Informationen u. a. im Kontext mobiler Arbeit	Einstellung	Gruppe A	3,67	4,23	4,56	4,52	4,16
		Gruppe B	3,59	4,31	x	x	4,17

(Fortsetzung Tabelle 54)

Kontext	Konstrukt	Gruppe	x̄ in T0	x̄ in T1	x̄ in T2	x̄ in T3	x̄ in T4
Umgang mit (mobilen) Speicher- und Endgeräten	Einstellung	Gruppe A	4,02	4,61	4,63	4,72	4,36
		Gruppe B	4,23	4,48	x	x	4,34
Zutritts- und Zugriffs-schutz	Einstellung	Gruppe A	4,21	4,41	4,40	4,50	4,08
		Gruppe B	4,19	4,25	x	x	4,13

Nach einigen Wochen nach der Durchführung der T1-Erhebung wurde die Erhebung T2 durchgeführt, an der nur die Gruppe A teilgenommen hat. Wie die Ergebnisse von T2 zeigen, haben sich nur die Mittelwerte für den Kontext „E-Mail-Bearbeitung“ und „Zutritts- und Zugriffsschutz“ verschlechtert. In den Kontexten „Passwortmanagement“, „Umgang mit Informationen u. a. im Kontext mobiler Arbeit“ und „Umgang mit (mobilen) Speicher- und Endgeräten“ haben sich die Ergebnisse sogar verbessert. Dies könnte dadurch erklärt werden, dass die Teilnehmer in der Zeit eine weitere informelle Sensibilisierung im beruflichen Alltag durch ihre Kollegen bekommen haben. Obwohl die Ergebnisse der T2-Erhebung in einigen Kontexten niedriger sind als die Ergebnisse der T1-Erhebung, sind die Ergebnisse der T2-Erhebung jedoch höher als die Ergebnisse der ersten Erhebung T0.

Direkt nach der Durchführung der T2-Erhebung fand die Security Arena statt und direkt danach wurde die Erhebung T3 durchgeführt. An dieser Erhebung hat auch nur die Gruppe A teilgenommen. Die Ergebnisse der Erhebung sind bei der Mehrheit der Kontexte höher als die Ergebnisse der T2-Erhebung – bis auf die Kontexte „Passwortmanagement“ und „Umgang mit Informationen u. a. im Kontext mobiler Arbeit“, wo die Ergebnisse eine leichte Senkung der Mittelwerte aufweisen.

Die Erhebung T4 wurde am 21.10.2020, also wenige Wochen nach der Durchführung von Erhebung T3 durchgeführt. Wie die Ergebnisse der Tabelle 55 veranschaulichen, sind die Ergebnisse der T4-Erhebung bei Gruppe A und Gruppe B fast identisch und in einigen Kontexten sind die Ergebnisse der Gruppe B sogar höher als die Ergebnisse der Gruppe A. Allerdings ist die Differenz zwischen T0 und T4 bei Gruppe A bei den Kontexten „Passwortmanagement“ und „Umgang mit (mobilen) Speicher- und Endgeräten“ deutlich höher als die entsprechende Differenz bei Gruppe B. Daraus lässt sich schlussfolgern, dass die Sensibilisierung in Form von einer Unterweisung mit zusätzlicher Security Arena in diesen Kontexten im Zeitverlauf effektiver ist als eine reine Unterweisung. Bei anderen Kontexten ist die Differenz zwischen T0 und T4 bei Gruppe B gleich (Kontext „E-Mail-Bearbeitung“) oder höher (Kontexte „Umgang mit Informationen u. a. im Kontext mobiler Arbeit“ und „Zutritts- und Zugriffsschutz“) als bei Gruppe A. Das heißt, dass die Sensibilisierung mit einer Unterweisung und der zusätzlichen Security Arena hier nicht so effektiv ist wie die Sensibilisierung mit ausschließlicher Unterweisung.

Tabelle 55: Mittelwerte des Awareness-Bereiches „Einstellung“ für T0 und T4 für die Gruppe A und die Gruppe B

	Gruppe A				Gruppe B		
Kontext	**Konstrukt**	**x̄ in T0**	**x̄ in T4**	**x̄ T4-T0**	**x̄ in T0**	**x̄ in T4**	**x̄ T4-T0**
E-Mail-Bearbeitung	Einstellung	3,81	4,02	0,21	3,88	4,09	0,21
Passwortmanagement	Einstellung	3,65	4,08	0,43	3,76	4,02	0,26
Umgang mit Informationen u. a. im Kontext mobiler Arbeit	Einstellung	3,67	4,16	0,49	3,59	4,17	0,58
Umgang mit (mobilen) Speicher- und Endgeräten	Einstellung	4,02	4,36	0,34	4,23	4,34	0,11
Zutritts- und Zugriffsschutz	Einstellung	4,21	4,08	–0,13	4,19	4,13	–0,06

Folglich kann die Hypothese H1.2, dass sich die Einstellung der jungen Erwachsenen der Volkswagen AG zum Thema Informationssicherheit nach der Durchführung der spielerischen Awareness-Veranstaltung zusätzlich zur klassischen Unterweisung im Zeitverlauf verbessert, nur teilweise bestätigt werden.

H1.3 Nach der Durchführung der spielerischen Awareness-Veranstaltung zusätzlich zur klassischen Unterweisung verhalten sich die jungen Erwachsenen der Volkswagen AG bewusster den Anforderungen des Themas Informationssicherheit gegenüber.

Diese Hypothese besagt, dass das Verhalten der Teilnehmer von einer spielerischen Awareness-Veranstaltung zusätzlich zur klassischen Unterweisung positiv beeinflusst werden sollte und sie sich danach entsprechend umsichtiger in Bezug auf Informationssicherheitsthemen verhalten sollten.

Generell existiert in der Forschung keine einheitliche Meinung darüber, welche Informationssicherheits-Awareness-Maßnahme das Verhalten von Menschen hinsichtlich der Informationssicherheit verbessert. Khan et al. (2011) erwähnen in ihrer Studie, dass eine klassische Unterweisung das Verhalten gegenüber der Informationssicherheit im Vergleich zu einer spielerischen Maßnahme effektiver beeinflusst. Nach Scholl aber (2018b, S. 34) hat sich bestätigt, dass sich die Security Arena besser als spielerische Maßnahme zur Beeinflussung von Verhalten eignet. Hieraus ergaben sich Hinweise dafür, dass eine klassische Unterweisung mit zusätzlich veranstalteter Security Arena eine positive Veränderung des Verhaltens der Teilnehmenden dieser Studie hinsichtlich der Informationssicherheit erzeugen könnte.

Um diese Arbeitshypothese weiter zu überprüfen, wird analog zur Überprüfung der Hypothesen H1, H1.1 und H1.2 ein Vergleich der Mittelwerte im Zeitverlauf von T0 bis T4 vorgenommen, ehe die Differenzwerte zwischen T4 und T0 herangezogen wer-

den, um eine mögliche Verhaltensänderung der Probanden in Bezug auf Informationssicherheits-Awareness zu eruieren.

Vor der jeweiligen Sensibilisierung sind die T0-Ergebnisse der Gruppen A und B in Bezug auf die Kontexte „Umgang mit (mobilen) Speicher- und Endgeräten“ und „Passwortmanagement“ relativ ähnlich, bei den anderen drei Kontexten weisen die Werte hingegen eine größere Spannbreite auf. An dieser Stelle ist hervorzuheben, dass Gruppe B im Kontext „E-Mail-Bearbeitung“ bei T0 bei allen drei Awareness-Bereichen (Wissen, Einstellung und Verhalten) einen besseren Mittelwert als Gruppe A hat (siehe Tabelle 56). Gruppe A hat ein besseres Mittelwertergebnis der T0-Erhebung als Gruppe B im Bereich „Verhalten“ in den Kontexten „Umgang mit Informationen u. a. im Kontext mobiler Arbeit“ und „Umgang mit mobilen Speicher- und Endgeräten“. Nach der Durchführung der Unterweisung wurde die Erhebung T1 durchgeführt. Die Ergebnisse dieser Erhebung zeigen deutlich, dass sich das Verhalten der beiden Gruppen äußerst positiv, in einigen Kontexten mit Werten > 0,80, verändert.

Wie schon erwähnt, wurde die Erhebung T2 6 Wochen nach der Erhebung T1 am 21.09.2020 durchgeführt. An der Erhebung T2 hat nur die Gruppe A teilgenommen. Die T2-Ergebnisse sind in einigen Kontexten niedriger als die T1-Ergebnisse, jedoch alle höher als die Werte zum Erhebungszeitpunkt T0. In den Kontexten „Umgang mit Informationen u. a. im Kontext mobiler Arbeit“ und „Umgang mit (mobilen) Speicher- und Endgeräten“ fallen die Ergebnisse der T2-Erhebung im Bereich Verhalten höher aus als die Ergebnisse der T1-Erhebung. Dies könnte dadurch erklärt werden, dass die Teilnehmenden aus Gruppe A in der Zeit zwischen den Erhebungen T1 und T2 eine Art der informellen Sensibilisierung (z. B. im Rahmen ihrer Einarbeitung) erhalten haben, die dazu beigetragen hat, das Verhalten der Teilnehmenden zu verändern.

Tabelle 56: Mittelwerte des Awareness-Bereiches „Verhalten“ von T0 bis T4 für die Gruppe A und die Gruppe B

Kontext	Konstrukt	Gruppe	$\bar{x}$ in T0	$\bar{x}$ in T1	$\bar{x}$ in T2	$\bar{x}$ in T3	$\bar{x}$ in T4
E-Mail-Bearbeitung	Verhalten	Gruppe A	3,45	4,31	3,96	4,18	3,88
		Gruppe B	3,84	4,14	x	x	3,54
Passwort-management	Verhalten	Gruppe A	3,57	4,32	3,82	3,84	3,71
		Gruppe B	3,58	4,38	x	x	3,56
Umgang mit Informationen u. a. im Kontext mobiler Arbeit	Verhalten	Gruppe A	3,34	3,72	4,16	4,66	4,43
		Gruppe B	2,99	3,87	x	x	3,51
Umgang mit (mobilen) Speicher- und Endgeräten	Verhalten	Gruppe A	3,94	4,54	4,55	4,70	4,25
		Gruppe B	3,91	4,28	x	x	4,15

(Fortsetzung Tabelle 56)

Kontext	Konstrukt	Gruppe	x̄ in T0	x̄ in T1	x̄ in T2	x̄ in T3	x̄ in T4
Zutritts- und Zugriffs-schutz	Verhalten	Gruppe A	3,83	4,42	4,21	4,37	4,30
		Gruppe B	4,01	4,29	x	x	4,17

Direkt nach der Durchführung der Erhebung T2 wurde mit den Teilnehmenden aus der Gruppe A die zusätzliche Security Arena durchgeführt. Die Ergebnisse des Erhebungszeitpunkts T3 zeigen deutlich, dass die Security Arena dazu beiträgt, das Verhalten zu verbessern. In einigen Kontexten sind die Ergebnisse von T3 deutlich besser als die Ergebnisse von T2, so hat sich z. B. im Kontext „Umgang mit Informationen u. a. im Kontext mobiler Arbeit" das Verhalten um 0,50 verbessert.

In Tabelle 57 sind die Werte des Differenzvergleichs der beiden Gruppen hinsichtlich des Zeitraums zwischen T0 und T4 ersichtlich.

Wie aus Tabelle 57 entnommen werden kann, sind die Ergebnisse der T4-Erhebung der Gruppe A in allen Kontexten deutlich höher als die Ergebnisse der Gruppe B. Das Gleiche gilt für die Differenz der Mittelwerte von T0 und T4. Der größte Unterschied zwischen den Erhebungszeitpunkten T0 und T4 der Gruppe A und Gruppe B findet sich in den Kontexten „Umgang mit Informationen u. a. im Kontext mobiler Arbeit", „E-Mail-Bearbeitung" und „Zutritts- und Zugriffsschutz". Dies führt zur Schlussfolgerung, dass die Sensibilisierung mit einer Unterweisung und Security Arena zu besseren Ergebnissen im Konstrukt „Verhalten" führt als eine Sensibilisierung mit nur einer Unterweisung.

Tabelle 57: Mittelwerte des Awareness-Bereiches „Verhalten" für T0 und T4 für die Gruppe A und die Gruppe B

Kontext	Konstrukt	Gruppe A			Gruppe B		
		x̄ in T0	x̄ in T4	x̄ T4-T0	x̄ in T0	x̄ in T4	x̄ T4-T0
E-Mail-Bearbeitung	Verhalten	3,45	3,88	0,43	3,84	3,54	–0,3
Passwortmanagement	Verhalten	3,57	3,71	0,14	3,58	3,56	–0,02
Umgang mit Informationen u. a. im Kontext mobiler Arbeit	Verhalten	3,34	4,43	1,09	2,99	3,51	0,52
Umgang mit (mobilen) Speicher- und Endgeräten	Verhalten	3,94	4,25	0,31	3,91	4,15	0,24
Zutritts- und Zugriffsschutz	Verhalten	3,83	4,30	0,47	4,01	4,17	0,16

Zusammenfassend kann die Hypothese H1.3, dass sich die jungen Erwachsenen nach der Durchführung der spielerischen Awareness-Veranstaltung zusätzlich zur klassischen Unterweisung bewusster den Anforderungen des Themas Informationssicherheit gegenüber verhalten, bestätigt werden.

H2 Einzelne Awareness-Bereiche korrelieren miteinander und haben einen Einfluss aufeinander.

Ein erster Hinweis für die Bestätigung dieser Arbeitshypothese konnte in der aktuellen Forschung gefunden werden. So kommen Parson et al. (2014, S. 172) in ihrer Studie teilweise zu dem Ergebnis, dass Wissen, Einstellung und Verhalten miteinander korrelieren und einen Einfluss aufeinander haben. Weiterhin wurde in der Analyse der Strukturmodelle (siehe Abb. 14) überprüft, inwiefern sich die Effektstärke der einzelnen exogenen Variable (unabhängige Variable „Wissen") auf die endogenen Variablen (abhängige Variablen „Einstellung" und „Verhalten") bestätigen lässt.

Tabelle 58: Mittelwerte der Awareness-Bereiche „Wissen-Einstellung-Verhalten" von T0 bis T4 für die Gruppe A mit den Entwicklungsdifferenzen zwischen den Erhebungsergebnissen

Kontext	Konstrukt	$\bar{x}$ in T0	$\bar{x}$ in T1	Differenz T1-T0	$\bar{x}$ in T2	Differenz T2-T1	$\bar{x}$ in T3	Differenz T3-T2	$\bar{x}$ in T4	Differenz T4-T3
E-Mail-Bearbeitung	Wissen	3,69	4,41	0,72	4,03	–0,38	4,26	0,23	4,35	0,09
	Einstellung	3,81	4,02	0,21	3,86	–0,16	4,17	0,31	4,02	–0,15
	Verhalten	3,45	4,31	0,86	3,96	–0,35	4,18	0,22	3,88	–0,3
Passwortmanagement	Wissen	3,87	4,71	0,84	3,87	–0,84	4,09	0,22	4,04	–0,05
	Einstellung	3,65	4,38	0,73	4,66	0,28	4,63	–0,03	4,08	–0,55
	Verhalten	3,57	4,32	0,75	3,82	–0,5	3,84	0,02	3,71	–0,13
Umgang mit Informationen u. a. im Kontext mobiler Arbeit	Wissen	4,28	4,38	0,1	4,61	0,23	4,63	0,02	4,03	–0,6
	Einstellung	3,67	4,23	0,56	4,56	0,33	4,52	–0,04	4,16	–0,36
	Verhalten	3,34	3,72	0,38	4,16	0,44	4,66	0,5	4,43	–0,23
Umgang mit (mobilen) Speicher- und Endgeräten	Wissen	3,81	4,26	0,45	4,47	0,21	4,62	0,15	4,27	–0,35
	Einstellung	4,02	4,61	0,59	4,63	0,02	4,72	0,09	4,36	–0,36
	Verhalten	3,94	4,54	0,6	4,55	0,01	4,7	0,15	4,25	–0,45
Zutritts- und Zugriffsschutz	Wissen	3,75	4,21	0,46	4,15	–0,06	4,25	0,1	4,1	–0,15
	Einstellung	4,21	4,41	0,2	4,4	–0,01	4,5	0,1	4,08	–0,42
	Verhalten	3,83	4,42	0,59	4,21	–0,21	4,37	0,41	4,30	–0,07

Dazu wurden die Beurteilung des Gütekriteriums Effektgröße f^2 über die fünf Ergebungszeitpunkte sowie die Beurteilung der Pfadkoeffizientenanalyse miteinbezogen. Obwohl letzteres Gütekriterium nicht direkt den Einfluss einer exogenen Variable auf eine endogene Variable zeigt, handelt es sich bei der Pfadkoeffizientenanalyse um eine Form der multiplen Regressionsanalyse, die sich an Kausalzusammenhängen orientiert (Nitzl, 2010, S. 34 in Anlehnung an Krafft, Götz & Liehr-Gobbers, 2005, S. 83). Darüber hinaus können bei der Betrachtung dieses Kriteriums die Einflüsse und Korrela-

tionen der einzelnen Awareness-Bereiche zusätzlich bestätigt oder widerlegt werden. Die detaillierte Beschreibung dieses Gütekriteriums ist in Kapitel 4.5.1.4 zu finden.

Die Mittelwertvergleiche zwischen den Konstrukten (Wissen, Einstellung und Verhalten) der Gruppen A und B über die Erhebungszeitpunkte hinweg werden in die Analyse einbezogen. Wie beschrieben wurde, gilt: Je größer das Wissen, desto informationssicherheitskonformer sollte die Einstellung und entsprechend auch das Verhalten sein. Dies wurde für jeden Kontext für jedes Konstrukt für beide Gruppen anhand der Differenzen zwischen T1 und T0 (für Gruppe A und B), zwischen T2 und T1 (für Gruppe A), zwischen T3 und T2 (für Gruppe A) und zwischen T4 und T3 (für Gruppe A) eruiert. Die Ergebnisse sind in den Tabellen 58 und 59 veranschaulicht.

Wie die Ergebnisse der ersten Erhebung T0 zeigen, kann die Korrelation der einzelnen Awareness-Bereiche festgestellt werden, da eine entsprechende Effektstärke vorhanden ist. Am größten jedoch ist der Einfluss von Wissen auf Einstellung im Kontext „Zutritts- und Zugriffsschutz". In den Kontexten „E-Mail-Bearbeitung" und „Umgang mit Informationen u. a. im Kontext mobiler Arbeit" ist der Einfluss von Wissen auf Einstellung gering und in den anderen Kontexten ist dieser Einfluss moderat. Der Einfluss der exogenen Variable „Wissen" auf die endogene Variable „Verhalten" ist im Kontext „Umgang mit (mobilen) Speicher- und Endgeräten" moderat und in den anderen Kontexten eher gering. Der Einfluss der Variable „Einstellung" auf die Variable „Verhalten" ist beim Erhebungszeitpunkt T0 insignifikant, bis auf den Kontext „Umgang mit (mobilen) Speicher- und Endgeräten", wo dieser Einfluss moderat ist. Die Ergebnisse der Effektgröße können auch teilweise durch die Pfadkoeffizientenanalyse bestätigt werden.

Die Ergebnisse des zweiten Erhebungszeitpunkts T1 bescheinigen, dass die Korrelation zwischen einzelnen Awareness-Bereichen vorhanden ist. Analog zur ersten T0-Erhebung ist hier der Einfluss des Wissens auf Einstellung im Kontext „Zutritts- und Zugriffsschutz" am größten. Dies wird auch durch die Ergebnisse der Pfadkoeffizientenanalyse bestätigt. Der Einfluss von Wissen auf Einstellung in anderen Kontexten bleibt jedoch insignifikant. Der Einfluss der Variable „Einstellung" auf die Variable „Verhalten" ist laut den Ergebnissen der Effektstärkeanalyse in allen Kontexten gering. Laut der Pfadkoeffizientenanalyse konnte aber eine starke Korrelation zwischen der Variable „Einstellung" und der Variable „Verhalten" in den Kontexten „Umgang mit Informationen u. a. im Kontext mobiler Arbeit" und „Zutritts- und Zugriffsschutz" festgestellt werden. In allen anderen Kontexten gibt es laut der Pfadkoeffizientenanalyse eine geringe Korrelation zwischen Einstellung und Verhalten. Der Einfluss von Wissen auf Verhalten ist am größten in den Kontexten „E-Mail-Bearbeitung", „Passwortmanagement" und „Zutritts- und Zugriffsschutz". Dies wird auch durch die Ergebnisse der Pfadkoeffizientenanalyse unterstützt. Durch die Mittelwertanalyse können die kausalen Zusammenhänge zwischen Wissen, Einstellung und Verhalten erklärt werden. Dafür wurden die Differenzen zwischen T1 und T0 für beide Gruppen berechnet.

Der Vergleich der Mittelwertresultate kann kausale Zusammenhänge, die durch die Pfadkoeffizientenanalyse und Effektgröße erklärt wurden, nur teilweise unterstüt-

zen. Anhand der Differenzen zwischen T1 und T0 konnte bestätigt werden, dass die Verbesserung im Wissen mit der Verbesserung in der Einstellung und in der Verbesserung in Verhalten generell in allen Kontexten und allen Konstrukten beider Gruppen einhergehen.

An dieser Stelle ist aber auch hervorzuheben, dass im Kontext „Umgang mit Informationen u. a. im Kontext mobiler Arbeit" beide Gruppen trotz eines relativ niedrigeren Zuwachses im Konstrukt „Wissen" einen stärkeren Zuwachs in den Konstrukten „Einstellung" und Verhalten" haben (siehe Tabelle 58). Also konnte hier nicht festgestellt werden, dass die insignifikante Veränderung im Wissen mit insignifikanten Veränderungen in der Einstellung und im Verhalten einhergeht. Im Kontext „Zutritts- und Zugriffsschutz" (Gruppe B) konnte trotz eines relativ starken Zuwachses im Konstrukt „Wissen" kein starker Zuwachs der Einstellung beobachtet werden (siehe Tabelle 59).

Die Kausalität zwischen Wissen, Einstellung und Verhalten kann weiter in den Strukturmodellen der dritten Erhebung T2 definiert werden, da hier analog zu den vorherigen Erhebungszeitpunkten die Effektstärke berechnet wurde. Hier ist der Einfluss von Wissen auf Einstellung im Kontext „Umgang mit (mobilen) Speicher- und Endgeräten" am größten. Diese Aussage wird teilweise durch die Ergebnisse der Pfadkoeffizientenanalyse untermauert, denn eine starke Korrelation konnte nicht nur im Kontext „Umgang mit (mobilen) Speicher- und Endgeräten" identifiziert werden, sondern auch in den Kontexten „E-Mail- Bearbeitung" und „Umgang mit Informationen u. a. im Kontext mobiler Arbeit".

Der Einfluss der Variable „Einstellung" auf die Variable „Verhalten" zum Erhebungszeitpunkt T2 ist ebenfalls im Kontext „Umgang mit (mobilen) Speicher- und Endgeräten" am größten. Diese Ergebnisse entsprechen auch den Ergebnissen der Pfadkoeffizientenanalyse, wobei eine starke Korrelation auch in den Kontexten „Passwortmanagement" und „Zutritts- und Zugriffsschutz" identifiziert werden konnte.

Der Einfluss von Wissen auf Verhalten ist in den Kontexten „E-Mail-Bearbeitung" und „Zutritts- und Zugriffsschutz" am größten. Diese Aussage unterstützen teilweise die Ergebnisse der Pfadkoeffizientenanalyse, weil die Pfadkoeffizienten im Pfad „Wissen auf Verhalten" zum Erhebungszeitpunkt T2 in allen Kontexten stark sind.

In der Mittelwertdifferenzanalyse T2-T1 konnte festgestellt werden, dass ein negativer Zuwachs im Wissen zu einem negativen Zuwachs in der Einstellung und im Verhalten im Kontext „E-Mail-Bearbeitung" (Gruppe A) führt. Ähnliche Ergebnisse konnten im Kontext „Zutritts- und Zugriffsschutz" beobachtet werden. In den Kontexten „Umgang mit Informationen u. a. im Kontext mobiler Arbeit" und „Umgang mit (mobilen) Speicher- und Endgeräten" konnte ein positiver Zuwachs in Wissen, Einstellung und Verhalten beobachtet werden, wobei der stärkste Zuwachs im Kontext „Umgang mit Informationen u. a. im Kontext mobiler Arbeit" auffiel. Dies impliziert, dass Veränderungen im Wissen in diesen Kontexten mit Veränderungen in der Einstellung und im Verhalten einhergehen. Im Kontext „Passwortmanagement" konnte aber trotz eines negativen Zuwachses im Wissen und Verhalten ein positiver Zuwachs in der Einstellung festgestellt werden. Daraus folgt, dass im Kontext „Passwortmanagement"

die Veränderungen im Wissen nicht mit Veränderungen in der Einstellung einhergehen. Allerdings lässt sich ableiten, dass negative Veränderungen im Wissen und negative Veränderungen im Verhalten in diesem Kontext miteinander einhergehen.

Tabelle 59: Mittelwerte der Awareness-Bereiche „Wissen-Einstellung-Verhalten" von T0 bis T4 für die Gruppe B mit den Entwicklungsdifferenzen zwischen den Erhebungsergebnissen

Kontext	Konstrukt	$\bar{x}$ in T0	$\bar{x}$ in T1	Differenz T1-T0	$\bar{x}$ in T2	$\bar{x}$ in T3	$\bar{x}$ in T4
E-Mail-Bearbeitung	Wissen	3,83	4,31	0,48	x	x	4,07
	Einstellung	3,88	4,21	0,33	x	x	4,09
	Verhalten	3,84	4,14	0,3	x	x	3,54
Passwort-management	Wissen	3,87	4,62	0,75	x	x	3,99
	Einstellung	3,76	4,21	0,45	x	x	4,02
	Verhalten	3,58	4,38	0,8	x	x	3,56
Umgang mit Informationen u. a. im Kontext mobiler Arbeit	Wissen	4,3	4,57	0,27	x	x	4,14
	Einstellung	3,59	4,31	0,72	x	x	4,17
	Verhalten	2,99	3,87	0,88	x	x	3,51
Umgang mit (mobilen) Speicher- und Endgeräten	Wissen	3,89	4,12	0,23	x	x	4,24
	Einstellung	4,23	4,48	0,25	x	x	4,34
	Verhalten	3,91	4,28	0,37	x	x	4,15
Zutritts- und Zugriffsschutz	Wissen	3,9	4,21	0,31	x	x	4,19
	Einstellung	4,19	4,25	0,06	x	x	4,13
	Verhalten	4,01	4,29	0,28	x	x	4,17

Die Ergebnisse der vierten Erhebung T3 bescheinigen, dass die Korrelation zwischen Wissen, Einstellung und Verhalten vorhanden ist und dass einzelne Awareness-Bereiche einander beeinflussen. Der Einfluss von Wissen auf Einstellung ist nur im Kontext „Umgang mit (mobilen) Speicher- und Endgeräten" signifikant und in allen weiteren Kontexten moderat bis gering. Laut der Pfadkoeffizientenanalyse ist der Einfluss von der Variable „Wissen" auf die Variable „Einstellung" aber in allen Kontexten stark, bis auf den Kontext „E-Mail- Bearbei-tung".

Der Einfluss von Einstellung auf Verhalten, basierend auf der Effektstärke, ist nur in den Kontexten „Passwortmanagement" und „Zutritts- und Zugriffsschutz" signifikant. Dies konnte nur teilweise von den Ergebnissen der Pfadkoeffizientenanalyse bestätigt werden, da die Pfadkoeffizienten von „Einstellung auf Verhalten" in allen Kontexten stark sind.

Der Einfluss von Wissen auf Verhalten ist nur im Kontext „E-Mail-Bearbeitung" signifikant. Dies wird teilweise durch die Ergebnissen der Pfadkoeffizientenanalyse unterstützt, weil die Pfadekoeffizienten in allen Kontexten stark sind, bis auf den Kontext „Umgang mit (mobilen) Speicher- und Endgeräten".

Die Mittelwertanalyse können die Ergebnisse der Analyse der Pfadkoeffizienten und der Effektstärke im Kontext „E-Mail-Bearbeitung" teilweise unterstützen, denn laut den Resultaten der Mittelwertdifferenz T3-T2 in der Gruppe A konnte ein positiver Zuwachs in Wissen, Einstellung und Verhalten festgestellt werden. Daraus ergibt sich, dass eine positive Veränderung im Wissen zu einer positiven Veränderung in der Einstellung und im Verhalten führt. Ähnliche Resultate liegen in den Kontexten „Umgang mit (mobilen) Speicher- und Endgeräten" und „Zutritts- und Zugriffsschutz" vor. Wobei im Kontext „Zutritts- und Zugriffsschutz" der Zuwachs von Wissen und Einstellung ähnlich gering ist, was auch wiederum darauf hindeutet, dass die Veränderungen im Wissen mit Veränderungen in der Einstellung einhergehen. In den Kontexten „Passwortmanagement" und „Umgang mit Informationen u. a. im Kontext mobiler Arbeit" konnte trotz eines positiven Zuwachses in den Bereichen Wissen und Verhalten ein negativer Zuwachs im Bereich Einstellung festgestellt werden. Dies führt zu der Schlussfolgerung, dass die Veränderungen im Wissen mit Veränderungen im Verhalten einhergehen. Die Einstellung in diesen Kontexten wird hingegen durch andere Faktoren erklärt.

Die Ergebnisse der letzten Erhebung T4 veranschaulichen, dass die Korrelation zwischen einzelnen Awareness-Bereichen vorhanden ist, wobei die Korrelation zwischen Wissen und Einstellung in allen Kontexten bedeutsam ist, bis auf den Kontext „Umgang mit Informationen u. a. im Kontext mobiler Arbeit", wo dieser Einfluss moderat ist. Die Korrelation zwischen Einstellung und Verhalten ist nur im Kontext „Umgang mit (mobilen) Speicher- und Endgeräten" hoch. Der Einfluss von Wissen auf Verhalten ist wiederum nur im Kontext „Umgang mit Informationen u. a. im Kontext mobiler Arbeit" signifikant. Dies wird auch teilweise durch die Ergebnisse der Pfadkoeffizientenanalyse bestätigt. Die Pfadkoeffizienten zwischen Wissen und Einstellung sind in allen Kontexten bedeutsam, genauso wie die Pfadkoeffizienten zwischen Einstellung und Verhalten. Was impliziert, dass es eine starke Korrelation zwischen Wissen und Einstellung und Einstellung und Verhalten gibt. Die Pfadkoeffizienten zwischen Wissen und Verhalten sind ebenfalls in allen Kontexten bedeutsam, bis auf die Kontexte „Passwortmanagement" und „Umgang mit (mobilen) Speicher- und Endgeräten".

Die Ergebnisse der Mittelwertanalyse der Differenzen T4-T3 können gewisse Veränderungen bei den Awareness-Konstrukten nachweisen, die in fast allen Kontexten vorliegen – bis auf den Kontext „E-Mail-Bearbeitung" laut den Ergebnissen der Differenz der Mittelwerte (Gruppe A).

Zusammenfassend konnte belegt werden, dass einzelne Awareness-Bereiche zu verschiedenen Erhebungszeitpunkten in verschiedenen Kontexten miteinander korrelieren und einen Einfluss aufeinander haben. Darüber hinaus kann die Hypothese H2 bestätigt werden.

H2.1 Das Wissen hinsichtlich Informationssicherheitsregeln beeinflusst die Einstellung zu Informationssicherheitsregeln.

Erste Hinweise zur Bestätigung dieser Hypothese können den Ergebnissen der HAIS-Q-Studie (Parson et al., 2014, S. 171 f.) entnommen werden. Die Forscher kommen zu dem Ergebnis, dass besseres Wissen zu 66 % zu einer besseren Einstellung der Teilnehmer zum Thema Informationssicherheit führt (Parson et al., 2014, S. 172).

Wie schon erwähnt, soll die Beurteilung des Gütekriteriums Effektgröße f^2 über die fünf Ergebungszeitpunkte miteinbezogen werden, um den Einfluss der exogenen Variable „Wissen" auf die endogene Variable „Einstellung" zu überprüfen. Zusätzlich werden die Ergebnisse der Pfadkoeffizientenanalyse betrachtet. Denn obwohl sie nicht direkt den Einfluss einer exogenen Variable auf eine endogene Variable aufzeigt, können durch die Pfadkoeffizientenanalyse die Kausalzusammenhänge identifiziert werden (Nitzl, 2010, S. 34 in Anlehnung an Krafft, Götz & Liehr-Gobbers, 2005, S. 83). Darüber hinaus können bei der Betrachtung der Ergebnisse der Pfadkoeffizientenanalyse die Einflüsse und Korrelationen der einzelnen Awareness-Bereiche zusätzlich bestätigt oder widerlegt werden.

Zusätzlich sollen die Differenzen in der Mittelwertanalyse in die finale Diskussion aufgenommen werden, um die Veränderungen in den Awareness-Bereichen tiefgreifender zu diskutieren. Die Mittelwertdifferenzberechnung kann für die T0-Erhebung nicht durchgeführt werden, da ein Vergleich der T0-Ergebnisse erst mit der Erhebung T1 möglich ist. Die Ergebnisse für Gruppe A sind in Tabelle 60 und die für Gruppe B in Tabelle 61 veranschaulicht.

Wie die Ergebnisse der ersten T0-Erhebung aus dem Kapitel 4.5.2.2 zeigen, ist die Effektstärke im Kontext „Zutritts- und Zugriffsschutz" am größten, was bedeutet, dass der Einfluss der Variable „Wissen" auf die Variable „Einstellung" in diesem Kontext entsprechend hoch ist. Die Effektstärke im Kontext „Umgang mit (mobilen) Speicher- und Endgeräten" ist fast genauso hoch wie im Kontext „Passwortmanagement" und fällt moderat aus, was bedeutet, dass der entsprechende Einfluss der Variable „Wissen" auf die Variable „Einstellung" auch moderat ist. In den Kontexten „E-Mail-Bearbeitung" und „Umgang mit Informationen u. a. im Kontext mobiler Arbeit" hat die Effektstärke einen geringen Wert. Das heißt, dass das Wissen in diesen Fällen die Einstellung eher gering beeinflusst. Dies wird auch teilweise durch die Ergebnisse der Pfadkoeffizientenanalyse unterstützt. Es konnte eine geringe Korrelation zwischen Wissen und Einstellung in den Kontexten „E-Mail-Bearbeitung" und „Umgang mit Informationen u. a. im Kontext mobiler Arbeit" nachgewiesen werden. In allen anderen Kontexten ist die Korrelation zwischen Wissen und Einstellung laut der Pfadkoeffizientenanalyse stark. Das bedeutet, dass die Hypothese H2.1 teilweise bestätigt werden kann, da nicht in allen Kontexten ein signifikanter Einfluss von Wissen auf Einstellung zum Zeitpunkt T0 identifiziert wurde.

Die Ergebnisse der zweiten Erhebung T1 aus dem Kapitel 4.5.3.2 zeigen, dass der Einfluss von Wissen auf Einstellung im Kontext „Zutritts- und Zugriffsschutz" am größten ist. In den anderen Kontexten bleibt der Einfluss insignifikant. Die Ergebnisse

der Pfadkoeffizientenanalyse untermauern diese Aussage. Die zweite Erhebung wurde direkt nach der Durchführung der klassischen Unterweisung durchgeführt. Es lässt sich schlussfolgern, dass das Wissen, was sich die Teilnehmer während der Unterweisung angeeignet haben, die Einstellung der Teilnehmer nur gering beeinflusst. Folglich ist die reine Unterweisung eine relativ uneffektive Methode, die Einstellung zum Thema Informationssicherheit zu fördern. Auch an dieser Stelle kann hervorgehoben werden, dass die Hypothese H2.1 teilweise bestätigt werden kann, weil nur in einem Kontext ein signifikanter Einfluss von Wissen auf Einstellung zum Zeitpunkt T1 identifiziert werden konnte.

Die Ergebnisse der Mittelwertanalysedifferenzen zwischen T1 und T0 können bestätigen, dass gewisse Veränderungen in allen Konstrukten vorliegen. Die Mittelwertergebnisse können die Ergebnisse der Pfadkoeffizientenanalyse und der Analyse der Effektstärke teilweise bestätigen. Der größte Zusammenhang findet sich zwischen Veränderungen in Wissen und Einstellung in den Kontexten „Passwortmanagement" (Gruppe A und B), „Umgang mit (mobilen) Speicher- und Endgeräten" (Gruppe A und B) und „E-Mail-Bearbeitung" (Gruppe B).

Tabelle 60: Mittelwerte der Awareness-Bereiche „Wissen-Einstellung" von T0 bis T4 für die Gruppe A mit den Entwicklungsdifferenzen der Erhebungsergebnisse

Kontext	Konstrukt	$\bar{x}$ in T0	$\bar{x}$ in T1	Differenz T1-T0	$\bar{x}$ in T2	Differenz T2-T1	$\bar{x}$ in T3	Differenz T3-T2	$\bar{x}$ in T4	Differenz T4-T3
E-Mail-Bearbeitung	Wissen	3,69	4,41	0,72	4,03	–0,38	4,26	0,23	4,35	0,09
	Einstellung	3,81	4,02	0,21	3,86	–0,16	4,17	0,31	4,02	–0,15
Passwort-management	Wissen	3,87	4,71	0,84	3,87	–0,84	4,09	0,22	4,04	–0,05
	Einstellung	3,65	4,38	0,73	4,66	0,28	4,63	–0,03	4,08	–0,55
Umgang mit Informationen u. a. im Kontext mobiler Arbeit	Wissen	4,28	4,38	0,1	4,61	0,23	4,63	0,02	4,03	–0,6
	Einstellung	3,67	4,23	0,56	4,56	0,33	4,52	–0,04	4,16	–0,36
Umgang mit (mobilen) Speicher- und Endgeräten	Wissen	3,81	4,26	0,45	4,47	0,21	4,62	0,15	4,27	–0,35
	Einstellung	4,02	4,61	0,59	4,63	0,02	4,72	0,09	4,36	–0,36
Zutritts- und Zugriffsschutz	Wissen	3,75	4,21	0,46	4,15	–0,06	4,25	0,1	4,1	–0,15
	Einstellung	4,21	4,41	0,2	4,4	–0,01	4,5	0,1	4,08	–0,42

Tabelle 61: Mittelwerte der Awareness-Bereiche „Wissen-Einstellung" von T0 bis T4 für die Gruppe B mit den Entwicklungsdifferenzen zwischen den Erhebungsergebnissen

Kontext	Konstrukt	x̄ in T0	x̄ in T1	Differenz T1-T0	x̄ in T2	x̄ in T3	x̄ in T4
E-Mail-Bearbeitung	Wissen	3,83	4,31	0,48	x	x	4,07
	Einstellung	3,88	4,21	0,33	x	x	4,09
Passwort-management	Wissen	3,87	4,62	0,75	x	x	3,99
	Einstellung	3,76	4,21	0,45	x	x	4,02
Umgang mit Informationen u. a. im Kontext mobiler Arbeit	Wissen	4,3	4,57	0,27	x	x	4,14
	Einstellung	3,59	4,31	0,72	x	x	4,17
Umgang mit (mobilen) Speicher- und Endgeräten	Wissen	3,89	4,12	0,23	x	x	4,24
	Einstellung	4,23	4,48	0,25	x	x	4,34
Zutritts- und Zugriffsschutz	Wissen	3,9	4,21	0,31	x	x	4,19
	Einstellung	4,19	4,25	0,06	x	x	4,13

Die Ergebnisse der dritten Erhebung T2 verdeutlichen, dass der größte Einfluss der Variable „Wissen" auf die Variable „Einstellung" nur im Kontext „Umgang mit (mobilen) Speicher- und Endgeräten" identifiziert werden kann. Der Einfluss von Wissen auf Einstellung ist im Kontext „Umgang mit Informationen u. a. im Kontext mobiler Arbeit" moderat und in den anderen Kontexten gering. Diese Ergebnisse werden nur teilweise von den Ergebnissen der Pfadkoeffizientenanalyse unterstützt, da die Korrelation zwischen Wissen und Einstellung nicht nur in den oben genannten Kontexten stark ist, sondern auch im Kontext „E-Mail-Bearbeitung". Daher kann die Hypothese H2.1 teilweise bestätigt werden, da der Einfluss von Wissen auf Einstellung zum Zeitpunkt T2 nicht in allen Kontexten stark ist.

Die Ergebnisse der Mittelwertanalysedifferenzen zwischen T2 und T1 belegen, dass gewisse Veränderungen in Wissen und Einstellung in allen Kontexten vorhanden sind, ausgenommen ist nur der Kontext „Passwortmanagement". An dieser Stelle konnte also festgestellt werden, dass negative Veränderungen in der Einstellung nicht mit einem ansteigenden Wissen erklärt werden können; daher steht aufgrund dieser Beobachtung die Annahme eines Kausalzusammenhangs infrage.

Die Erhebung T3 wurde direkt nach der Durchführung der Security Arena durchgeführt. Die Ergebnisse der vierten Erhebung T3 zeigen, dass der Einfluss von Wissen auf Einstellung nur im Kontext „Umgang mit (mobilen) Speicher- und Endgeräten" stark ist. In allen anderen Kontexten ist dieser Einfluss moderat bis gering. Dies wird teilweise durch die Ergebnisse der Pfadkoeffizientenanalyse bestätigt, denn es konnte eine starke Korrelation zwischen allen Kontexten auf dem Pfad Wissen auf Einstellung identifiziert werden, bis auf den Kontext „E-Mail-Bearbeitung". Dies kann zur Schlussfolgerung führen, dass durch das in der Security Arena erworbene Wissen die Einstel-

lung der Teilnehmer mehr beeinflusst werden konnte als z. B. durch die Durchführung von einer klassischen Unterweisung. In der Erhebung T3 konnte teilweise ein Einfluss von Wissen auf Einstellung identifiziert werden, deswegen kann die Hypothese H2.1 teilweise bestätigt werden.

Laut den Ergebnissen der Mittelwertanalysedifferenzen zwischen T3 und T2 kann festgehalten werden, dass Veränderungen im Wissen gewisse Veränderungen in der Einstellung in fast allen Kontexten verursachen, abgesehen von den Kontexten „Passwortmanagement" und „Umgang mit Informationen u. a. im Kontext mobiler Arbeit". Hier sei hervorgehoben, dass in diesen beiden Kontexten eine negative Veränderung in der Einstellung nicht mit ansteigendem Wissen erklärt werden kann; somit steht aufgrund dieser Beobachtung die Annahme eines Kausalzusammenhangs in diesen Kontexten infrage.

Die letzte Erhebung T4 wurde am 21.10.2020 30 Tage nach der Durchführung der Security Arena durchgeführt. Hier legen die Ergebnisse dar, dass in allen Kontexten ein sehr starker Einfluss von Wissen auf Einstellung präsent ist, bis auf den Kontext „Umgang mit Informationen u. a. im Kontext mobiler Arbeit", wo dieser Einfluss moderat ist. Am größten ist der Einfluss von Wissen auf Einstellung in den Kontexten „E-Mail-Bearbeitung" und „Passwortmanagement". Dies wird auch teilweise durch die Ergebnisse der Pfadkoeffizientenanalyse unterstützt, denn es konnte eine starke Korrelation in allen Kontexten festgestellt werden.

Die Mittelwertanalysedifferenzergebnisse zwischen T4 und T3 können in allen Kontexten bestätigen, dass Veränderungen im Wissen mit Veränderungen in der Einstellung einhergehen, bis auf den Kontext „E-Mail-Bearbeitung". Hier kann eine negative Veränderung in der Einstellung nicht mit einer positiven Veränderung im Wissen erklärt werden, weshalb auch die Annahme eines Kausalzusammenhangs infrage gestellt werden soll.

Insgesamt konnte festgestellt werden, dass ein kontinuierlicher Einfluss der Variable „Wissen" auf die Variable „Einstellung" innerhalb aller fünf Erhebungszeitpunkte vorhanden ist, aber nicht in allen Kontexten. Daher konnte die Hypothese H2.1 nur teilweise bestätigt werden.

H2.2 Die Einstellung zu Informationssicherheitsregeln beeinflusst das Verhalten gegenüber der Informationssicherheit.

Die ersten Hinweise zur Bestätigung dieser Hypothese lassen sich in der Forschung finden. So kommen Parson et al. (2014) in der HAIS-Q Studie zu dem Ergebnis, dass die Einstellung das Verhalten zwar beeinflusst, wenn auch nur teilweise. Die Forscher kommen zu dem Schluss, dass ca. 78 % der Abweichungen im Verhalten durch die Einstellung und das Wissen zum Thema Informationssicherheit (Parson et al., 2014, S. 172) determiniert werden.

Des Weiteren wurde die Auswertung des Gütekriteriums der Effektgröße f^2 über die fünf Ergebungszeitpunkte miteinbezogen, um den Einfluss von Einstellung auf

Verhalten zu überprüfen. Gleiches gilt für die Pfadkoeffizientenanalyse, um die Kausalzusammenhänge zu kontrollieren.

Zusätzlich werden noch die Ergebnisse der Mittelwertanalysedifferenzen betrachtet, um die Kausalität zwischen den Awareness-Bereichen Einstellung und Verhalten zu diskutieren. Die Ergebnisse für Gruppe A sind in Tabelle 62, die für Gruppe B in Tabelle 63 veranschaulicht.

Wie die Ergebnisse der ersten Erhebung T0 aus dem Kapitel 4.5.2.2 zeigen, ist der Einfluss der Einstellung auf das Verhalten in jedem Konstrukt vorhanden, jedoch relativ gering. Allerdings konnte ein moderater Einfluss der Variable „Einstellung" auf die Variable „Verhalten" im Kontext „Umgang mit (mobilen) Speicher- und Endgeräten" identifiziert werden. Laut den Ergebnissen der Pfadkoeffizientenanalyse ist die Korrelation zwischen Einstellung und Verhalten stark, bis auf die Kontexte „Passwortmanagement" und „Zutritts- und Zugriffsschutz", wo diese Korrelation gering ist.

Wie die Ergebnisse der zweiten Erhebung T1 aus dem Kapitel 4.5.3.2 belegen, ist der Einfluss von Einstellung auf Verhalten zwar vorhanden, bleibt hier jedoch sehr gering. Dies wird teilweise von den Ergebnissen der Pfadkoeffizientenanalyse unterstützt, da die Pfadkoeffizienten in allen Bereichen relativ niedrig sind, was impliziert, dass es eine geringe Korrelation zwischen Einstellung und Verhalten gibt, bis auf die Kontexte „Umgang mit Informationen u. a. im Kontext mobiler Arbeit" und „Zutritts- und Zugriffsschutz". Daher ist auch die Korrelation zwischen Einstellung und Verhalten in diesen beiden Kontexten am stärksten. Diese Aussage wird auch von den Ergebnissen der Analyse der Effektstärken untermauert, denn der größte Einfluss auf dem Pfad „Einstellung ↔ Verhalten" kann in den Kontexten „Umgang mit Informationen u. a. im Kontext mobiler Arbeit" und „Zutritts- und Zugriffsschutz" identifiziert werden. Die Erhebung T1 wurde direkt nach der Durchführung der Unterweisung durchgeführt. Laut den Ergebnissen bleibt der Einfluss der Variable „Einstellung" auf die Variable „Verhalten" generell gering. Folglich kann die Schlussfolgerung gezogen werden, dass die Unterweisung das Verhalten durch die Beeinflussung der Einstellung nur bedingt fördert.

Tabelle 62: Mittelwerte der Awareness-Bereiche „Einstellung-Verhalten" von T0 bis T4 für die Gruppe A mit den Entwicklungsdifferenzen der Erhebungsergebnisse

Kontext	Konstrukt	$\bar{x}$ in T0	$\bar{x}$ in T1	Differenz T1-T0	$\bar{x}$ in T2	Differenz T2-T1	$\bar{x}$ in T3	Differenz T3-T2	$\bar{x}$ in T4	Differenz T4-T3
E-Mail-Bearbeitung	Einstellung	3,81	4,02	0,21	3,86	–0,16	4,17	0,31	4,02	–0,15
	Verhalten	3,45	4,31	0,86	3,96	–0,35	4,18	0,22	3,88	–0,3
Passwort-management	Einstellung	3,65	4,38	0,73	4,66	0,28	4,63	–0,03	4,08	–0,55
	Verhalten	3,57	4,32	0,75	3,82	–0,5	3,84	0,02	3,71	–0,13
Umgang mit Informationen u. a. im Kontext mobiler Arbeit	Einstellung	3,67	4,23	0,56	4,56	0,33	4,52	–0,04	4,16	–0,36
	Verhalten	3,34	3,72	0,38	4,16	0,44	4,66	0,5	4,43	–0,23

(Fortsetzung Tabelle 62)

Kontext	Konstrukt	x̄ in T0	x̄ in T1	Differenz T1-T0	x̄ in T2	Differenz T2-T1	x̄ in T3	Differenz T3-T2	x̄ in T4	Differenz T4-T3
Umgang mit (mobilen) Speicher- und Endgeräten	Einstellung	4,02	4,61	0,59	4,63	0,02	4,72	0,09	4,36	–0,36
	Verhalten	3,94	4,54	0,6	4,55	0,01	4,7	0,15	4,25	–0,45
Zutritts- und Zugriffsschutz	Einstellung	4,21	4,41	0,2	4,4	–0,01	4,5	0,1	4,08	–0,42
	Verhalten	3,83	4,42	0,59	4,21	–0,21	4,37	0,41	4,30	–0,07

Die Ergebnisse der Mittelwertdifferenzen zwischen T1 und T0 beider Gruppen können nachweisen, dass die Veränderung in Einstellung mit Veränderungen im Verhalten in allen Kontexten einhergehen (siehe Tabelle 62 und 63).

Die nächste Erhebung T2 wurde 6 Wochen nach der Erhebung T1 am 21.09.2020 durchgeführt. Wie die Ergebnisse aus dem Kapitel 4.5.4.2 zeigen, wurde sowohl die Korrelation zwischen Einstellung und Verhalten als auch ein gewisser Einfluss von Einstellung auf Verhalten erkenntlich. Den Ergebnissen der Pfadkoeffizientenanalyse zufolge korrelieren Einstellung und Verhalten stark in allen Kontexten, bis auf die Kontexte „E-Mail-Bearbeitung" und „Umgang mit Informationen u. a. im Kontext mobiler Arbeit", wo die Korrelation auf einem niedrigen Niveau ist. Die Ergebnisse der Effektstärkeanalyse bestätigen, dass der Einfluss von Einstellung auf Verhalten im Kontext „Umgang mit (mobilen) Speicher- und Endgeräten" hoch ist, während dieser Einfluss in allen anderen Kontexten moderat bis gering ausfällt.

Tabelle 63: Mittelwerte der Awareness-Bereiche „Einstellung-Verhalten" von T0 bis T4 für die Gruppe B mit den Entwicklungsdifferenzen der Erhebungsergebnisse

Kontext	Konstrukt	x̄ in T0	x̄ in T1	Differenz T1-T0	x̄ in T2	x̄ in T3	x̄ in T4
E-Mail-Bearbeitung	Einstellung	3,88	4,21	0,33	x	x	4,09
	Verhalten	3,84	4,14	0,3	x	x	3,54
Passwortmanagement	Einstellung	3,76	4,21	0,45	x	x	4,02
	Verhalten	3,58	4,38	0,8	x	x	3,56
Umgang mit Informationen u. a. im Kontext mobiler Arbeit	Einstellung	3,59	4,31	0,72	x	x	4,17
	Verhalten	2,99	3,87	0,88	x	x	3,51
Umgang mit (mobilen) Speicher- und Endgeräten	Einstellung	4,23	4,48	0,25	x	x	4,34
	Verhalten	3,91	4,28	0,37	x	x	4,15
Zutritts- und Zugriffsschutz	Einstellung	4,19	4,25	0,06	x	x	4,13
	Verhalten	4,01	4,29	0,28	x	x	4,17

Die Ergebnisse der Mittelwertdifferenzanalyse zwischen T2 und T1 beweisen Veränderungen in Einstellung und Verhalten in allen Kontexten bis auf „Passwortmanagement". Hier konnte also festgestellt werden, dass es trotz eines positiven Zuwachses in der Einstellung einen negativen Zuwachs im Verhalten gibt. Somit steht durch diese Beobachtung die Annahme eines Kausalzusammenhangs zwischen Einstellung und Verhalten im Kontext „Passwortmanagement" zu diesen Erhebungszeitpunkten infrage.

Die T3-Erhebung wurde direkt nach der Veranstaltung „Security Arena" durchgeführt. Deren Ergebnisse veranschaulichen, dass sowohl die Korrelation zwischen den Variablen „Einstellung" und „Verhalten" als auch der Einfluss der Variable „Einstellung" auf die Variable „Verhalten" stärker wird. Die Pfadkoeffizientenanalyse zeigt, dass die Variablen „Einstellung" und „Verhalten" in den Kontexten „Passwortmanagement" und „Zutritts- und Zugriffsschutz" am stärksten korrelieren, wobei eine starke Korrelation in allen Kontexten identifiziert werden konnte. Die Effektstärke bestätigt, dass der Einfluss von Einstellung auf Verhalten in den Kontexten „Passwortmanagement" und „Zutritts- und Zugriffsschutz" am höchsten ist. In anderen Kontexten ist der Einfluss moderat. Ab Erhebung T2 und nach der Erhebung T3 konnte eine kontinuierliche Verstärkung der Korrelation zwischen Einstellung und Verhalten und des Einflusses von Einstellung auf Verhalten beobachtet werden. Dies erlaubt die Schlussfolgerung, dass die Durchführung der Security Arena eine positive Beeinflussung des Verhaltes durch die Beeinflussung der Einstellung fördert. Darüber hinaus wurde deutlich, dass die Einstellungsänderung der Teilnehmer und die kausale Verhaltensänderung einige Zeit in Anspruch nehmen. Dieser Sachverhalt kann durch die Mittelwertanalyse bestätigt werden, da die Mittelwerte der T3-Analyse größer sind als z. B. die Mittelwerte der T1-Analyse. Letztlich lässt sich daraus ableiten, dass mit der Zeit eine bessere Korrelation von Einstellung und Verhalten und eine kontinuierliche Sensibilisierung gefördert werden können.

Laut den Ergebnissen der Mittelwertdifferenzen zwischen T3 und T2 können in allen Kontexten Veränderungen in der Einstellung und Veränderungen im Verhalten festgestellt werden, ausgenommen sind die Kontexte „Passwortmanagement" und „Umgang mit Informationen u. a. im Kontext mobiler Arbeit" (siehe Tabelle 62). Hier konnte trotz einer negativen Veränderung in der Einstellung eine positive Veränderung im Verhalten beobachtet werden, also steht durch diese Beobachtung die Annahme eines Kausalzusammenhangs in den Kontexten „Passwortmanagement" und „Umgang mit Informationen u. a. im Kontext mobiler Arbeit" infrage.

Die letzte Erhebung T4 wurde knapp 4 Wochen nach der Erhebung T3 durchgeführt. Deren Ergebnisse veranschaulichen, dass zum einen die Einstellung und das Verhalten korrelieren und dass zum anderen die Einstellung das Verhalten beeinflusst. Eine sehr starke Korrelation von Einstellung und Verhalten kann laut Pfadkoeffizientenanalyse im Kontext „Umgang mit (mobilen) Speicher- und Endgeräten" beobachtet werden, wobei die Korrelation in allen Kontexten stark ist. Die Ergebnisse der Effektgröße demonstrieren, dass der Einfluss der Variable „Einstellung" auf die Varia-

ble „Verhalten“ im Kontext „Umgang mit (mobilen) Speicher- und Endgeräten“ am größten ist, während er in den anderen Kontexten eher gering ausfällt.

Laut den Ergebnissen der Mittelwertdifferenzen zwischen T4 und T3 kann in allen Kontexten nachgewiesen werden, dass die Veränderungen in der Einstellung mit Veränderungen im Verhalten einhergehen.

Zusammenfassend konnte festgestellt werden, dass ein kontinuierlicher Einfluss der Variable „Einstellung“ auf die Variable „Verhalten“ innerhalb von allen fünf Erhebungszeitpunkten vorhanden ist, allerdings nicht bei allen Kontexten durchgehend. Somit kann die Hypothese H2.2 teilweise bestätigt werden.

H2.3 Das Wissen hinsichtlich Informationssicherheitsregeln beeinflusst das Verhalten gegenüber der Informationssicherheit.

Die ersten Hinweise zur Bestätigung dieser Hypothese gab es in den Ergebnissen der HAIS-Q-Studie, wo Parsons et al. (2014, S. 172) zu dem Schluss gekommen sind, dass das Wissen über Informationssicherheit das Verhalten gegenüber Informationssicherheit im gewissen Grad beeinflusst.

Zur Überprüfung dieser Hypothese wurden ebenfalls wieder die Auswertung des Gütekriteriums der Effektgröße f^2 über die fünf Ergebungszeitpunkte sowie die Pfadkoeffizientenanalyse miteinbezogen.

Um die Kausalität zwischen den Awareness-Bereichen Wissen und Verhalten zu eruieren, werden zusätzlich wieder die Mittelwertdifferenzen betrachtet (zwischen T1 und T0, T2 und T1, T3 und T2 sowie T4 und T3). Daraus lässt sich ableiten, inwiefern die Steigerung oder Reduktion des Wissens zu einer Steigerung oder Reduktion im Verhalten führt. Die Ergebnisse für Gruppe A sind in Tabelle 64, die für Gruppe B in Tabelle 65 abgebildet.

Die Ergebnisse der ersten Erhebung T0 legen dar, dass der Einfluss von Wissen auf Verhalten in der Mehrzahl der Kontexte gering ist, bis auf den Kontext „Umgang mit (mobilen) Speicher- und Endgeräten“, wo der entsprechende Einfluss moderat ist. Die Korrelation zwischen den Variablen „Wissen“ und „Verhalten“ laut Pfadkoeffizientenanalyse ist in den Kontexten „Umgang mit Informationen u. a. im Kontext mobiler Arbeit“, „Umgang mit (mobilen) Speicher- und Endgeräten“ und „Zutritt und Zugriffschutz“ stark und in anderen Kontexten gering.

Die zweite Erhebung T1 wurde direkt nach der Durchführung der Unterweisung veranstaltet, und wie die Ergebnisse zeigen, ist der Einfluss von Wissen auf Verhalten in den Kontexten „E-Mail-Bearbeitung“, „Passwortmanagement“ und „Zutritts- und Zugriffsschutz“ groß, in den anderen Kontexten hingegen gering. Die Ergebnisse der Pfadkoeffizientenanalyse zeigen auch, dass die Korrelation zwischen Wissen und Verhalten in den gleichen Kontexten am stärksten ausgeprägt ist, wobei diese auch im Kontext „Umgang mit (mobilen) Speicher- und Endgeräten“ stark ist. Dadurch, dass die Erhebung T1 direkt nach der Durchführung der Unterweisung stattgefunden hat, lässt sich schlussfolgern, dass die Unterweisung besonders positive Effekte auf die Korrelations- und Einflussförderung von Wissen auf Verhalten in den Kontexten „E-Mail-

Bearbeitung“, „Passwortmanagement“, „Zutritts- und Zugriffsschutz“ und „Umgang mit (mobilen) Speicher- und Endgeräten“ hat.

Tabelle 64: Mittelwerte der Awareness-Bereiche „Wissen-Verhalten“ von T0 bis T4 für die Gruppe A mit den Entwicklungsdifferenzen der Erhebungsergebnisse

Kontext	Konstrukt	$\bar{x}$ in T0	$\bar{x}$ in T1	Differenz T1-T0	$\bar{x}$ in T2	Differenz T2-T1	$\bar{x}$ in T3	Differenz T3-T2	$\bar{x}$ in T4	Differenz T4-T3
E-Mail-Bearbeitung	Wissen	3,69	4,41	0,72	4,03	–0,38	4,26	0,23	4,35	0,09
	Verhalten	3,45	4,31	0,86	3,96	–0,35	4,18	0,22	3,88	–0,3
Passwort-management	Wissen	3,87	4,71	0,84	3,87	–0,84	4,09	0,22	4,04	–0,05
	Verhalten	3,57	4,32	0,75	3,82	–0,5	3,84	0,02	3,71	–0,13
Umgang mit Informationen u. a. im Kontext mobiler Arbeit	Wissen	4,28	4,38	0,1	4,61	0,23	4,63	0,02	4,03	–0,6
	Verhalten	3,34	3,72	0,38	4,16	0,44	4,66	0,5	4,43	–0,23
Umgang mit (mobilen) Speicher- und Endgeräten	Wissen	3,81	4,26	0,45	4,47	0,21	4,62	0,15	4,27	–0,35
	Verhalten	3,94	4,54	0,6	4,55	0,01	4,7	0,15	4,25	–0,45
Zutritts- und Zugriffsschutz	Wissen	3,75	4,21	0,46	4,15	–0,06	4,25	0,1	4,1	–0,15
	Verhalten	3,83	4,42	0,59	4,21	–0,21	4,37	0,41	4,30	–0,07

Den Mitteldifferenzwerten zufolge konnte in allen Kontexten zwischen T1 und T0 festgestellt werden, dass die Veränderungen im Wissen mit Veränderungen im Verhalten einhergehen.

Die Erhebung T2 wurde am 21.09.2020 durchgeführt. Wie die Ergebnisse belegen, konnte ein starker Einfluss von Wissen auf Verhalten in den Kontexten „E-Mail-Bearbeitung“ und „Zutritts- und Zugriffsschutz“ identifiziert werden. Im Kontext „Passwortmanagement“ ist dieser Einfluss moderat. In den anderen Kontexten bleibt der Einfluss der Variable „Wissen“ auf die Variable „Verhalten“ gering. Die Ergebnisse der Pfadkoeffizienten verdeutlichen, dass die Korrelation zwischen Wissen und Verhalten überall stark ist, allerdings in den Kontexten „E-Mail-Bearbeitung“ und „Zutritts- und Zugriffsschutz“ am stärksten.

Laut den Ergebnissen der Mittelwertanalyse der Differenzgrößen zwischen T2 und T1 konnte festgestellt werden, dass die Veränderungen im Wissen mit Veränderungen im Verhalten einhergehen, wobei die größte Veränderung im Kontext „E-Mail-Bearbeitung“ nachgewiesen werden konnte. In den anderen Kontexten ist die Differenz zwischen den Differenzgrößen bezüglich Wissen und Verhalten über 0,15. Dies konnte die Ergebnisse der Pfadkoeffizienten und Effektgröße teilweise bestätigen.

Tabelle 65: Mittelwerte der Awareness-Bereiche „Wissen-Verhalten“ von T0 bis T4 für die Gruppe B mit den Entwicklungsdifferenzen der Erhebungsergebnisse

Kontext	Konstrukt	x̄ in T0	x̄ in T1	Differenz T1-T0	x̄ in T2	x̄ in T3	x̄ in T4
E-Mail-Bearbeitung	Wissen	3,83	4,31	0,48	x	x	4,07
	Verhalten	3,84	4,14	0,3	x	x	3,54
Passwort-management	Wissen	3,87	4,62	0,75	x	x	3,99
	Verhalten	3,58	4,38	0,8	x	x	3,56
Umgang mit Informationen u. a. im Kontext mobiler Arbeit	Wissen	4,3	4,57	0,27	x	x	4,14
	Verhalten	2,99	3,87	0,88	x	x	3,51
Umgang mit (mobilen) Speicher- und Endgeräten	Wissen	3,89	4,12	0,23	x	x	4,24
	Verhalten	3,91	4,28	0,37	x	x	4,15
Zutritts- und Zugriffsschutz	Wissen	3,9	4,21	0,31	x	x	4,19
	Verhalten	4,01	4,29	0,28	x	x	4,17

Die Erhebung T3 wurde direkt nach der Security Arena durchgeführt. Die Ergebnisse der Analyse der Effektstärke zeigen, dass der Einfluss von Wissen auf Verhalten in allen Kontexten vorhanden ist, im Kontext „E-Mail-Bearbeitung“ jedoch am stärksten. Im Kontext „Passwortmanagement“ ist dieser Einfluss moderat. In den anderen Kontexten ist der Einfluss von Wissen auf Verhalten gering. Die Ergebnisse der Pfadkoeffizientenanalyse bestätigen, dass die stärkste Korrelation zwischen Wissen und Verhalten im Kontext „E-Mail-Bearbeitung“ vorliegt, wobei laut Pfadkoeffizientenanalyse die Korrelation zwischen Wissen und Verhalten in allen Kontexten stark ist, bis auf den Kontext „Umgang mit (mobilen) Speicher- und Endgeräten“. Dadurch, dass die Erhebung T3 direkt nach der Durchführung der Security Arena stattgefunden hat, lässt sich schlussfolgern, dass die Security Arena besonders positive Effekte auf die Korrelations- und Einflussförderung von Wissen auf Verhalten im Kontext „E-Mail-Bearbeitung“ hat.

Die Ergebnisse der Mittelwertanalyse der Differenzgrößen zwischen T3 und T2 können bestätigen, dass es Veränderungen im Wissen und Verhalten in allen Kontexten gibt. Die größte einhergehende Veränderung in den beiden Konstrukten konnte in den Kontexten „E-Mail-Bearbeitung“ und „Umgang mit (mobilen) Speicher- und Endgeräten“ festgestellt werden. In allen anderen Kontexten ist die Differenz zwischen den Differenzgrößen von Wissen und Verhalten > 0,20. Dies konnte die Ergebnisse der Pfadkoeffizienten und Effektgröße für den Kontext „E-Mail-Bearbeitung“ bestätigen.

Die letzte Erhebung T4 wurde am 21.10.2020 durchgeführt. Deren Ergebnisse zeigen, dass die Variable „Wissen“ einen geringen Einfluss auf die Variable „Verhalten“ hat, abgesehen vom Kontext „Umgang mit Informationen u. a. im Kontext mobiler Arbeit“, wo der Einfluss stark ausfällt. Die Ergebnisse der Pfadkoeffizientenanalyse bestä-

tigen die stärkste Korrelation auf dem Pfad „Wissen ↔ Verhalten“ im Kontext „Umgang mit Informationen u. a. im Kontext mobiler Arbeit“, wobei eine starke Korrelation in allen Kontexten bestätigt werden konnte, bis auf die Kontexte „Umgang mit (mobilen) Speicher- und Endgeräten“ und „Passwortmanagement“, wo diese Korrelation gering ist. Dass die Effekt- und Korrelationsstärke der Erhebungsergebnisse für T4 in fast allen Kontexten gesunken ist, im Vergleich zu den Ergebnissen der Erhebung T3, lässt den Schluss zu, dass das durch die Security Arena gesteigerte Wissen maximal als kurzfristige Förderung des Verhaltens dienen kann.

Die Ergebnisse der Mittelwertanalyse der Differenzgrößen zwischen T3 und T4 können die Veränderungen im Wissen und im Verhalten in allen Kontexten, bis auf den Kontext „E-Mail-Bearbeitung“, bestätigen. Im Kontext „E-Mail-Bearbeitung“ sollte die Vermutung einer kausalen Beziehung zwischen Wissen und Verhalten infrage gestellt werden.

Generell kann die Hypothese H2.3 teilweise bestätigt werden, da ein kontinuierlicher Einfluss der Variable „Wissen“ auf die Variable „Verhalten“ innerhalb von allen fünf Erhebungszeitpunkten vorhanden ist, jedoch nicht in allen Kontexten.

H3 Die Informationssicherheits-Awareness der jungen Erwachsenen der Volkswagen AG verbessert sich nach der Durchführung der spielerischen Awareness-Maßnahmen zusätzlich zu einer klassischen Unterweisung in einzelnen Kontexten stärker als in anderen Kontexten (E-Mail-Bearbeitung, Passwortmanagement, Umgang mit (mobilen) Speicher- und Endgeräten, Umgang mit Informationen u. a. im Kontext mobiler Arbeit, Zutritts- und Zugriffsschutz) im Vergleich zu einer ausschließlich erfolgten Unterweisung.

Diese Arbeitshypothese besagt, dass sich die Informationssicherheits-Awareness der Probanden dieser Studie nach der Durchführung der Unterweisung mit zusätzlicher spielerischer Awareness-Maßnahme im Vergleich zu einer ausschließlich erfolgten Unterweisung in den einzelnen Kontexten unterschiedlich stark entwickelt. In dieser Arbeitshypothese wird die Informationssicherheits-Awareness als eine Kombination von Wissen, Einstellung und Verhalten interpretiert (Kapitel 2.1). In der Forschung herrscht aktuell keine eindeutige Meinung vor, dass spielerische Maßnahmen die Informationssicherheits-Awareness in bestimmten Kontexten besser als eine klassische Unterweisung fördern (siehe Kapitel 2.3).

Um die Hypothese H3 zu überprüfen und zu analysieren, ob die Informationssicherheits-Awareness der jungen Erwachsenen der Volkswagen AG sich nach der Durchführung der spielerischen Awareness-Veranstaltung zusätzlich zur klassischen Unterweisung im Zeitverlauf in einzelnen Kontexten verbessert, wurden die Mittelwerte von T0 und T4 der Gruppen A und B für jeden einzelnen Kontext berechnet und miteinander verglichen. Wie sich aus der Tabelle 51 ableiten lässt, fördert die Unterweisung mit zusätzlicher Security Arena die Awareness der jungen Erwachsenen der Volkswagen AG in allen Kontexten besser als nur die Unterweisung. Allerdings ist die Differenz zwischen den Awareness-Werten der Gruppe A und der Gruppe B im Kontext „E-Mail-Bearbeitung“ am größten. Besonders in diesem Kontext ist die Sensibili-

sierung mit Unterweisung und einer zusätzlichen Security Arena also deutlich effektiver als die Sensibilisierung mit einer reinen Unterweisung. Bei den anderen Kontexten ist diese Differenz fast identisch, jedoch fallen die Ergebnisse der Gruppe A pro Kontext deutlich höher aus als die Ergebnisse der Gruppe B. Folglich kann die Hypothese H3 bestätigt werden.

In Anbetracht der Ergebnisse der quantitativen Studie lassen sich die Forschungsfragen 2 und 3 wie folgt beantworten:

Forschungsfrage 2: Wie kann Informationssicherheits-Awareness gemessen werden?

Diese Forschungsfrage enthält die Zielsetzung, eine Messung der Informationssicherheits-Awareness zu entwickeln und durchzuführen. Zudem sollen die Möglichkeiten, diese zu beeinflussen und zu steigern, eruiert werden.

Wie bereits zu Beginn dieser Arbeit beschrieben wurde (siehe Kapitel 2.1), beinhaltet der Begriff „Awareness" drei Ebenen: Wissen, Einstellung und Verhalten. Die Untersuchung in dieser Arbeit fokussiert sich auf die Änderungen dieser drei Aspekte.

Hierfür wurden anhand einer Literaturrecherche und der Ergebnisse der Experteninterviews fünf Kontexte aus dem Bereich Informationssicherheits-Awareness entwickelt: E-Mail-Bearbeitung, Passwortmanagement, Umgang mit (mobilen) Speicher- und Endgeräten, Umgang mit Informationen u. a. im Kontext mobiler Arbeit und Zutritts- und Zugriffsschutz. Diese Kontexte beinhalten eine große Bandbreite aktueller Informationssicherheitsthemen, die für Beschäftigte im Rahmen ihrer Tätigkeitsausübung – sowohl während ihres Präsenzjobs als auch außerhalb des Unternehmens im Rahmen von z. B. mobiler Arbeit – relevant sind. Mit ihnen lässt sich ein breites Spektrum von Sicherheitsaspekten und -risiken abdecken, die Auskunft über den Stand der Sicherheits-Awareness der untersuchten Zielgruppe geben.

Die Informationssicherheits-Awareness, genauer gesagt die Veränderungen und Korrelationen auf den drei Ebenen Wissen, Einstellung und Verhalten, wurde analog zur HAIS-Q-Studie innerhalb der fünf Kontexte durch eine quantitative Fragebogenerhebung analysiert. Unter dem Begriff „Wissen" wurde diesbezüglich das Wissen um die in der Volkswagen AG etablierten Regeln zum Thema „Informationssicherheits-Awareness" im Rahmen der ausgewählten fünf Kontexte verstanden. Die „Einstellung" wurde als ein Empfinden gegenüber gewissen Thematiken der Informationssicherheits-Awareness und deren Einschätzungen definiert. Das Verhalten der Probanden wiederum sollte über mehrere theoretische Situationen erhoben werden, bei denen die Probanden im Fragebogen beantworten sollten, wie sie darauf reagieren. Die Ergebnisse einer ersten Befragung liefern einen generellen Überblick über das Informationssicherheitsniveau der Beschäftigten. Mithilfe der Befragung zu unterschiedlichen Zeitpunkten (vor und nach den jeweils durchgeführten Sicherheits-Awareness-Maßnahmen) lässt sich nachzeichnen, wie sich dieses Informationssicherheitsniveau verändert. Der Vergleich zweier Gruppen, die in unterschiedlicher Form für informationssicherheitsrelevante Themen sensibilisiert wurden (hier Unterweisung mit zusätzlicher Security Arena vs. reine Unterweisung) zeigt auf, welche Art der Sensibilisierung besser

geeignet und langfristig effektiver ist. Die Informationssicherheitserhebung kann folglich eingesetzt werden, um Schwachstellen in der Informationssicherheits-Awareness der Beschäftigten zu identifizieren und eine weitere Sensibilisierung gezielter zu gestalten. Darüber hinaus eignet sich das in dieser Arbeit entwickelte Befragungsinstrument als Basis zur Untersuchungen weiterer Zielgruppen und weiterführender Messungen von Informationssicherheit.

Nichtsdestotrotz bestehen natürlich auch Limitationen bei diesem Vorgehen. So ist beispielsweise die Überprüfung menschlichen Verhaltens anhand eines Fragebogens nur beschränkt möglich. Auch dass den Befragten konkrete Situationen nur innerhalb der beschriebenen fünf Informationssicherheitskontexte zur Verfügung gestellt wurden, ist einschränkend zu erwähnen. Generell ist zu hinterfragen, ob noch weitere Informationssicherheitskontexte außerhalb der Automobilindustrie existieren und inwiefern Awareness hier gemessen werden könnte.

Wie in dieser Arbeit teilweise bestätigt wurde, korrelieren die Aspekte Wissen, Einstellung und Verhalten miteinander und stehen teils in einem kausalen Zusammenhang. Folglich sollten in weiteren Studien auch alle Aspekte bei der Messung von Informationssicherheits-Awareness berücksichtigt werden. Zudem sollten in künftigen Studien statt Fragebogenerhebungen z. B. auch Simulationen oder Cyber-Security-Experimente zum Einsatz kommen, um das Verhalten basierend auf den Handlungen der Teilnehmenden zu messen.

Die Messung der Informationssicherheits-Awareness anhand des Modells Wissen-Einstellung-Verhalten inkludiert außerdem keine weiteren Aspekte, wie z. B. subjektive Normen von Personen zum Thema, die vermuteten Erwartungen, die für die handelnde Person wichtige Bezugspersonen bezüglich des Verhaltens haben (vgl. Graf, 2007 in Anlehnung an Ajzen, 1985, 2005, 2006; Ajzen & Madden, 1986), oder wie Verhaltensentscheidungen getroffen werden (vgl. Rauch, 2009 in Anlehnung an Endsley, 1995). Diese und weitere Aspekte sollten in zukünftigen Studien in Verbindung mit Wissen, Einstellung und Verhalten untersucht werden, um ein möglichst umfängliches Bild der Informationssicherheits-Awareness zu erhalten.

Weitere Limitationen dieser Studie werden ausführlich im nachfolgenden Kapitel erörtert.

Forschungsfrage 3: Wie effektiv und nachhaltig für die Förderung von Awareness-Aspekten (Wissen, Einstellung und Verhalten) ist das Konzept „Serious Games" und inwiefern korrelieren die einzelnen Awareness-Aspekte (Wissen, Einstellung und Verhalten) miteinander?

Um den ersten Teil dieser Forschungsfrage zu beantworten, wurden die in den vorherigen Kapiteln präsentierten Hypothesen entwickelt und überprüft. Um die Effektivität der Förderung der Informationssicherheits-Awareness durch Serious Games (Security Arena) zu überprüfen, wurden die Erhebungen zu fünf verschiedenen Zeitpunkten durchgeführt.

Basierend auf den Ergebnissen der Erhebungen kann schlussfolgernd bestätigt werden, dass sich das Wissen der jungen Erwachsenen direkt nach der Durchführung der jeweiligen Awareness-Maßnahme deutlich in allen Kontexten verbessert. Wie ein genereller Vergleich zwischen den Erhebungszeitpunkten T0 und T4 zeigt, sind die beiden Awareness-Maßnahmen allgemein im Zeitverlauf relativ nachhaltig. Wie anhand der Ergebnisse aus Tabelle 51 ersichtlich, fördert die Security Arena mit einer zusätzlichen Unterweisung die Awareness besser als nur eine Unterweisung. Daher kann die Schlussfolgerung gezogen werden, dass Serious Games (in diesem Fall die Security Arena) effektiv für die Förderung von Informationssicherheits-Awareness-Aspekten sind, zusammen mit anderen Awareness-Methoden wie z. B. der Unterweisung. Allerdings stößt die Messung der Effektivität des Serious-Game-Konzeptes in dieser Studie an ihre Grenzen, daher werden im nachfolgenden Kapitel die Limitationen der Studie eruiert.

Die finalen Ergebnisse der Studie zeigen insgesamt, dass sich die Kombination der beiden Awareness-Methoden für die Förderung der allgemeinen Informationssicherheits-Awareness als nachhaltiger erweist als nur eine Unterweisung, da die Ergebnisse der Probanden hinsichtlich der Informationssicherheits-Awareness im Zeitverlauf in Gruppe A deutlich höher ausfallen als die in Gruppe B.

Aus den Ergebnissen der Erhebungen wird auch ersichtlich, dass einzelne Awareness-Bereiche (Wissen, Einstellung und Verhalten) miteinander korrelieren und einen Einfluss aufeinander haben, jedoch nur bedingt. Es konnte festgestellt werden, dass in fast allen Kontexten das Wissen die Einstellung und das Verhalten beeinflusst und die Variable „Wissen“ mit den Variablen „Einstellung“ und „Verhalten“ stark korreliert. Bedeutsam ist, dass die größte Korrelation zwischen den Variablen „Wissen“ und „Einstellung“ und der größte Einfluss von Wissen auf Einstellung in der Erhebung T4 identifiziert wurde. Diese Erhebung wurde erst Wochen nach der letzten Sensibilisierung durchgeführt. Daraus lässt sich schließen, dass die Teilnehmenden nach zwei Awareness-Maßnahmen ein bestimmtes Sensibilisierungsniveau erreicht haben und darüber hinaus bei ihnen eine hohe Korrelation und ein relativ starker Einfluss zwischen Wissen und Einstellung vorhanden sind. Allerdings wurde auch festgestellt, dass die Variable „Einstellung“ zu fast allen Erhebungszeitpunkten einen relativ geringen Einfluss auf die Variable „Verhalten“ hat. Um Veränderungen im Verhalten hervorzurufen, sollte daher erst das Wissen hinsichtlich der untersuchten Thematik gesteigert werden. Eine direkte Korrelation zwischen Wissen und Verhalten und ein direkter Einfluss von Wissen auf Verhalten sind laut den Ergebnissen in den verschiedenen Informationssicherheits-Awareness-Kontexten auch nicht konstant geblieben. Den Ergebnissen von Hypothese 3 zufolge beeinflussen die Awareness-Maßnahmen nicht nur das Wissen, die Einstellung und das Verhalten der Teilnehmenden, sondern haben ebenso unterschiedliche Effekte auf die Awareness-Kontexte. Folglich sollten verschiedene Informationssicherheits-Awareness-Methoden eingesetzt werden, um die Informationssicherheits-Awareness der Probanden in verschiedenen Kontexten passend und adäquat zu fördern.

Wie die Ergebnisse der Studie gezeigt haben, sollte der Fokus künftiger Awareness-Maßnahmen auf der Vermittlung von Wissen liegen, um das Verhalten positiv zu beeinflussen und sicherheitskonformer zu machen, denn wie das Awareness-Messmodell bestätigt hat, beeinflusst die Wissensförderung das Verhalten entweder direkt oder durch die Einstellung. Insgesamt lässt sich festhalten, dass die Durchführung der Unterweisung mit zusätzlicher Security Arena in regelmäßigen Abständen durchgeführt werden sollte, um langfristig Informationssicherheits-Awareness herzustellen, da beide Awareness-Maßnahmen allein nur einen relativ kurzfristigen Effekt haben.

4.6.2 Theoretische und methodische Ergebnisse, Limitationen und zukünftiges Forschungspotenzial

In diesem Kapitel werden sowohl die theoretischen als auch die methodischen Ergebnisse präsentiert und diskutiert. Außerdem werden die Limitationen dieser Studie und zukünftige Forschungspotenziale eruiert.

In dieser Studie wurden die Korrelationen zwischen den Aspekten des in der Forschung bestehenden Awareness-Modells überprüft. Die in bisheriger Literatur bestehenden Ergebnisse über die Korrelation zwischen Wissen, Einstellung und Verhalten, als die Bestandsteile des Awareness-Modells, konnten teilweise bestätigt werden. Allerdings sollte in ergänzender Forschung untersucht werden, inwiefern und zu welchem Maß das Wissen die Einstellung und das Verhalten beeinflusst und welchen Einfluss das Verhalten auf die Einstellung hat. Eines der Ziele dieser Studie war es, das theoretische Awareness-Messmodell zu erproben, es ist jedoch notwendig, nicht nur die theoretische Einstellung und das theoretische Verhalten der Probanden zu beforschen, sondern anhand von praktischen Experimenten das Awareness-Modell, und somit auch die Einstellung und das Verhalten der Informationssicherheit gegenüber, zu evaluieren.

Ein weiterer Fokus der Studie lag auf der Messung der Informationssicherheits-Awareness anhand einer standardisierten Befragung, die bei der Informationssicherheits-Awareness-Überprüfung zu allen fünf Zeitpunkten im Rahmen der drei Informationssicherheitsaspekte (Wissen, Einstellung und Verhalten) genutzt wurde. Obwohl sich das Wissen, als ein Aspekt der Informationssicherheits-Awareness, mit einer standardisierten Befragung relativ unproblematisch untersuchen lässt, soll der Einsatz dieser Methode bei der Untersuchung von Einstellung und Verhalten kritisch betrachtet werden. Bei dieser Untersuchung konnten beispielsweise die Einstellung und das Verhalten der Probanden anhand von realen Experimenten nicht untersucht und evaluiert werden, daher ist es von großer Bedeutung, dass die zukünftige Forschung sich in diese Richtung entwickelt. Darüber hinaus könnte in weiteren Studien eine standardisierte Befragung analog zu der, die in dieser Studie eingesetzt wurde, verwendet werden, um beispielsweise das Wissen der Probanden zu messen. Allerdings sollten die Einstellung und das Verhalten mit zusätzlichen Methoden gemessen werden.

Das in dieser Studie entwickelte und erprobte Fragebogenkonstrukt für die fünf relevantesten Themen der Informationssicherheit kann künftig zur Messung der Informationssicherheits-Awareness in weiteren Studien benutzt werden. Allerdings wurden

die gleichen Indikatoren und Items zu allen fünf Erhebungszeitpunkten eingesetzt, um die höchste Erhebungsanzahl zu aktuellen Kontexten der Informationssicherheit zu erhalten, die schon in der Forschung analysiert werden. Für weitere Studien ist es aber empfehlenswert, weitere Indikatoren und Items oder Experimente für die Informationssicherheits-Awareness-Überprüfung einzusetzen. Zudem decken die genutzten fünf Kontexte viele, aber nicht alle Bereiche der Informationssicherheit ab. Die IT-Industrie und somit auch die Methoden der Social Engineers entwickeln sich rasch weiter, wodurch fraglich ist, welche Themen im Rahmen der Informationssicherheit in näherer Zukunft von Priorität sind. Daher sollten in zukünftigen Studien weitere Informationssicherheitskontexte bei der Überprüfung der Informationssicherheits-Awareness inkludiert werden.

Eins der Ziele dieser Studie war, zu überprüfen, inwiefern sich die Informationssicherheits-Awareness junger Mitarbeiter bei der Volkswagen AG nach einer bestimmten Art der Sensibilisierung ändert. Obwohl die Ergebnisse der Studie für eine bestimmte Zielgruppe gültig sind, nämlich „junge Erwachsene bei der Volkswagen AG", unterliegt diese Studie einigen Limitationen, aus denen sich Potenzial für zukünftige Forschung ableiten lässt. Eine der bedeutendsten Limitationen ist, dass diese Studie nur über einen bedingten Datensatz verfügt – es wurde nur eine bestimmte definierte Zielgruppe betrachtet. Es ist fraglich, ob die Ergebnisse auf andere Personengruppen übertragbar sind, dies sollte in weiteren Studien evaluiert werden. Außerdem sollte in weiteren Studien überprüft werden, inwiefern das Informationssicherheits-Awareness-Messinstrument auf andere und größere Zielgruppen (statt wie hier Auszubildende der Volkswagen AG) anwendbar ist.

Eine weitere Limitation dieser Studie liegt im Forschungsdesign, nämlich im Einsatz der Security Arena zusätzlich zu einer Grundsensibilisierung zum Thema Informationssicherheits-Awareness. Wie schon erwähnt, ist es die interne Regelung bei der Volkswagen AG, dass jeder Beschäftigte erst eine Grundsensibilisierung bekommen soll. Erst danach durfte die Security Arena durchgeführt werden. Für weitere Studien in diesem Bereich wäre es sinnvoll, zwei separate Gruppen von Probanden in den Blick zu nehmen, die zwei verschiedene Arten der Sensibilisierung durchlaufen, um einen Vergleich zwischen einer spielerischen und einer klassischen Awareness-Methode zu untersuchen.

Andere Einflüsse, die eventuell eine Rolle im Informationssicherheits-Awareness-Bereich spielen und die Informationssicherheits-Awareness der Zielgruppe beeinflussen, beispielsweise das soziale Umfeld, die Motivation der Probanden oder die Kultur des Unternehmens etc., wurden in dieser Studie nicht berücksichtigt und bieten folglich in weiteren Untersuchungen noch mehr Forschungspotenzial.

Die Ergebnisse, die ausgewählten Kontexte und die Zielgruppe dieser Studie gelten für den Bereich Automobilindustrie. Es ist es fraglich, inwiefern sowohl das Informationssicherheits-Awareness-Messmodell als auch die spielerische Awareness-Methode für weitere Unternehmen und Branchen relevant und aktuell bleiben. Zukünftige Studien sollten in anderen Unternehmen oder Institutionen durchgeführt werden, um dies zu überprüfen.

Die Auswertung dieser Studie erfolgte anhand der PLS-Methode. Wie schon beschrieben, erfolgte die Beurteilung der PLS-Modelle basierend auf einer Betrachtung der in den Kapiteln 4.5.1.3 und 4.5.1.4 vorgestellten Gütekriterien. Allerdings existieren in der Forschung unterschiedliche Bewertungskriterien für einige Gütekriterien der PLS-Methode (siehe Kapitel 4.5.1.3). Zukünftige Studien sollten sich darauf konzentrieren, weitere reflektive und formative Modelle zu evaluieren, um optimale Bewertungsgrade der Gütekriterien zu finden. Nitzl (2010, S. 39) beschreibt auch, dass trotz beispielsweise hohem R^2 und positivem Q^2 in einem Modell andere Modelle zur besseren Erklärung einer Zielvariable existieren könnten. Laut Nitzl (2010, S. 40) soll der Forscher eigenständig wesentliche von unwesentlichen Einflussvariablen trennen. In zukünftiger Forschung sollte weitergehend analysiert werden, nach welchen Prinzipien die wesentlichen von den unwesentlichen Einflussvariablen getrennt werden, um die optimale Anzahl der berücksichtigten Variablen in einem Modell zu behalten. Interessant wäre auch, zu eruieren, inwiefern formative Modelle anstelle von reflektiven Modellen eingesetzt werden können, denn laut Nitzl (2010, S. 54 in Anlehnung an Reinartz, Haenlein & Henseler, 2009, S. 333; Weiber & Mühlhaus, 2010, S. 201) werden die formativen Modelle in der Forschung vernachlässigt, da kovarianzbasierte Modelle aktuell darin dominieren. Laut Nitzl (2010, S. 55) soll die PLS-Auswertungsmethode jedoch weiter in der anwendungsorientierten Wissenschaft eingesetzt werden, da sie konkrete Lösungen und Handlungsempfehlungen basierend auf der Beurteilung der Modelle generiert.

Literaturverzeichnis

Abraham, S. (2011). Information security behavior: factors and research directions. *AMCIS 2011 Proceedings – All Submissions, 462*. Abgerufen am 28.07.2024 von https://aisel.aisnet.org/amcis2011_submissions/462

Abramovaite, J., Bandyopadhyay, S., Bhattacharya, S. & Cowen, N. (2023). Classical deterrence theory revisited: An empirical analysis of Police Force Areas in England and Wales. *European Journal of Criminology 2023, 20*(5), 1663–1680. doi: 10.1177/14773708211072415. Abgerufen am 28.07.2024.

Abt, C. (1970). *Serious Games*. New York: The Viking Press.

Adams, M. J., Tenney, Y. J. & Pew, R. W. (1995). Situation awareness and the cognitive management of complex systems. *Human Factors, 37*(1), 85–104. doi: 10.1518/001872095779049462. Abgerufen am 28.07.2024.

Agarwal, R. & Karahanna, E. (2000). Time flies when you're having fun: Cognitive absorption and beliefs about information technology usage. *MIS Quarterly, 24*(4), 665–694. doi: 10.2307/3250951. Abgerufen am 28.07.2024.

Ajzen I. (1985). From intentions to actions: A theory of planned behavior. In J. Kuhl & J. Beckman (Hg.), *Action-control. SSSP Springer Series in Social Psychology* (S. 11–39). Berlin, Heidelberg: Springer.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179–211. doi: 10.1016/0749-5978(91)90020-T. Abgerufen am 28.07.2024.

Ajzen I. (2005). *Attitudes, Personality and Behavior*. Maidenhead, UK: Open Press.

Ajzen I. (2006). *Behavioral Interventions Based on the Theory of Planned Behavior*. Abgerufen am 28.07.2024 von https://people.umass.edu/aizen/pdf/tpb.intervention.pdf

Ajzen, I. & Fishbein, M. (1977). Attitude-behavior relations: A theoretical analysis and review of empirical research. *Psychological Bulletin, 84*(5), 888–918. doi: 10.1037/0033-2909.84.5.888. Abgerufen am 28.07.2024.

Ajzen, I. & Fishbein, M. (1980) *Understanding attitudes and predicting social behavior*. Englewood Cliffs, NJ: Prentice-Hall.

Ajzen, I. & Fishbein, M. (2005). The influence of attitudes on behavior. In D. Albarracin, B. T. Johnson & M. P. Zanna (Hg.), *The handbook of attitudes* (S. 173–221). Mahwah, NJ: Lawrence Erlbaum Associates. Abgerufen am 28.07.2024 von https://www.researchgate.net/publication/264000974_The_Influence_of_Attitudes_on_Behavior#full-text

Ajzen, I. & Madden, T. J. (1986). Prediction of goal-directed behavior: attitudes, intentions and perceived behavior control. *Journal of Experimental Social Psychology, 22*(5), 453–474. doi: 10.1016/0022-1031(86)90045-4. Abgerufen am 28.07.2024.

Akers, R. L. (2010). *Deviant behavior. A social learning approach*. Belmont, CA: Wadsworth Pub. Co.

Aladawy, D., Beckers, K. & Pape, S. (2018). PERSUADED: Fighting Social Engineering Attacks with a Serious Game. In S. Furnell, H. Mouratidis, G. Pernul (Hg.), *Trust, Privacy and Security in Digital Business. Lecture Notes in Computer Science* (S. 103–118). doi: 10.1007/978-3-319-98385-1_8. Abgerufen am 28.07.2024.

Albers, S & Götz, O. (2006). Messmodelle mit Konstrukten zweiter Ordnung in der betriebswirtschaftlichen Forschung. *Die Betriebswirtschaft, 66*(6), 669–677. Abgerufen am 28.07.2024 von https://www.researchgate.net/publication/284038462_Messmodel le_mit_Konstrukten_zweiter_Ordnung_in_der_betriebswirtschaftlichen_Forschung

Albrechtsen E. (2007). A qualitative study of users' view on information security. *Computers & Security, 26*(4), 276–289. doi: 10.1016/j.cose.2006.11.004. Abgerufen am 16.02.2022.

Aldawood H. & Skinner, G. (2018). *Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review*. 2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE), 62–68. doi: 10.1109/TALE.2018.86 15162. Abgerufen am 28.07.2029 von https://ieeexplore.ieee.org/document/8615162

Alexander, P. A. & Dochy, F. J. R. C. (1995). Conceptions of knowledge and beliefs: A comparison across varying cultural and educational communities. *American Educational Research Journal, 32*(2), 413–442. doi: 10.3102/00028312032002413. Abgerufen am 28.07.2024.

Aloul, F. A. (2012). The Need for Effective Information Security Awareness. *Journal of advances in information technology, 3*(3), 176–183. doi: 10.4304/jait.3.3.176-183. Abgerufen am 28.07.2024.

Amelang, M. & Bartussek, D. (2001). *Differentielle Psychologie und Persönlichkeitsforschung* (5., aktualisierte und erweiterte Auflage). Stuttgart: Kohlhammer.

Anderson, J., Gerbing, D. & Hunter, E. (1987). On the Assessment of Unidimenional Measurement: Internal and External Consistency, and Overall Consistency Criteria. *Journal of Marketing Research, 24*(4), 432–437. doi: 10.1177/002224378702400412. Abgerufen am 28.07.2024.

Anderson, R., Barton, C., Bohme, R., Clayton, R., van Eeten, M. J. G., Levi, M., Moore, T. & Savage, S. (2012). Measuring the cost of cybercrime. *11th annual workshop on the economics of information security, Berlin, Germany 2012*. doi: 10.1007/978-3-642-39498-0_12. Abgerufen am 28.07.2024 von https://www.researchgate.net/publication/263605690_ Measuring_the_Cost_of_Cybercrime

Ashfaq, S., Chandre, P., Pathan, S., Mande, U., Nimbalkar, M. & Mahalle, P. (2024). Defending Against Vishing Attacks: A Comprehensive Review for Prevention and Mitigation Techniques. In N. R. Roy, S. Tanwar & U. Batra (Hg.), *Cyber Security and Digital Forensics. Lecture Notes in Networks and System* (S. 411–422). Springer, Singapore. doi: 10.1007/978-981-99-9811-1_33. Abgerufen am 28.07.2024.

Atteslander, P. (2003). *Methoden der empirischen Sozialforschung*. Berlin: de Gruyter.

Backhaus, K., Blechschmidt, B. & Eisenbeiß, M. (2006a). Der Stichprobeneinfluss bei Kausalanalysen. *Die Betriebswirtschaft, 66*(6), 711–726. Abgerufen am 28.07.2024 von https://www.proquest.com/docview/208919266?pq-origsite=gscholar&fromopen view=true&sourcetype=Scholarly%20Journals

Backhaus, K., Erichson, B., Wulff, P. & Weiber, R. (2006b). *Multivariate Analysemethoden – Eine anwendungsorientierte Einführung* (11., überarbeitete Auflage). Berlin: Springer.

Backhaus, K., Erichson, B. & Weiber, R. (2011). *Fortgeschrittene multivariate Analysemethoden. Eine anwendungsorientierte Einführung*. Berlin: Springer.

Baranowski, T., Cullen, K. W., Nicklas, A., Thompson, D. & Baranowski, J. (2003). Are current health behavioral change models helpful in guiding prevention of weight gain efforts? *Obesity Research, 11*(10), 23–43. doi: 10.1038/oby.2003.222. Abgerufen am 28.07.2024 von https://www.researchgate.net/publication/231584367_Are_Current_Health_Behavioral_Change_Models_Helpful_in_Guiding_Prevention_of_Weight_Gain_Efforts

Bartholomew, D. J., Steele, F., Moustaki, I. & Galbraith, J. (2002). *The analysis and interpretation of multivariate data for social scientists*. CRC Press.

Baur, N. & Fromm, S. (2004). Einleitung: Die Rolle von SPSS im Forschungsprozess. In N. Baur & S. Fromm (Hg.), *Datenanalyse mit SPSS für Fortgeschrittene* (S. 13–15). Wiesbaden: VS Verlag für Sozialwissenschaften.

Baur, N. & Lück, D. (2004). Vom Fragbogen zum Datensatz. In N. Baur & S. Fromm (Hg.), *Datenanalyse mit SPSS für Fortgeschrittene* (S. 18–51). Wiesbaden: VS Verlag für Sozialwissenschaften.

Benning, V. (2020). *Arithmetisches Mittel verstehen und berechnen – mit Beispielen*. Abgerufen am 28.07.2024 von https://www.scribbr.de/statistik/arithmetisches-mittel/

Berelson, B. (1952). *Content Analysis in Communication Research*. Clencoe, Ill.: Free Press.

Bergkvist, L. & Rossiter, J. (2007). The predictive validity of multiple-item versus single-item measures of the same constructs. *Journal of Markeing Research, 44*(2), 175–184. doi: 10.1509/jmkr.44.2.175. Abgerufen am 28.07.2024.

Bisson, D. (01.03.2023). *5 Social Engineering Attacks to Watch Out For*. Tripwire Retrieved [Weblog-Eintrag]. Abgerufen am 28.07.2024 von http://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/

Block, M., Brassler, M., Frohnwieser, C. & Westholm H. (2018). *Nachhaltigkeit in der Lehre – Perspektiven der Universität Hamburg*. Hamburg: Kompetenzzentrum Nachhaltige Universität (KNU)/Team 2 Studium und Lehre. Abgerufen am 28.07.2024 von https://www.nachhaltige.uni-hamburg.de/downloads/2018/broschuere-nachhaltigkeit-in-der-lehre.pdf

Bloom B. (1964). *Taxonomy of educational objectives: The classification of educational goals*. New York: David McKay Company.

Bohnsack, R. (2000). *Rekonstruktive Sozialforschung. Einführung in Methodologie und Praxis qualitativer Forschung* (4. Auflage). Opladen: Leske + Budrich.

Bohnsack, R. (2010). *Rekonstruktive Sozialforschung. Einführung in qualitative Methoden* (8. Auflage). Opladen und Farmington Hills: Verlag Barbara Budrich.

Blötz, U., Ballin, D. & Gust M. (2015). Planspiele im Vergleich zu anderen Trainingsmethoden. In U. Blötz (Hg.), *Planspiele und Serious Games in der beruflichen Bildung. Auswahl, Konzepte, Lernarrangements, Erfahrungen – Aktueller Katalog für Planspiele und Serious Games 2015* (5. Auflage, S. 26–35). Bundesinstitut für Berufsbildung. Bielefeld: W. Bertelsmann.

Bogner, A. & Menz, W. (2005). Das theoriegenerierende Experteninterview. Erkenntnisinteresse, Wissensformen, Interaktion. In A. Bogner, B. Littig & W. Menz (Hg.), *Das Experteninterview: Theorie, Methode, Anwendung* (S. 7–30). Wiesbaden: VS-Verlag.

Boomsma, A. (1982). The Robustness of LISREL against Small Sample Size in Factor Analysis Models. In K. Jöreskog & H. Wold (Hg.), *Systems Under Direct Observations: Causality, Structure, Prediction, Part 1* (S. 149–174). Amsterdam: North-Holland Publ. Co.

Bopp, K. (2009). *Serious Games Ein Literaturbericht*. Unveröffentlichtes Manuskript. Abgerufen am 28.07.2024 von https://www.researchgate.net/publication/260198503_Serious_Games_Ein_Literaturbericht#full-text

Bortz, J. & Döring, N. (2005). *Forschungsmethoden und Evaluation für Human- und Sozialwissenschaftler* (3., überarbeitete Auflage). Heidelberg: Springer Medizin Verlag.

Bortz, J. & Döring, N. (2006). *Forschungsmethoden und Evaluation für Human- und Sozialwissenschaftler* (4., überarbeitete Auflage). Berlin: Springer-Verlag.

Bošnjak, L. & Brumen, B. (2019). Shoulder surfing: From an experimental study to a comparative framework. *International Journal of Human-Computer Studies, 130*(20), 1–20. doi: 10.1016/j.ijhcs.2019.04.003. Abgerufen am 28.07.2023.

Bremer T. & Busch C. (2009). SpielZeit – Meilensteine der Spielentwicklung, ein Abriss. In J. Sieck & M. A. Herzog (Hg.), *Kultur und Informatik: Serious Games* (S. 7–17). Boizenburg: Verlag Werner Hülsbusch.

Breton, R. & Rousseau, R. (2001). *Situational Awareness. A review of the concept and its measurement*. Technical Report No. 2001–220, Defense Research and Development. Canada: Valcartier.

Breuer, J. S. & Bente, G. (2010). Why so serious? On the relation of serious games and learning. *Journal for Computer Game Culture, 4*(1), 7–24. doi: 10.7557/23.6111. Abgerufen am 28.07.2024.

Brosius, H.-B. & Koschel, F. (2001). *Methoden der empirischen Kommunikationsforschung. Eine Einführung*. Wiesbaden: Westdeutscher Verlag.

Bruvold, W. H. (1990). A meta-analysis of the California school-based risk reduction program. *Journal of Drug Education, 20*(2), 139–152. doi: 10.2190/7CRH-5R8T-MHR6-6UD7. Abgerufen am 28.07.2024.

Bulgurcu B. (2008). *The antecedents of information security policy compliance (MSc thesis)*. Canada: The University of British Columbia. doi: 10.14288/1.0066478. Abgerufen am 28.07.2024 von http://hdl.handle.net/2429/1121

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. doi: 10.2307/25750690. Abgerufen am 28.07.2024.

Bryman, A. (2006). Integrating quantitative and qualitative research: How is it done? *Qualitative Research, 6*(1), 97–113. doi: 10.1177/1468794106058877. Abgerufen am 28.07.2024.

Bundesamt für Sicherheit in der Informationstechnik (2015). *Cyber-Sicherheits-Umfrage 2015*. Bonn: BSI. Abgerufen am 28.07.2024 von http://docplayer.org/23467522-Cyber-sicherheits-umfrage-ergebnisse-stand.html

Bundesamt für Sicherheit in der Informationstechnik (2018). *Cyber-Sicherheits-Umfrage 2017. Cyber-Risiken, Meinungen und Maßnahmen*. Bonn: BSI. Abgerufen am 28.07.2024 von https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/cyber-sicherheits-umfrage_2017.pdf?__blob=publicationFile&v=1

Bundesamt für Sicherheit und Informationstechnik (2023). *Tipps zum sicheren Umgang mit sozialen Netzwerken*. Abgerufen am 28.07.2024 von https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Onlinekommunikation/Soziale-Netzwerke/Sichere-Verwendung/sichere-verwendung.html

CBS (2019). *1.2 million cybercrime victims*. Abgerufen am 28.07.2024 von https://www.cbs.nl/en-gb/news/2019/29/1-2-million-cybercrime-victims

Chenoweth, T., Minch, R. & Gattiker, T. (2009). Application of Protection Motivation Theory to Adoption of Protective Technologies. 42nd Hawaii International Conference on System Sciences. doi: 10.1109/HICSS.2009.74. Abgerufen am 28.07.2024 von https://ieeexplore.ieee.org/document/4755604

Chin, W. W. (1998a). Issues and Opinion on Structural Equation Modeling. *MIS Quarterly, 22*(1), 7–16.

Chin, W. W. (1998b). The partial least squares approach to structural equation modeling. In G. A. Marcoulides (Hg.), *Modern Business Research Methods* (S. 295–336). New Jersey: Lawrence Erlbaum Associates.

Chin, W. & Newsted, P. (1999). Structural Equation Modeling Analysis with Small Samples Using Partial Least Squares. In R. Hoyle (Hg.), *Strategies for Small Sample Research* (S. 307–342). Thousend Oaks: Sage Publications.

Christophersen, T. & Grape, C. (2007). Die Erfassung latenter Konstrukte mit Hilfe formativer und reflektiver Messmodelle. In A. Sönke, D. Klapper, U. Konradt, A. Walter & J. Wolf (Hg.), *Methodik der empirischen Forschung* (2., überarbeitete und erweiterte Auflage, S. 104–118). Wiesbaden: Gabler.

Churchill, G. (1979). A Paradigm for Developing Better Measures of Marketing Constructs. *Journal of Marketing, 16*(1), 64–73. doi: 10.2307/3150876 Abgerufen am 28.07.2024.

Cicourel, A. V. (1975). *Sprache in der sozialen Interaktion*. München: List.

Cohen, J. (1988). Statistical Power Analysis for the Behavioral Sciences (2.' Ausgabe). Hilsdale: Lawrence Earlbaum Associates.

Collins German Dictionary (2004). *Reverso Wörterbuch* (5., komplette und ungekürzte Ausgabe). © William Collins Sons & Co. Ltd., 1980 © HarperCollins Publishers 1991, 1997, 1999, 2004. Abgerufen am 28.07.2024 von https://woerterbuch.reverso.net/deutsch-englisch/

Cook, T. D. & Campbell, D. T. (1979). *Quasi-experimentation: Design and analysis issues for field settings*. Boston: Houghton Mifflin.

Creswell, J. W. & Plano Clark, V. L. (2011). *Designing and Conducting Mixed Methods Research*. Thousand Oaks, CA: Sage Publications.

Creswell, J. W. & Plano Clark, V. L. (2018). *Designing and Conducting Mixed Methods Research* (3. Auflage). Thousand Oaks, CA: Sage Publications.

Crookall, D. (2005). Video games: Issues in research and learning, Part 1. *Simulations and Gaming, 36*(4), 437–439. doi: 10.1177/1046878105283148. Abgerufen am 28.07.2024.

Cyber Security Intelligence (CSI) (2018). *Millennials More Likely To Fall Victim To Cybercrime*. Abgerufen am 28.07.2024 von https://www.cybersecurityintelligence.com/blog/millennials-more-likely-to-fall-victim-to-cybercrime-3225.html

D'Arcy, J. & Herath, T. (2017). A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. *European Journal of Information Systems, 20*(6), 643–658. doi: 10.1057/ejis.2011.23. Abgerufen am 28.07.2024.

D'Arcy, J. & Hovav, A. (2007). Deterring internal information systems misuse. *Communications of the ACM, 50*(10), 113–117. doi: 10.1145/1290958.1290971. Abgerufen am 28.07.2024.

D'Arcy, J. & Hovav, A. (2008). Towards a best fit between organizational security countermeasures and information systems misuse behaviors. *Journal of Information System Security, 3*(2), 3–30.

D'Arcy, J. & Hovav, A. (2009). Does one size fit all? Examining the differential effects of IS security countermeasures. *Journal of Business Ethics, 89*(1), 59–71. doi: 10.1007/s10551-008-9909-7. Abgerufen am 28.07.2024.

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. doi: 10.1287/isre.1070.0160. Abgerufen am 28.07.2024.

Da Veiga, A. (2016). Comparing the information security culture of employees who had read the information security policy and those who had not. *Information & Computer Security, 24*(2), 139–151. doi: 10.1108/ICS-12-2015-0048. Abgerufen am 28.07.2024.

Deloitte. (2011). *Raising the bar: 2011 TMT global security study with key findings*. Bericht veröffentlicht von Deloitte.

Deloitte. (2018). *Cyber Security Report 2018 Teil 2: Unternehmen – das Risikobewusstsein sinkt*. Bericht veröffentlicht von Deloitte. Abgerufen am 28.07.2024 von https://www2.deloitte.com/content/dam/Deloitte/de/Documents/risk/Studie-Risk-Advisory-RA-Cyber-Security-Report-2018-Teil-2.pdf

Desolda, G., Ferro, L. S., Marrella, A., Costabile, M. F. & Catarci, T. (2022). Human Factors in Phishing Attacks: A Systematic Literature Review. *ACM Computing Surveys, 54*(35). doi: 10.1145/3469886. Abgerufen am 28.07.2024.

Deterding, S., Dixon, D., Khaled, R. & Nacke, L. (2011). From game design elements to gamefulness: Defining "gamification". *Proceedings of the 15th International Academic MindTrek Conference: Envisioning Future Media Environment, 9* – 15. doi: 10.1145/2181037.2181040. Abgerufen am 28.07.2024.

Diamantopoulos, A. (1999). Viewpoint: Export Performance Measurement – Reflective versus Formative lndicators. *International Marketing Review, 16*(6), 444–457. doi: 10.1108/02651339910300422. Abgerufen am 28.07.2024.

Dhillon, G. & Moores, S. (2001). Computer crimes: Theorizing about the enemy within. *Computers & Security, 20*(8), 715–723. doi: 10.1016/S0167-4048(01)00813-6. Abgerufen am 28.07.2024.

Diekmann, A. (2005). *Empirische Sozialforschung. Grundlagen, Methoden, Anwendungen*. Reinbek: Rowohlt.

Diller, H. (2006). Probleme der Handhabung von Strukturgleichungsmodellen in der betriebswirtschaftlichen Forschung – Eine kritische Einführung. *Die Betriebswirtschaft, 66*(6), 611–617.

Dominguez, C. (1994). Can SA be defined? In M. Vidulich, C. Dominguez, E. Vogel & G. McMillan (Hg.), *Situation Awareness: Papers and Annotated Biography* (S. 5–17). Wright-Patterson AFB, OH: Armstrong Laboratory. doi: 10.21236/ada284752. Abgerufen am 28.07.2024 von https://apps.dtic.mil/sti/pdfs/ADA284752.pdf

Drolet, A. & Morrison, D. (2001). Do We Really Need Multiple-Item Measures in Service Research? *Journal of Service Research, 3*, 196–204. doi: 10.1177/109467050133001. Abgerufen am 28.07.2024.

Durso, F. T. & Gronlund, P. (1999). Situation Awareness. In F. T. Durso, R. S. Nickerson, R. W. Schvaneveldt, S. Dumais, S. Lindsay & M. Chi (Hg.), *Handbook of applied cognition* (S. 283–314). New York: John Wiley & Sons.

Eberl, M. (2004). Formative und reflektive Indikatoren im Forschungsprozess: Entscheidungsregeln und die Dominanz des reflektiven Modells, *Schriften zur Empirischen Forschung und Quantitativen Unternehmensplanung*. München: Ludwig-Maximilians-Universität.

Eberl, M. (2006). Formative und reflektive Konstrukte und die Wahl des Strukturgleichungsverfahrens. Eine statistische Entscheidungshilfe. *Die Betriebswirtschaft, 66*(6), 651–668.

Edwards, J. & Bagozzi, R. (2000). On the Nature and Direction of Relationships Between Constructs and Measures. *Psychological Methods, 5*(2), 155–174. doi: 10.1037/1082-989X.5.2.155. Abgerufen am 28.07.2024 von https://www.researchgate.net/publication/12384011_On_the_Nature_and_Direction_of_Relationships_Between_Constructs_and_Measures

Efron, B. (1979). Bootstrap Methods: Another Look at the Jackknife. *The Annals of Statistics, 7*(1), 1–26. doi: 10.1214/aos/1176344552. Abgerufen am 28.07.2024.

Egenfeldt-Nielsen, S. (2006). Overview of research on the educational use of video games. *Nordic Journal of Digital Literacy, 1*(3), 184–214. doi: 10.18261/ISSN1891-943X-2006-03-03. Abgerufen am 28.07.2024.

Egenfeldt-Nielsen, S. (2013). Die ersten zehn Jahre der Serious Games-Bewegung. Zehn Lektionen. In G. S. Freyermuth, L. Gotto & F. Wallenfels (Hg.), *Serious Games, Exergames, Exerlearning. Zur Transmedialisierung und Gamification des Wissenstransfers* (S. 145–164). Bielefeld: transcript. doi: 10.14361/transcript.9783839421666.145. Abgerufen am 28.07.2024.

Eid, M., Gollwitzer, M. & Schmitt, M. (2017). *Statistik und Forschungsmethoden* (5. Auflage). Weinheim: Beltz.

Endsley, M. R. (1988). *Situation Awareness global assessment technique (SAGAT)*. Proceedings of the National Aerospace and Electronics Conference (NAECON) (S. 789–795). New York: IEEE. doi: 10.1109/NAECON.1988.195097. Abgerufen am 28.07.2024.

Endsley, M. R. (1995). Toward a Theory of Situation Awareness in Dynamic Systems. *Human Factors Journal, 37*(1), 32–64. doi: 10.1518/001872095779049543. Abgerufen am 28.07.2024.

Engineering & Technology (2021). *Younger people more likely to fall victim to cyber crime, survey finds*. Abgerufen am 28.07.2024 von https://eandt.theiet.org/2021/11/04/younger-people-more-likely-fall-victim-cyber-crime-survey-finds.

Ermi, L. & Mäyrä, F. (2005). Player-Centred Game Design: Experiences in Using Scenario Study to Inform Mobile Game Design. *The international journal of computer game research, 5*(1). Abgerufen am 28.07.2024 von https://www.gamestudies.org/0501/ermi_mayra/

Ernst & Young. (2011). *Into the cloud, out of the fog: Ernst & Young's 2011 global information security survey.* Bericht veröffentlicht von Ernst & Young.

Fan J. & Zhang P. (2011). Study on e-government information misuse based on General Deterrence Theory. *8th international conference on service systems and service management (ICSSSM)*, 1–6. Tianjin. doi: 10.1109/ICSSSM.2011.5959454. Abgerufen am 28.07.2024 von https://ieeexplore.ieee.org/document/5959454

Fassott, G. (2006). Operationalisierung latenter Variablen in Strukturgleichungsmodellen: Eine Standortbestimmung. *Zeitschrift für betriebswirtschaftliche Forschung, 58*(2), 67–88. doi: 10.1007/BF03371644. Abgerufen am 03.08.2024.

Fassott, G. & Eggert, A. (2005). Zur Verwendung formativer und reflektiver Indikatoren in Strukturgleichungsmodellen: Bestandsaufnahme und Anwendungsempfehlungen. In F. Bliemel, A. Eggert, G. Fassott & J. Henseler (Hg.), *Handbuch PLS-Pfadmodellierung: Methode, Anwendung, Praxisbeispiele* (S. 31–47). Stuttgart: Schäffer-Poeschel Verlag.

Faulbaum, F. (2019). *Methodische Grundlagen der Umfrageforschung*. Wiesbaden: VS Verlag Sozialwissenschaften.

Fishbein, M. (1967). Attitude and the prediction of behavior. In M. Fishbein (Hg.), *Readings in attitude theory and measurement* (S. 477–492). New York: John Wiley & Sons.

Fishbein, M. & Ajzen, I. (1981). On construct validity: A critique of Miniard and Cohen's paper. *Journal of Experimental Social Psychology, 17*(3), 340–350. doi: 10.1016/0022-1031(81)90032-9. Abgerufen am 03.08.2024.

Flandorfer, P. (2023). *Cronbachs Alpha berechnen und interpretieren – mit Beispiel*. Scribbr. Abgerufen am 28.07.2024 von https://www.scribbr.de/statistik/cronbachs-alpha/

Flick, U. (1987). Methodenangemessene Gütekriterien in der qualitativ-interpretativen Forschung. In J. B. Bergold & U. Flick (Hg.), *Ein-Sichten. Zugänge zur Sicht des Subjekts mittels qualitativer Forschung* (S. 247–262). Tübingen: DGVT.

Flick, U. (2014). *Qualitative Sozialforschung. Eine Einführung* (6. Auflage). Reinbek bei Hamburg: Rowohlt Taschenbuch Verlag.

Flick, U., Kardorff, E. V., Keupp, H., Rosenstiel, L. V. & Wolff, S. (1991). *Handbuch qualitative Sozialforschung: Grundlagen. Konzepte, Methoden und Anwendungen*. München: Psychologie Verlags Union.

Foltz, C. B. (2000). *The impact of deterrent countermeasures upon individual intent to commit misuse: A behavioral approach*. Unpublished doctoral dissertation, University of Arkansas, Fayetteville.

Fornell, C. & Cha, J. (1994). Partial Least Squares. In R. Bagozzi (Hg.), *Advanced Methods of Marketing Research* (S. 52–87). Cambridge: Blackwell Business.

Fornell, C. & Larcker, D. F. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. *Journal of Marketing Research, 18*(1), 39–50. doi: 10.2307/3151312. Abgerufen am 03.08.2024.

Fowler, F. J. (1988). *Survey research methods* (2., überarbeitete Auflage). Newbury Park: Sage.

Fox, D. & Kaun, S. (2005). Security Awareness-Kampagnen. *9. Deutscher IT-Sicherheitskongress des BSI*. Abgerufen am 28.07.2024 von https://www.secorvo.de/publikationen/awareness-kampagnen-fox-kaun-2005.pdf

Frick, H. & Hitz D. (2011). Die Leistung von Serious Games wird oft (noch) unterschätzt. In M. Metz & F. Theis (Hg.), *Digitale Lernwelt – Serious Games. Einsatz in der beruflichen Weiterbildung* (S. 161–173). Bielefeld: W. Bertelsmann Verlag GmbH & Co. KG.

Friedrichs, J. (1973). *Methoden empirischer Sozialforschung*. Reinbek: Rowohlt.

Friedrichs, J. (1990). *Methoden empirischer Sozialforschung*. Opladen: Westdeutscher Verlag.

Fritz, W. (1995). *Marketing-Management und Unternehmenserfolg: Grundlagen und Ergebnisse einer empirischen Untersuchung* (2. Auflage). Stuttgart: Schäffer-Poeschel.

Fuchs, C & Diamantopoulos, A. (2009). Using single-item measures for construct measurement, *Die Betriebswirtschaft, 69*(2), 195–210.

Fuß, S. & Karbach, U. (2014). *Grundlagen der Transkription. Eine praktische Einführung*. Opladen, Toronto: Verlag Barbara Budrich.

Galbraith, J. R. (2002). *Designing Organizations. An executive guide to strategy, structure and process*. San Francisco, California: Jossey-Bass.

Galvez, S. M. & Guzman, I. R. (2009). *Identifying factors that influence corporate information security behavior*. AMCIS 2009 Proceedings. San Francisco, California.

Ganguin, S. & Hoblitz, A. (2013). Serious Games – Ernstes Spielen? Über das Problem von Spielen, Lernen und Wissenstransfer. In G. S. Freyermuth, L. Gotto & F. Wallenfels (Hg.), *Serious Games, Exergames, Exerlearning. Zur Transmedialisierung und Gamification des Wissenstransfers*. Bielefeld: transcript.

Garfinkel, H. (1967). *Studies in Ethnomethodology*. Englewood Cliffs (New Jersey): Prentice-Hall.

Gibbs, J. P. (1975). *Crime, Punishment and Deterrence*. New York: Elsevier.

Gläser, J. & Laude, G. (2004). *Experteninterviews und qualitative Inhaltsanalyse*. Wiesbaden: VS Verlag.

Gold, A. H., Malhotra, A. & Segars, A. H. (2001). Knowledge management: an organizational capabilities perspective. *Journal of Management Information Systems, 18*(1), 185–214. doi: 10.1080/07421222.2001.11045669. Abgerufen am 28.07.2024.

Gopal, R. D. & G. L. Sanders. (1997). Preventative and deterrent controls for software piracy. *Journal of Management Information Systems, 13*(4), 29–48. doi: 10.1080/07421222.1997.11518141. Abgerufen am 28.07.2024.

Götz, O. & Liehr-Gobbers, K. (2004). Analyse von Strukturgleichungsmodellen mit Hilfe der Partial-Least-Squares(PLS)-Methode. *Die Betriebswirtschaft, 64*(6), 714–738.

Graf, D. (2007). Die Theorie des geplanten Verhaltens. In D. Krüger & H. Voigt (Hg.), *Theorien in der biologiedidaktischen Forschung* (S. 33–43). Berlin, Heidelberg: Springer. doi: 10.1007/978-3-540-68166-3_4. Abgerufen am 28.07.2024.

Graffer, I., Line, M. B. & Bernsmed, K. (2015). *Play2Prepare: A Board Game Supporting IT Security Preparedness Exercises for Industrial Control Organizations*. Norwegian Information Security Conference 2015 (NISK-2015). Abgerufen am 28.07.2024 von https://sintef.brage.unit.no/sintef-xmlui/bitstream/handle/11250/2375121/2015%2BNISK%2B-%2BPlay2Prepare%2B-%2BA%2BBoard%2BGame%2BSupporting%2BIT%2BSecurity.pdf?sequence=3

Grimes, R. & Maier, R. (2018). Was ist Pentesting? *Computerwoche. Voice of digital*. Abgerufen am 28.07.2024 von https://www.computerwoche.de/a/was-ist-pentesting,3544219

Gulden, H. & Littger, M. (2014). *Verhaltensregeln zum Thema „Social Engineering"*. Spezialausgabe: Leitfaden für Mitarbeiter (1). Abgerufen am 28.07.2024 von https://www.sicher-im-netz.de/sites/default/files/download/leitfaden_social_engineering.pdf

Hackett, G. (1981). Survey Research Methods. *The Personnel and Guidance Journal, 59*(9), 599–604. doi: 10.1002/j.2164-4918.1981.tb00626.x. Abgerufen am 28.07.2024.

Häder, M. (2010). *Empirische Sozialforschung. Eine Einführung*. Wiesbaden: VS Verlag für Sozialwissenschaften. doi: 10.1007/978-3-531-92187-7. Abgerufen am 03.08.2024.

Hair, J. F., Black, W., Babin, B. & Anderson, R. (2010). *Multivariate Data Analysis* (7. Auflage). New Jersey: Pearson.

Hair, J. F., Hult, G. T. M., Ringle, C. M. & Sarstedt, M. (2017a). *A primer on partial least squares structural equation modeling (PLS-SEM)* (2. Auflage). Los Angeles: Sage.

Hair, J. F., Hult, G. T. M., Ringle, C. M., Sarstedt, M., Richter, N. F. & Hauff, S. (2017b). *Partial Least Squares Strukturgleichungsmodellierung. Eine anwendungsorientierte Einführung*. München: Franz Vahlen.

Harhoff, D. & Wagner, S. (2009). Regressionsanalyse. In A. Meyer & M. Schwaiger (Hg.), *Theorien und Methoden der Betriebswirtschaft* (S. 477–490). München: C. H. Beck.

Harrington, S. J. (1996). The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions. *MIS Quart, 20*(3), 257–278. doi: 10.2307/249656. Abgerufen am 28.07.2024.

Hart, S., Margheri, A., Paci, F. & Sassone, V. (2020). Riskio: A Serious Game for Cyber Security Awareness and Education. *Computers & Security, 95*(101827). doi: 10.1016/j.cose.2020.101827. Abgerufen am 28.07.2024.

Hatfield, J. M. (2018). Social engineering in cybersecurity: The evolution of a concept. *Computers & Security, 73*, 102–113. doi: 10.1016/j.cose.2017.10.008. Abgerufen am 28.07.2024.

Haucke, A. & Pokoyski, D. (2018). Mea culpa – Schuld, Scham und Opferrolle bei Social Engineering. Abgerufen am 28.07.2024 von https://www.kes-informationssicherheit.de/print/titelthema-identity-und-access-management-iam/mea-culpa/

Helisch, M. & Pokoyski, D. (2009). *Security Awareness: Neue Wege zur erfolgreichen Mitarbeiter – Sensibilisierung*. Wiesbaden: Vieweg+Teubner.

Henderson, S., Hoffman, R., Bunch, L. & Bradshaw, J. (2015). *Applying the Principles of Magic and the Concepts of Macrocognition to Counter-Deception in Cyber Operations*. Conference: Hawaii International Conference on System Sciences. doi: 10.24251/HICSS.2021.240. Abgerufen am 28.07.2024.

Henseler, J. (2005). Einführung in die PLS-Pfadmodellierung. *Wirtschaftswissenschaftliches Studium, 34*(2), 70–75. Abgerufen am 28.07.2024 von https://repository.ubn.ru.nl//bitstream/handle/2066/46752/46752.pdf

Henseler, J., Ringle, C. M. & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science, 43*(1), 115–135. doi: 10.1007/s11747-014-0403-8. Abgerufen am 28.07.2024.

Henseler, J., Ringle, C. M. & Sinkovics, R. R. (2009). The use of partial least squares path modeling in international marketing. In R. R. Sinkovics & P. N. Ghauri (Hg.), *New Challenges to International Marketing* (*Advances in International Marketing, Vol. 20)* (S. 277–319). doi: 10.1108/S1474-7979(2009)0000020014. Abgerufen am 28.07.2024.

Herath, T. & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*(2), 154–165. doi: 10.1016/j.dss.2009.02.005. Abgerufen am 02.07.2024.

Herrmann, T. (2018). *Kampagnen vs. Programme: Wortklauberei oder eine Frage des Mindsets?* Abgerufen am 17.02.2022 von https://www.chainrelations.de/kampagnen-vs-programme/

Hesse, C. (2015). *Keine Geheimnisse mehr. Methoden des Social Engineering*. Abgerufen am 05.08.2020 von https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/partner/150420_Partnerbeitrag_Riskworkers.pdf?__blob=publicationFile&v=4

Hesselhorn, M. & Goldt, A. (2009). *Pädagogische Psychologie. Erfolgreiches Lernen und Lehren*. Stuttgart: Kohlhammer.

Hildebrandt, L. & Temme, D. (2006). Probleme der Validierung mit Strukturgleichungsmodellen, *Die Betriebswirtschaft, 66*(6), 618–639.

Himme, A. (2007). Gütekriterien der Messung: Reliabilität, Validität und Generalisierbarkeit. In A. Sönke, D. Klapper, U. Konradt, A. Walter & J. Wolf (Hg.), *Methodik der empirischen Forschung* (2., überarbeitete und erweiterte Auflage, S. 375–390). Wiesbaden: Gabler.

Hirsch, E. D. (1967). *Validity in Interpretation*. New Haven, Conn: University Press.

Hoblitz, A. (2015). Spielen lernen im Flow. Die motivationale Wirkung von Serious Games im Schulunterricht. In J. Fromme, W. Marotzki, N. Meder, D. M. Meister & U. Sandler (Hg.), *Medienbildung und Gesellschaft* (Band 33). Wiesbaden: Springer.

Hofer, M., Fries, S., Clausen, M., Reinders, H., Dietz, F. & Schmid, S. (2005). *Fragebogen im Rahmen des Projekts ‚Wertewandel und Lernmotivation'*. Mannheim: Universität Mannheim.

Hoffmann, J. (2019). Virtuelle Angriffe im Keim ersticken. Wenn Finanzberater unterwegs sind, drohen Übergriffe auf das Smartphone oder den Computer. Wie Sie ihre Geräte vor Datendieben schützen. *Handelsblatt*. Abgerufen am 30.03.2022 von https://www.handelsblatt.com/finanzen/it-sicherheit-virtuelle-angriffe-im-keim-ersticken/25140048.html

Hoffman, M. L. (1986). Affect, cognition, and motivation. In R. M. Sorrentino & E. T. Higgins (Hg.), *Handbook of motivation and cognition* (S. 244–280). New York: Guilford Press.

Högsdal, N. (2011). Serious Games, Simulationen und Planspiele: same but different? In M. Metz & F. Theis (Hg.), *Digitale Lernwelt – Serious Games. Einsatz in der beruflichen Weiterbildung* (S. 117–131). Bielefeld: W. Bertelsmann.

Homburg, C. & Klarmann, M. (2006). Die Kausalanalyse in der empirischen Forschung – Problemfelder und Anwendungsempfehlungen. *Die Betriebswirtschaft, 66*(6), 727–748.

Hommel W. & Reiser, H. (2016). *Kapitel 4: Social Engineering – der Faktor Mensch in der IT-Sicherheit*. Abgerufen am 28.07.2024. von http://www.nm.ifi.lmu.de/teaching/Vorlesungen/2015ws/itsec/_skript/itsec-k4-v11.0.pdf

Huber, F., Herrmann, A., Meyer, F., Vogel, J. & Vollhardt, K. (2007). *Kausalmodellierung mit Partial Least Squares – Eine anwendungsorientierte Einführung*. Wiesbaden: Gabler.

Hulland, J. (1999). Use of Partial Least Squares (PLS) in strategic Management Research: A Review of Four Recent Studies. *Strategie Management Journal, 20*(4), 195–204. doi: 10.1002/(SICI)1097-0266(199902)20:23.0.CO;2-7. Abgerufen am 02.07.2024.

Huma, Z.-E., Hussain, S., Thurasamy, R. & Malik, M. I. (2017). Determinants of cyberloafing: A comparative study of a public and private sector organization. *Internet Research, 27*(1), 97–117. doi: 10.1108/IntR-12-2014-0317. Abgerufen am 28.07.2024.

Hwang, H., Malhotra, N. K., Kim, Y., Tomiuk, M. A. & Hong, S. (2010). A Comparative Study on Parameter Recovery of Three Approaches to Structural Equation Modeling. *Journal of Marketing Research, 47*(4), 699–712. doi: 10.1509/jmkr.47.4.699. Abgerufen am 28.07.2024.

Hwang, H. & Takane, Y. (2014). Generalized Structured Component Analysis. *Psychometrika, 69*(1), 81–99. doi: 10.1201/b17872. Abgerufen am 28.07.2024.

Ivaturi, K. & Janczewski, L. (2012). *A Typology of Social Engineering Attacks – An Information Science Perspective*. PACIS 2012 Proceedings. Abgerufen am 28.07.2024 von https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1192&context=pacis2012

Jaeger, L. (2018). *Information Security Awareness: Literature Review and Integrative Framework*. Proceedings of the 51st Hawaii International Conference on System Sciences 2018. Abgerufen am 28.07.2024 von https://pdfs.semanticscholar.org/5ae3/6dbae54c62629ab6be0201594f27ed74ad47.pdf

Jameson, F. (1991). *Postmodernism or The Cultural Logic of Late Capitalism*. London: Verso.

Jarvis, C., MacKenzie, S. & Podsakoff, P. (2003). A Critical Review of Construct lndicators and Measurement Model Misspecification in Marketing and Consumer Research. *Journal of Consumer Research, 30*(2), 199–218. doi: 10.1086/376806. Abgerufen am 28.07.2024.

Jeon, S., Kim, Y.-G. & Koh, J. (2011). An integrative model for knowledge sharing in communities-of-practice. *Journal of Knowledge Management, 15*(2), 251–269. doi: 10.1108/13673271111119682. Abgerufen am 28.07.2024.

Johnson, R. B., Onwuegbuzie, A. J. & Turner, L. A. (2007). Toward a definition of mixed methods research. *Journal of Mixed Methods Research, 1*(2), 112–133. doi: 10.1177/1558689806298224. Abgerufen am 28.07.2024.

Jonas, K. & Doll, J. (1996). Eine kritische Bewertung der Theorie überlegten Handelns und der Theorie geplanten Verhaltens. *Zeitschrift für Sozialpsychologie, 27*(1), 18–31. Abgerufen am 28.07.2024 von https://www.researchgate.net/publication/279851059_Eine_kritische_Bewertung_der_Theorie_uberlegten_Handelns_und_der_Theorie_geplanten_Verhaltens

Kankanhalli, A., Teo, H.-H., Tan, B. C. Y. & Wei, K.-K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management, 23*(2), 139–154. doi: 10.1016/S0268-4012(02)00105-6. Abgerufen am 28.07.2024.

Karjalainen M. (2011). *Improving employees' information systems (IS) security behaviour: Toward a meta-theory of is security training and a new framework for understanding employees' is security behaviour*. PhD. Oulu: The University of Oulu (A 579).

Karner, T. (1993). *Eine empirische Anwendung des Modells von Müller für kontinuierliche Antwortskalen (mittels des computerisierten Meyer-Briggs-Typenindikator)*. Unveröffentlichte Dissertation, Universität Wien.

Kelle, U. (2007). *Die Integration qualitativer und quantitativer Methoden in der empirischen Sozialforschung*. Wiesbaden: VS Verlag.

Kerlinger, F. M. (1975). *Grundlagen der Sozialwissenschaften*. Weinheim: Beltz.

Kerres, M., Bormann, M. & Vervenne, M. (2009). Didaktische Konzeption von Serious Games: Zur Verknüpfung von Spiel- und Lernangeboten. *Medien Pädagogik. Zeitschrift für Theorie und Praxis der Medienbildung*. Abgerufen am 28.07.2024 von https://learninglab.uni-due.de/sites/default/files/kerres0908_0.pdf

Keyworth, M. (2016). *Vishing and smishing: The rise of social engineering fraud*. Business reporter, BBC World Service. Abgerufen am 17.02.2022 von https://www.bbc.com/news/business-35201188

Khan, B., Alghabar, K., Khan, M. K. & Nabi, S. I. (2011). Effectiveness of information security awareness methods based on psychological theories. *African Journal of Business Management, 5*(26), 10862–10868. doi: 10.5897/AJBM11.067. Abgerufen am 28.07.2024 von https://www.researchgate.net/publication/267805604_Effectiveness_of_information_security_awareness_methods_based_on_psychological_theories

Kim, M.-S. & Hunter, J. E. (1993). Attitude-behavior relations: A meta-analysis of attitudinal relevance and topic. *Journal of Communication, 43*(1), 101–141. doi: 10.1111/j.1460-2466.1993.tb01251.x. Abgerufen am 28.07.2024.

Kim S., Yang K. H. & Park S. (2014). An integrative behavioral model of information security policy compliance. *The Scientific World Journal*. doi: 10.1155/2014/463870. Abgerufen am 28.07.2024.

Kirby, D. (1985). Sexuality education: A more realistic view of its effects. *Journal of School Health, 55*(10), 421–424. doi: 10.1111/j.1746-1561.1985.tb01169.x. Abgerufen am 28.07.2024.

Kirk, J. & Miller, M. L. (1986). *Reliability and validity in qualitative research*. Sage university paper series on qualitative research methods, Vol. 1. Beverly Hills, CA: Sage.

Klauer, K. J. (1975). *Intelligenztraining im Kindesalter*. Weinheim: Beltz.

Kleinjohann, M. & Reinecke, V. (2020). Marketing-kommunikation mit der Generation Z. Erfolgsfaktoren für das Marketing mit Digital Natives. Wiesbaden: Springer.

König, M. (2019). *Gesprächskompetenzen Auszubildender fördern Konzeption und Wirkung eines Lernarrangements in einer gewerblich-technischen Berufsausbildung*. Bielefeld: wbv Media GmbH & Co. KG.

Koolwijk, J. van (1975). *Techniken der empirischen Sozialforschung Untersuchungsformen* (Reprint 2015 Ausgabe). München: De Gruyter Oldenbourg.

Korn, O. (2011). Potenziale und Fallstricke bei der spielerischen Kontextualisierung von Lernangeboten. In M. Metz & F. Theis (Hg.), *Digitale Lernwelt – Serious Games. Einsatz in der beruflichen Weiterbildung* (S. 15–27). Bielefeld: W. Bertelsmann Verlag.

Krafft, M., Götz, O. & Liehr-Gobbers, K. (2005). Die Validierung von Strukturgleichungsmodellen mit Hilfe des Partial-Least-Squares (PLS)-Ansatz. In F. Bliemel, A. Eggert, G. Fassott & J. Henseler (Hg.), *Handbuch PLS-Pfadmodellierung – Methode, Anwendung, Praxisbeispiele* (S. 71–116). Stuttgart: Schäffer-Poeschel.

Krathwohl, D. von., Bloom, B. & Masia B. B. (1975). *Taxonomie von Lernzielen im affektiven Bereich*. Weinheim: Beltz.

Kritzinger, E. & Smith, E. (2008). Information security management: An information security retrieval and awareness model for industry. *Computers & Security, 27*(5–6), 224–231. doi: 10.1016/j.cose.2008.05.006. Abgerufen am 28.07.2024.

Kriz, W.-C. (2010). Mit Planspielen den Wandel in Organisationen professionell gestalten. In F. Trautwein, S. Hitzler S. & B. Zürn (Hg.), *26. Europäisches Planspielforum „Trends und Effizienz beim Planspieleinsatz" – Tagungsunterlagen*. Stuttgart: ZMS DHWB.

Krüger, H. (1983). Gruppendiskussionen. Überlegungen zur Rekonstruktion sozialer Wirklichkeit aus der Sicht der Betroffenen. *Soziale Welt, 34*(1), 90–109. Abgerufen am 28.07.2024 von https://www.jstor.org/stable/40877374

Krüger, H. & Vogt, H. (2007). *Theorien in der biologiedidaktischen Forschung. Ein Handbuch für Lehramtsstudenten und Doktoranden*. Berlin, Heidelberg: Springer-Verlag. doi: 10.1007/978-3-540-68166-3. Abgerufen am 28.07.2024.

Kruger, H. A. & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security, 25*(4), 289–296. doi: 10.1016/j.cose.2006.02.008. Abgerufen am 28.07.2024.

Kruse, J. (2015). *Qualitative Interviewforschung. Ein integrativer Ansatz (Grundlegende Methode)* (2., überarbeitete und ergänzte Auflage). Weinheim: Beltz.

Kuhalampi, M. (2017). *Impact of deterrence theory methods on employees' information security behaviour*. Jyväskylän yliopiston informaatioteknologian tiedekunta. Jyväskylä: University of Jyväskylä, Information Systems, Bachelor's thesis. Abgerufen am 28.07.2024 von https://jyx.jyu.fi/bitstream/handle/123456789/53983/URN%3ANBN%3Afi%3Ajyu-201705172387.pdf?sequence=1&isAllowed=y

Kumar, K. (1995). *From Post-Industrial to Post-Modern Society*. Oxford: Blackwells.

Kvale, S. (1986). Validity in the qualitative research Interview. In D. Ashworth, A. Giorgi & A. de Koning (Hg.), *Research methodology in psychology: The qualitative perspective*. Pittsburg: Duquesne University Press.

Lagerberg, D. (1975). *Kontext och funktion. Summary: Contribution to the theory and method of content analysis* (Dissertation). Uppsala, Sweden: University.

Lamnek, S. (1995). *Qualitative Sozialforschung*. Bd. 1. München, Weinheim: Beltz Verlag.

Lamnek, S. (1998). *Gruppendiskussion. Theorie und Praxis*. Weinheim: Beltz Psychologie Verl.-Union.

Lamnek, S. (2005). *Gruppendiskussion. Theorie und Praxis* (2. Auflage). Weinheim, Basel: Beltz Verlag.

Lamnek, S. & Krell, C. (2016). *Qualitative Sozialforschung* (6. Auflage). Weinheim, Basel: Beltz Verlag.

Lang, S. (2010). *Die standardisierte Befragung in der Markt- und Sozialforschung*. Zweibrücken: KV Klein Verlag.

Lebek, B., Uffen, J., Neumann, M., Hohler, B. & Breitner, M. H. (2014). Information security awareness and behavior: A theory-based literature review. *Management Research Review*, *37*(12), 1049–1092. doi: 10.1108/MRR-04-2013-0085. Abgerufen am 28.07.2024.

Lechner, U., Dännart, S., Rieb, A. & Rudel, S. (2018). *Fallstudien zur IT-Sicherheit in Kritischen Infrastrukturen*. Universität der Bundeswehr München.

Lee, S. M., Lee, S.-G. & Yoo. S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. *Information Management*, *41*(6), 707–718. doi: 10.1016/j.im.2003.08.008. Abgerufen am 28.07.2024.

Liebig, B. & Nentwig-Gesemann, I. (2009). Gruppendiskussion. In S. Kühl, P. Strodtholz & A. Taffertshofer (Hg.), *Handbuch Methoden der Organisationsforschung. Quantitative und Qualitative Methoden* (S. 102–123). Wiesbaden: VS Verlag.

Liebold, R. & Trinczek, R. (2009). Experteninterview. In S. Kühl, P. Strodtholz & A. Taffertshofer (Hg.), *Handbuch Methoden der Organisationsforschung* (S. 32–56). Wiesbaden: VS Verlag. doi: 10.1007/978-3-531-91570-8_3. Abgerufen am 28.07.2024.

Lisch, R. (1978). Stichproben. In R. Lisch & J. Kritz (Hg.), *Grundlagen und Modelle der Inhaltsanalyse* (S. 56–68). Reinbek: Rowohlt.

Littig, B. & Wallace, C. (1997). *Möglichkeiten und Grenzen von Fokus-Gruppendiskussionen für die sozialwissenschaftliche Forschung* (Reihe Soziologie/Institut für Höhere Studien, Abt. Soziologie, 21). Wien: Institut für Höhere Studien (IHS). Abgerufen am 31.03.2022 von https://www.ssoar.info/ssoar/handle/document/22202

Lohmöller, J. B. (1989). *Latent Path Modelling with Partial Least Squares*. Heidelberg: Physica-Verlag.

Malzew, M. (2023). *Qualitative oder Quantitative Umfrage: Empirische Forschungsmethoden im direkten Vergleich*. Abgerufen am 17.06.2023 von https://www.empirio.de/empirio wissen/qualitative-und-quantitative-forschungsmethoden

Marr, A. (2010). *Serious Games für die Informations- und Wissensvermittlung. Bibliotheken auf neuen Wegen*. Wiesbaden: Dinges & Frick.

Mayring, P. (2002). *Einführung in die Qualitative Sozialforschung. Eine Anleitung zu qualitativem Denken* (5. Auflage). Weinheim: Beltz.

Mayring, P. (2008). *Qualitative Inhaltsanalyse. Grundlagen und Techniken (*8., aktualisierte und überarbeitete Auflage). Weinheim: Beltz.

Mayring, P (2015). *Qualitative Inhaltsanalyse. Grundlagen und Techniken* (12., aktualisierte und überarbeitete Auflage). Weinheim: Beltz.

McGuire W. J. (1969). *The nature of attitudes and attitude change* (3. Auflage). Reading, MA: Addison-Wesley.

McMahan, A. (2003). Immersion, Engagement, and Presence. A Method for Analyzing 3-D Video Games. In M. Wolf & B. Perron (Hg.), *The Video Game, Theory Reader* (S. 67–86). New York, NY: Routledge, Taylor & Francis Group. Abgerufen am 03.08.2024 von https://www.researchgate.net/publication/284055280_Immersion_engagement_and_presence_A_method_for_analyzing_3-D_video_games

Metz, M. & Theis, F. (2011). Mit Serious Games zum Lernerfolg. In M. Metz & F. Theis (Hg.), *Digitale Lernwelt – Serious Games. Einsatz in der beruflichen Weiterbildung* (S. 69–77). Bielefeld: W. Bertelsmann Verlag.

Meuser, M. & Nagel, U. (2005). Experteninterviews – vielfach erprobt, wenig bedacht. Ein Beitrag zur qualitativen Methodendiskussion. In A. Bogner, B. Littig & W. Menz (Hg.), *Das Experteninterview: Theorie, Methode, Anwendung* (S. 71–94). Wiesbaden: VS-Verlag (Reprint von 1991).

Meuser, M. & Nagel, U. (2009). Das Experteninterview – konzeptionelle Grundlagen und methodische Anlage. In S. Pickel, G. Pickel, G., H.-J. Lauth & D. Jahn (Hg.), *Methoden der vergleichenden Politik- und Sozialwissenschaft* (S. 465–479). Wiesbaden: VS Verlag für Sozialwissenschaften. doi: 10.1007/978-3-531-91826-6_23. Abgerufen am 28.07.2024.

Michael, D. R. & Chen, S. (2006). *Serious Games: Games That Educate, Train and Inform*. Boston: Thomson Course Technology.

Miles, J. (o. J.). *Was ist der Unterschied zwischen formativen und reflektiven Messmodellen?* Abgerufen am 28.07.2024 von https://qastack.com.de/stats/184947/what-is-the-difference-between-formative-and-reflective-measurement-models#:~:text=Ja%2C%20sie%20sind%20sehr%20unterschiedlich.%20Ein%20reflektierendes%20Messmodell,die%20richtige%20Antwort%20auf%20eine%20Frage%20zu%20erhalten

Miller, T. E., Booraem, C., Flowers, J. V. & Iversen, A. E. (1990). Changes in knowledge, attitudes, and behavior as a result of a community-based AIDS prevention program. *AIDS Education and Prevention*, *2*(1), 12–23.

Mostafa, M. & Faragallah, O. S. (2019). Development of Serious Games for Teaching Information Security Courses. *IEEE Access*, *7*, 169293–169305. doi: 10.1109/ACCESS.2019.2955639. Abgerufen am 01.07.2024 von https://ieeexplore.ieee.org/document/8911357

Müller-Lietzkow, J. & Jacobs, S. (2011). Serious Games Games – Theory and Reality. In A. Hoblitz (Hg.), *Serious Games – Theory, Technology & Practice. Proceedings GameDays, 2011, September 12–13* (S. 147–156). Darmstadt: Technische Universtität Darmstadt.

Mummendey, H. D. (2003). *Die Fragebogen-Methode*. Göttinen: Hogrefe.

Muniz, J. & Lakhani, A. (2013). *The Social media deception Project: How We Created Emily Williams to Compromise Our Target*. Abgerufen am 28.07.2024 von http://www.thesecurityblogger.com/fake-social-network-account-owned-you-how-emily-williams-compromised-our-friends-and-employer/

Naqvi, B., Perova, K., Farooq, A., Makhdoom, I., Oyedeji, S. & Porras, J. (2023). Mitigation strategies against the phishing attacks: A systematic literature review. *Computers & Security*, *132*. doi: 10.1016/j.cose.2023.103387. Abgerufen am 28.07.2024.

Nebel, J. (2018). Haftung bei IT-Sicherheitsverstößen. *Frankfurter Allgemeine*. Abgerufen am 27.03.2023 von https://www.faz.net/asv/it-sicherheit-1/haftung-bei-it-sicherheitsverstoessen-15799391.html

Ng, B.-Y, Kankanhalli A. & Xu, Y. (2009). Studying users' computer security behavior: a health belief perspective. *Decision Support Systems*, *46*(4), 815–825. doi: 10.1016/j.dss.2008.11.010. Abgerufen am 28.07.2024.

Nittel-Neubert, A. (o. J.). *Faktorladung – Informatives*. Abgerufen am 21.06.2023 von https://www.helpster.de/faktorladung-informatives_195715

Nitzl, C. (2010). Eine anwenderorientierte Einführung in die Partial Least Square (PLS) Methode. *SSRN Electronic Journal*. doi: 10.2139/ssrn.2097324. Abgerufen am 28.07.2024.

Oerter, R. (1995). Motivation und Handlungssteuerung. In R. Oerter & L. Montada (Hg), *Entwicklungspsychologie* (3. Auflage, S. 758–821). Weinheim: Beltz.

Oevermann, U., Allert, T. & Konau, E. (1980). Zur Logik der Interpretation von Interviewtexten: Fallanalyse anhand eines Interviews mit einer Fernstudentin. In T. Heinze, H. W. Klusemann & H.-G. Soeffner (Hg.), *Interpretation einer Bildungsgeschichte* (S. 15–69). Bensheim: Päd. Extra.

O'Neill, T. A., Hambley, L. A. & Bercovich, A. (2014). Prediction of cyberslacking when employees are working away from the office. *Computers in Human Behavior*, *34*, 291–298. doi: 10.1016/j.chb.2014.02.015. Abgerufen am 28.07.2024.

Pahnila, S., Siponen, M. T. & Mahmood, A. (2007a). *Employees' behavior towards IS security policy compliance*. Proceedings of the 40th Hawaii International Conference on System Sciences, Big Island, 1–10.

Pahnila, S., Siponen, M. T. & Mahmood, A. (2007b). *Which factors explain employees' adherence to information security policies?* An empirical study. Proceedings of the Pacific Asia Conference on Information Systems, Auckland, Paper 73.

Panten, G. & Boßow-Thies, S. (2007). Analyse kausaler Wirkungszusammenhänge mit Hilfe von Partial Least Squares (PLS). In A. Sänke, D. Klapper, U. Konradt, A. Walter & J. Wolf (Hg.), *Methodik der empirischen Forschung* (2., überarbeitete und erweiterte Auflage, S. 311–326). Wiesbaden: Gabler.

Parsons, K., Calic D., Pattinson M., Butavicius M., McCormac, A. & Zwaans T. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. *Computers and Security*, *66*, 40–51. doi: 10.1016/j.cose.2017.01.004. Abgerufen am 28.07.2024.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M. & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers and Security*, *42*, 165–167. doi: 10.1016/j.cose.2013.12.003. Abgerufen am 28.07.2024.

Pelz, R. (2008). Empirische Untersuchung. *In Anzeigenmarketing im Verlag. Eine empirische Analyse der Marketingressourcen und Marketingkompetenzen im Anzeigenmarketing von Zeitschriftenverlagen* (S. 139–247). Wiesbaden: Gabler Verlag | Springer Fachmedien Wiesbaden GmbH. doi: 10.1007/978-3-8350-5568-1_4. Abgerufen am 28.07.2024.

Pew, R. W. (2000). The state of situation awareness measurement: Heading toward the next century. In M. R. Endsley & D. J. Garland (Hg.), *Situation awareness and measurement* (S. 33–47). Mahwah: Lawrence Erlbaum Associates Inc.

Pew, R. W. & Mavor, A. (1998). *Modeling Human and Organizational Behaviour*. Washington: National Academy of Sciences Press.

Pfeiffer, R. (2023). *Gruppendiskussion für die wissenschaftliche Arbeit + Beispiele*. Abgerufen am 28.07.2024 von https://www.scribbr.de/methodik/gruppendiskussion/

Phishing-Kampagne der Volkswagen AG. (2019). *Eine interne Phishing-Kampagne der Volkswagen AG*. Unveröffentlichter Bericht von Volkswagen AG.

Piquero, A. & Tibbetts, S. (1996). Specifying the direct and indirect effects of low self-control and situational factors in offenders' decision making: Toward a more complete model of rational offending. *Justice Quarterly, 13*(3), 481–510. doi: 10.1080/07418829600093061. Abgerufen am 28.07.2024.

Pixabay. Abgerufen am 27.07.2024 von https://pixabay.com/de/images/search/

Pöge, A. (2008). Persönliche Codes „reloaded". *Methoden – Daten – Analysen, 2*(1), 59–70. Abgerufen am 28.07.2024 von https://www.gesis.org/fileadmin/upload/forschung/publikationen/zeitschriften/mda/Vol.2_Heft_1/2008_MDA1_Poege.pdf

Pokoyski D. (2009). Security Awareness: Von der Oldschool in die Next Generation – eine Einführung. In M. Helisch & D. Pokoyski (Hg.), *Security Awareness. Neue Wege zu erfolgreichen Mitarbeiter-Sensibilisierung* (S. 1–8). Wiesbaden: Vieweg+Teubner.

PricewaterhouseCoopers. (2013). *Changing the game – key findings from the global state of information security survey 2013*. Bericht veröffentlicht von PricewaterhouseCoopers.

Pryazhnykova, N. (2018). *Lernkonzept „Serious Games" in der betrieblichen Aus- und Weiterbildung. Eine qualitative Untersuchung am Beispiel Volkswagen AG*. Masterarbeit. Unveröffentlichtes Manuskript. Otto-von-Guericke-Universität Magdeburg.

Raczkowski F. (2016). *Digitalisierung des Spiels. Games, Gamification und Serious Games*. Dissertation. Ruhr Universität Bochum. Abgerufen am 28.07.2024 von: https://d-nb.info/1121909310/34

Raithel, J. (2006). *Quantitative Forschung. Ein Praxiskurs* (1. Auflage). Wiesbaden: GWV Fachverlage GmbH.

Ratan R. & Ritterfeld U. (2009). Classifying Serious Games. In U. Ritterfeld, M. Cody & P. Vorderer (Hg.), *Serious Games. Mechanisms and Effects* (S. 10–24). New York, London: Routledge. doi: 10.4324/9780203891650. Abgerufen am 28.07.2024.

Rauch, N. (2009). *Ein verhaltensbasiertes Messmodell zur Erfassung von Situationsbewusstsein im Fahrkontext*. Würzburg: Psychologisches Institut der Universität Würzburg Lehrstuhl III – Methodenlehre und Verkehrspsychologie. Abgerufen am 28.07.2024 von: https://d-nb.info/995681015/34

Raza, M., Iqbal, M., Sharif, M. & Haider, W. (2012). A Survey of Password Attacks and Comparative Analysis on Methods for Secure Authentication. *World Applied Sciences Journal, 19*, 439–444. doi: 10.5829/idosi.wasj.2012.19.04.1837. Abgerufen am 28.07.2024 von https://www.researchgate.net/publication/236898951_A_Survey_of_Password_Attacks_and_Comparative_Analysis_on_Methods_for_Secure_Authentication

Regorz, A. (2023). *SEM: Reflektive und formative Messmodelle*. Abgerufen am 28.07.2024 von http://www.regorz-statistik.de/inhalte/pls_sem_3.html

Reinartz, W., Haenlein, M. & Henseler, J. (2009). An empirical comparison of the efficacy of covariance-based and variance-based SEM. *International Journal of Research in Marketing, 26*(4), 332–344. doi: 10.1016/j.ijresmar.2009.08.001. Abgerufen am 28.07.2024.

Reinders, H., Ditton, H., Gräsel, C. & Gniewosz, B. (2011). *Empirische Bildungsforschung: Strukturen und Methoden*. Wiesbaden: VS Verlag für Sozialwissenschaften.

Rhee, H.-S., Ryu, Y. U. & Kim, C.-T. (2005). *I Am Fine but You Are Not: Optimistic Bias and Illusion of Control on Information Security.* Proceedings of the 26th International Conference, Las Vegas, NV. Abgerufen am 28.07.2024 von https://www.researchgate.net/publication/221599035_I_Am_Fine_but_You_Are_Not_Optimistic_Bias_and_Illusion_of_Control_on_Information_Security

Ries, A. (2012). *Serious Games in der Wissensvermittlung. Wenn die Grenzen zwischen virtueller und realer Welt verschmelzen*. Norderstedt: Grin Verlag.

Ringle, C. (2004). Gütemaße des Partial Least Square-Ansatzes zur Bestimmung von Kausalmodellen. *Arbeitspapier Nr. 16 des Instituts für Industriebetriebslehre und Organisation*. Universität Hamburg. Abgerufen am 28.07.2024 von https://www.academia.edu/6759883/G%C3%BCtema%C3%9Fe_f%C3%BCr_den_Partial_Least_Squares_Ansatz_zur_Bestimmung_von_Kausalmodellen

Ringle, C. M., Boysen, N., Wende, S. & Will, A. (2006). Messung von Kausalmodellen mit dem Partial-Least-Squares-Verfahren. *Das Wirtschaftsstudium,* Zeitschrift für Ausbildung, Prüfung, Berufseinstieg und Fortbildung, *35*(1), 81–87.

Ringle, C. M., Sarstedt, M. & D. W. Straub (2012). Editor's Comments: A Critical Look at the Use of PLS-SEM in MIS Quarterly. *MIS Quarterly, 36*(1), 3–14. doi: 10.2307/41410402. Abgerufen am 28.07.2024.

Ringle, C. & Spreen, F. (2007). Beurteilung der Ergebnisse von PLS-Pfadanalysen. *Das Wirtschaftsstudium,* Zeitschrift für Ausbildung, Prüfung, Berufseinstieg und Fortbildung, *36*(2), 211–216.

Ringle, C. M., Wende, S. & Becker, J.-M. (2020). *SmartPLS 4 (Version 4.0.9.4.)*. Bönningstedt: SmartPLS. Abgerufen am 18.02.2022 von https://www.smartpls.com

Roch, S. (2017). Der Mixed-Methods-Ansatz. In J. Winkel, W. Fichten & K. Großmann (Hg.), *Forschendes Lernen an der Europa-Universität Flensburg – Erhebungsmethoden* (S. 95–210). Abgerufen am 12.09.2019 von https://www.researchgate.net/publication/320877887_Der_Mixed-Methods-Ansatz

Römer, E., Schuberth, F. & Henseler, J. (2021). HTMT2 – An improved criterion for assessing discriminant validity in structural equation modeling. *Industrial Management & Data Systems, 121,* 2637–2650. doi: 10.1108/IMDS-02-2021-0082. Abgerufen am 28.07.2024.

Rönkkö, M. & Evermann, J. (2013). A critical examination of common beliefs about partial least squares path modeling. *Organizational Research Methods, 16*(3), 425–448. doi: 10.1177/1094428112474693. Abgerufen am 28.07.2024.

Rost, J. (2004). *Lehrbuch Testtheorie – Testkonstruktion*. (2., vollständig überarbeitete und erweiterte Auflage). Bern: Verlag Hans Hubert.

Rouse, G. (2022). *Common Types of Social Engineering Attacks*. Abgerufen am 28.07.2024 von https://www.datto.com/blog/5-types-of-social-engineering-attacks

Roy, T. K., Acharya, R. & Roy, A. (2016). *Statistical Survey Design and Evaluating Impact*. Cambridge: Cambridge University Press.

Rudel, S. & Rieb, A. (2017). Technik vs. Mensch: Was nutzt ein hoher technischer Standard, wenn die Schwachstelle Mensch umgangen wird? In Bundesamt für Sicherheit in der Informationstechnik (Hg.), *Digitale Gesellschaft zwischen Risikobereitschaft und Sicherheitsbedürfnisse* (S. 345–352). Tagungsband zum 15. Deutschen IT-Sicherheitskongress, 16.-18.5.2017 in Bonn.

Ryan, T. (2010). *Getting In Bed with Robin Sage*. Abgerufen am 28.07.2024 von http://media.blackhat.com/bh-us-10/whitepapers/Ryan/BlackHat-USA-2010-Ryan-Getting-In-Bed-With-Robin-Sage-v1.0.pdf

Saad, A., Liebers, J., Schneegass, S. & Gruenefeld, U. (2023). They see me scrollin – Lessons Learned from Investigating Shoulder Surfing Behavior and Attack Mitigation Strategies. In N. Gerber, A. Stöver, K. Marky (Hg.). *Human Factors in Privacy Research* (S. 199–218). Cham: Springer. doi: 10.1007/978-3-031-28643-8_10. Abgerufen am 28.07.2024.

Sacks, H. (1992). *Lectures on conversation*. Herausgegeben von G. Jefferson. Oxford, UK: Blackwell.

Safa, S. N. & Solms, R. von (2016). An information security knowledge sharing model in organizations. *Computers in Human Behavior, 57*, 442–451. doi: 10.1016/j.chb.2015.12.037. Abgerufen am 02.07.2024.

San Nicolas-Rocca T., Schooley B. & Spears J. L. (2014). *Designing effective knowledge transfer practices to improve is security awareness and compliance*. 47th Hawaii International Conference on System Sciences (HICSS). doi: 10.1109/HICSS.2014.427. Abgerufen am 02.07.2024 von https://ieeexplore.ieee.org/abstract/document/6759029

Sarter, N. B. & Woods, D. D. (1995). How in the world did we ever get in that mode? Mode error and awareness in supervisory control. *The Journal of the Human Factors and Ergonomics Society, 37*(1), 5–19. doi: 10.1518/001872095779049516. Abgerufen am 28.07.2024.

Sawyer, B. (2004). *The „Serious Games" Landscape*. Presentation at Serious Games Summit: Game Developers Conference, 2004, San Jose, 22–26.

Schaub, H. & Zenke, K. G. (2007). *Wörterbuch der Pädagogik*. München: Dt. Taschenbuch-Verlag. Abgerufen am 28.07.2024 von https://beckassets.blob.core.windows.net/product/readingsample/117059/9783423343466_excerpt_001.pdf

Schegloff, E. A. (1984). On Some Questions and Ambiguities in Conversation. In J. A. Maxwell & J. Heritage (Hg.), *Structures of Social Actions. Studies in Conversation Analysis* (S. 28–52). Cambridge: Cambridge University Press.

Schmidt, H., Gondolf, J. & Haufs-Brusberg, P. (2018). *Studie zur Information Security Awareness in kleinen und mittleren Unternehmen (KMU)*. Hochschule Düsseldorf. doi: 10.20385/2625-3690/2018.1. Abgerufen am 28.07.2024.

Schnell, R., Hill, P. B. & Esser, E. (2005). *Methoden der empirischen Sozialforschung*. München: Oldenbourg.

Schloderer, M., Ringle, C. & Sarstedt, M. (2009). Einführung in varianzbasierte Strukturgleichungsmodellierung: Grundlagen, Modellevaluation und lnteraktionseffekte am Beispiel von SmartPLS. In A. Meyer & M. Schwaiger (Hg.), *Theorien und Methoden der Betriebswirtschaft* (S. 583–611). München: Vahlen.

Scholderer, J. & Balderjahn, I. (2005). PLS versus LISREL: Ein Methodenvergleich. In F. Bliemel, A. Eggert, G. Fassott & J. Henseler (Hg.), *Handbuch PLS-Pfadmodellierung – Methode, Anwendung, Praxisbeispiele* (S. 87–98). Stuttgart: Schäffer-Poeschel.

Scholderer, J. & Balderjahn, I. (2006). Was unterscheidet harte und weiche Strukturgleichungsmodelle nun wirklich? Ein Klärungsversuch zur LISREL-PLS-Frage. *Marketing – Zeitschrift für Forschung und Praxis, 28*(1), 57–70. doi: 10.15358/0344-1369-2006-1-57. Abgerufen am 28.07.2024.

Scholl, M. (2018a). *Information Security Awareness in Public Administrations (Provisional chapter)*. Ubaldo Comite, Public Management and Administration. Open Access: INTECH d. d. o. Rijeka (InTechOpen). doi: 10.5772/intechopen.74572. Abgerufen am 28.07.2024.

Scholl, M. (2018b). Play the Game! Analogue Gamification for Raising Information Security Awareness. *The Open Cybernetics & Systemics Journal, 16*(3), 32–35. Abgerufen am 17.02.2022 von https://www.researchgate.net/publication/328428842_Play_the_Game#full-text

Schöneck, N. M. & Voß, W. (2005). *Das Forschungsprojekt. Planung, Durchführung und Auswertung einer quantitativen Studie*. Wiesbaden: VS Verlag.

Schons, J. (2009). *Das narrative und problemzentrierte Interview: Eine Gegenüberstellung*. Grin Verlag GmbH.

Schrader, C. (2010). Computerbasierte Lernspiele – Stand der Forschung. In S. Ganguin & B. Hoffmann (Hg.), *Digitale Spielkultur* (S. 179–190). München: Schriftenreihe zur Medienpädagogik.

Schrader, P. G. & Lawless, K. (2004). The knowledge, attitudes & behaviors approach how to evaluate performance and learning in complex environments. *Performance Improvement, 43*(9), 8–15. doi: 10.1002/pfi.4140430905. Abgerufen am 28.07.2024 von https://www.researchgate.net/publication/229542766_The_knowledge_attitudes_behaviors_approach_how_to_evaluate_performance_and_learning_in_complex_environments

Schütz, A. & Weber, K. (2017). *Security Awareness: Nicht nur schulen – überzeugen Sie!* Conference: DACH Security 2017. Abgerufen am 17.02.2022 von https://www.researchgate.net/publication/319511331_Security_Awareness_Nicht_nur_schulen_-_uberzeugen_Sie

Seipel, C. & Rieker, P. (2003). *Integrative Sozialforschung*. Weinheim u. München: Juventa.

Shen, C., Yu, T., Xu, H, Yang, G. & Guan, X. (2016). User practice in password security: An empirical study of real-life passwords in the wild. *Computers & Security, 61*, 130–141. doi: 10.1016/j.cose.2016.05.007. Abgerufen am 28.07.2024.

Sieger, H. (2019). Passwort-Management: Nach wie vor entscheidend für IT-Sicherheit. *Digital Business Cloud*. Abgerufen am 28.07.2024 von https://www.digitalbusiness-cloud.de/passwort-management-nach-wie-vor-entscheidend-fuer-it-sicherheit/

Slawinski, N. (2005). *Die Wahl qualitativer Forschungsmethoden*. Abgerufen am 28.07.2024 von https://www.barrierefreies-webdesign.de/spezial/internet-hoeren-und-fuehlen/wahl-qualitativer-forschungsmethoden.html

Smith, K. & Hancock, P. A. (1995). Situation Awareness Is Adaptive, Externally Directed Consciousness. *Human Factors: The Journal of the Human Factors and Ergonomics Society, 37*(1), 137–148. doi: 10.1518/001872095779049444. Abgerufen am 28.07.2024.

Sniehotta, F., Presseau, J. & Araújo-Soares, V. (2014). Time to retire the theory of planned behaviour. *Health Psychology Review, 8*(1), 1–7, doi: 10.1080/17437199.2013.869710. Abgerufen am 28.07.2024.

Spears, J. L. & Barki, H. (2010). User participation in information systems security risk management. *MIS Quarterly, 34*(3), 503–522, doi: 10.2307/25750689. Abgerufen am 28.07.2024.

Stanton J. M., Stam K. R., Mastrangelo P. & Jolton J. (2005). Analysis of end user security behaviors. *Computer Security, 24*(2), 124–133. doi: 10.1016/j.cose.2004.07.001. Abgerufen am 28.07.2024.

Statista Research Department (2022). *Arbeiten Sie ausschließlich an einem festen, vom Arbeitgeber zugewiesenen Arbeitsplatz im Betrieb?* Abgerufen am 28.07.2024 von https://de.statista.com/statistik/daten/studie/1209474/umfrage/verbreitung-mobiler-arbeit/#:~:text=Verbreitung%20mobiler%20Arbeit%202020.%20Ver%C3%B6ffentlicht%20von%20Statista%20Research,mobiler%20Arbeit%20war%20mit%20rund%2040%20Prozent%20verbreitet

Steiner, E. & Bensch, M. (2021). *Der Fragebogen, Von der Forschungsidee zur SPSS-Auswertung* (6. aktualisierte und überarbeitete Auflage). Wien: Faculta Verlags- und Buchhandels AG.

Steiner, G. (2001). Lernen und Wissenserwerb. In A. Krapp & B. Weidenmann (Hg.), *Pädagogische Psychologie* (S. 139–205). Weinheim: Beltz.

Stöcklin N. (2018). Vielfältige Möglichkeiten von Gamification. Framework zur Kategorisierung von Gamification-Ansätzen im Bildungskontext. In T. Junge & C. Schumacher (Hg.), *Digitale Spiele im Diskurs* (S. 1–14). Hagen: Fernuniversität Hagen. Abgerufen am 12.03.2023 von https://www.researchgate.net/publication/326683487_Vielfaltige_Moglichkeiten_von_Gamification_Framework_zur_Kategorisierung_von_Gamification-Ansatzen_im_Bildungskontext

Straub, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research, 1*(3), 255–276. doi: 10.1287/isre.1.3.255. Abgerufen am 28.07.2024 von https://www.researchgate.net/publication/220079472_Effective_IS_Security_An_Empirical_Study

Straub D. W. & Welke R. J. (1998). Coping with systems risk. Security planning models for management decision making. *MIS Quarterly, 22*, 441–469. doi: 10.2307/249551. Abgerufen am 28.07.2024.

Studienretter (o. J.). *Theorie des geplanten Verhaltens*. Abgerufen am 28.07.2024 von https://studienretter.de/theorie-des-geplanten-verhaltens/#Welche%20Variablen%20umfasst%20Die%20Theorie%20Des%20geplanten%20Verhaltens?#:~:text=Die%20Theorie%20beinhaltet%20drei%20unabh%C3%A4ngige%20Variablen

Sutherland, E. H. (1937). *The Professional Thief*. Chicago: University of Chicago Press.

Sutherland, E. H. (1968). Die Theorie der differentiellen Kontakte. In F. Sack & R. König (Hg.), *Kriminalsoziologie* (S. 395–399). Frankfurt am Main: Akademische Verlagsgesellschaft.

Sykes, G. & Matza, D. (1957). Techniques of Neutralization: A Theory of Delinquency. *American Sociological Review, 22*(6), 664–670. doi: 10.2307/2089195. Abgerufen am 28.07.2024.

Talin, B. (2022). Social Engineering & Political Nudges – Änderung des gesellschaftlichen Verhaltens der Bevölkerung in großem Maßstab. *MoreThanDigital*. Abgerufen am 28.07.2024 von https://morethandigital.info/social-engineering-political-nudges-aenderung-des-gesellschaftlichen-verhaltens-der-bevoelkerung-in-grossem-massstab/

Teo, T. S. H., Srivastava, S. C. & Jiang, L. (2008). Trust and electronic government success: an empirical study. *Journal of Management Information Systems, 25*(3), 99–132. doi: 10.2753/MIS0742-1222250303. Abgerufen am 28.07.2024.

Tiwari, A. (2018). *What Is Social Engineering? What Are Different Types of Social Engineering Attacks?* Abgerufen am 28.07.2024 von https://fossbytes.com/what-is-social-engineering-types-techniques/

Tolks, D. & Lampert, C. (2016). Abgrenzung von Serious Games zu anderen Lehr- und Lernkonzepten. In K. Dadaczynski, S. Schiemann & P. Paulus (Hg.), *Gesundheit spielend fördern. Potenziale und Herausforderungen von digitalen Spieleanwendungen für die Gesundheitsförderung und Prävention* (S. 191–217). Weinheim: Beltz Verlag.

Trang, S. & Brendel, A. (2019). A Meta-Analysis of Deterrence Theory in Information Security Policy Compliance Research. *Information Systems Frontiers, 21*, 1265–1284. doi: 10.1007/s10796-019-09956-4. Abgerufen am 28.07.2024.

Trickel, E., Disperati, F., Gustafson, E., Kalantari, F., Mabey, M., Tiwari, N., Safaei, Y., Doupé, A. & Vigna G. (2017). *Shell we play a game? CTF-as-a-service for security education*. USENIX Workshop on Advances in Security Education (ASE 2017), Vancouver, BC: USENIX Association. Abgerufen am 28.07.2024 von https://sites.cs.ucsb.edu/~vigna/publications/2017_ASE_SWPAG.pdf

Tsohou, A., Karyda, M., Kokolakis, S. & Kiountouzis, E. (2015). Managing the introduction of information security awareness programmes in organisations. *European Journal of Information Systems, 24*(1), 38–58. doi: 10.1057/ejis.2013.27. Abgerufen am 28.07.2024.

Turner, B. S. (1990). *Theories of Modernity and Postmodernity*. California, London and New Delhi: Sage.

Unger T., Goossens, J. & Becker, L. (2015). Digitale Serious Games. In U. Blötz (Hg.), *Planspiele und Serious Games in der beruflichen Bildung. Auswahl, Konzepte, Lernarrangements, Erfahrungen – Aktueller Katalog für Planspiele und Serious Games 2015* (S. 157–184). Bielefeld: W. Bertelsmann.

Vance A. (2010). *Why do employees violate is security policies? Insights from multiple theoretical perspectives*. PhD. Oulu: The University of Oulu. Abgerufen am 28.07.2024 von https://oulurepo.oulu.fi/handle/10024/36060

Vance, A., Lowry, P. B. & Eggett, D. (2015). Increasing accountability through user-interface design artifacts: A new approach to addressing the problem of access-policy violations. *MIS Quarterly*, *39*(2), 345–366. doi: 10.25300/MISQ/2015/39.2.04. Abgerufen am 28.07.2024.

Vance. A., Siponen M. & Pahnila S. (2012). Motivating IS Security Compliance: Insights from Habit and Protection Motivation Theory. *Information and Management*, *49*(3/4), 190–198. doi: 10.1016/j.im.2012.04.002. Abgerufen am 28.07.2024.

Venkatraman, S., Cheung, M. K. C., Lee, Z. W. Y., Davis, F. D. & Venkatesh, V. (2018). The "Darth" Side of Technology Use: An Inductively Derived Typology of Cyberdeviance. *Journal of Management Information Systems*, *35*(4), 1060–1091. doi: 10.1080/07421222.2018.1523531. Abgerufen am 28.07.2024.

Verizon Data Breach Investigations Report (2019). *Results and analysis*. Abgerufen am 12.03.2023 von https://www.verizon.com/business/resources/reports/dbir/2019/results-and-analysis/

Vogl, S. (2015). *Interviews mit Kindern führen: eine praxisorientierte Einführung*. Weinheim, Basel: Beltz Juventa.

Vroom, R. & Solms, R. von (2004). Towards information security behavioural compliance. *Computers & Security*, *23*, 191–198. doi: 10.1016/j.cose.2004.01.012. Abgerufen am 28.07.2024.

Wagner, H. & Schönhagen, P. (2009). Die Gruppendiskussion: Von der Erschließung kollektiver Erfahrungsräume. *Qualitative Methoden der Kommunikationswissenschaft* (3. Auflage, S. 273–304). Abgerufen am 28.07.2024 von https://docplayer.org/32009351-Die-gruppendiskussion-von-der-erschliessung-kollektiver-erfahrungsraeume.html

Waterman, S. (2010). Fictitious femme fatale fooled cybersecurity. *The Washington Times*. Abgerufen am 28.07.2024 von https://www.washingtontimes.com/news/2010/jul/18/fictitious-femme-fatale-fooled-cybersecurity/

Wechselberger, U. (2009). Eine theoretische Überlegung über das pädagogische Potential digitaler Lernspiele. In T. Bevc & H. Zapf (Hg.), *Wie wir spielen, was wir lernen* (S. 95–111). Konstanz: UVK. Abgerufen am 28.07.2024 von http://www.ulrichwechselberger.de/wp-content/uploads/2009/03/ueberlegungen_2008.pdf

Weiber, R. & Mühlhaus, D. (2010). *Strukturgleichungsmodellierung: Eine anwendungsorientierte Einführung in die Kausalanalyse mit Hilfe von AMOS, SmartPLS, und SPSS*. Berlin u. Heidelberg: Springer.

Weiber, R. & Mühlhaus, D. (2014). *Strukturgleichungsmodellierung: Eine anwendungsorientierte Einführung in die Kausalanalyse mit Hilfe von AMOS, SmartPLS und SPSS* (2. Auflage). Heidelberg: Springer.

Weidenhammer, A. (2023). *Social Engineering*. Dresdener Institut für Datenschutz. Abgerufen am 28.07.2024 von https://www.dids.de/social-engineering/#more-19544

Werbach, K. & Hunter, D. (2012). *For the win: How game thinking can revolutionize your business*. Philadelphia: Wharton Digital Press.

Whitty, M. T. & Carr, A. N. (2006). New rules in the workplace: Applying object-relations theory to explain problem internet and email behaviour in the workplace. *Computers in Human Behavior, 22*(2), 235–250. doi: 10.1016/j.chb.2004.06.005. Abgerufen am 28.07.2024.

Wiant, T. L. (2003). *Policy and its impact on medical record security.* Unpublished doctoral dissertation. Lexington: University of Kentucky. doi: 10.5555/936569. Abgerufen am 28.07.2024.

Wickert, C. (2018). *Neutralisierungsthese (Sykes und Matza)*. Abgerufen am 28.07.2024 von https://soztheo.de/kriminalitaetstheorien/lernen-subkultur/neutralisierungsthese-sykes-und-matza/

Williams, K. R. & Hawkins, R. (1986). Perceptual Research on General Deterrence: A Critical Review. *Law & Society Review, 20*(4), 545–572. doi: 10.2307/3053466. Abgerufen am 28.07.2024.

Witzel, A. (2000). Das problemzentrierte Interview. *Forum: Qualitative Sozialforschung/ Qualitative Social Research, 1*(22). Abgerufen am 28.07.2024 von http://www.qualitative-research.net/index.php/fqs/article/view/1132/2520

Wold, H. (1980). Model construction and evaluation when theoretical knowledge is scarce: Theory and application of partial least squares. In K. Kmenta & J. Ramsey (Hg.), *Evaluation of econometric models* (S. 47–74). New York: Academic Press.

Wolf, S. (2008). *Der Methodenstreit quantitativer und qualitativer Sozialforschung unter besonderer Berücksichtigung der grundlegenden Unterschiede beider Forschungstraditionen*. Abgerufen am 28.07.2024 von http://websquare.imb-uni-augsburg.de/files/Bachelorarbeit_Wolf.pdf

Zyda, M. (2005). From visual simulation to virtual reality to games. *Computer, 38*(9), 25–32. IEEE. doi: 10.1109/MC.2005.297. Abgerufen am 28.07.2024.

Anhängeverzeichnis[2]

2 Aufgrund ihres großen Datenvolumens befinden sich alle Anhänge dieser Arbeit online unter https://www.wbv.de/isbn/9783763974122 unter dem Punkt ZUSATZMATERIAL kostenfrei heruntergeladen werden.

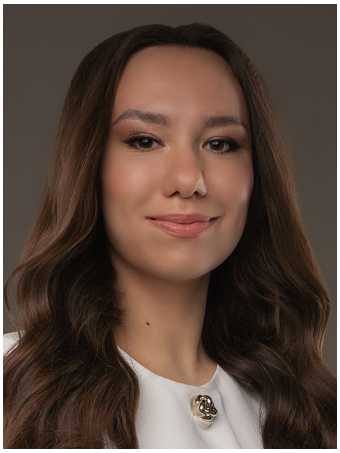
Abkürzungsverzeichnis

AL	Authentic Learning (authentisches Lernen)
CERT	Computer Emergency Response Team. Interne Abteilung, die sich mit den Fragen der Cybersicherheit beschäftigt
BSI	Bundesamts für Sicherheit in der Informationstechnik
DEV	Durchschnittlich erfasste Varianz
EHDD	Enterprise Helpdesk Deutschland. Firma, die Call-Center-Dienstleistungen zu Themen wie z. B. Passwörter, Software oder Zugänge anbietet
FB	Facebook (soziales Netzwerk)
HAIS-Q-Studie	Studie „Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)“
HTMT	Heterotrait-monotrait ratio
IT	Informationstechnik
KAB-Modell	Knowledge-Attitude-Behaviour-Modell (Wissen-Einstellung-Verhalten-Modell)
KR	Konstruktreliabilität
MA	Mitarbeiter
o. J.	ohne Jahr
u. a.	Unter anderem

Abbildungsverzeichnis

Tabellenverzeichnis

Autorin



Frau Dr.in Natalya Pryazhnykova wurde in Donezk, Ukraine, geboren. An der Nationalen Universität Donezk studierte sie von 2010 bis 2014 Translationswissenschaft (Englisch/Ukrainisch). Seit 2014 lebt Frau Pryazhnykova in Deutschland, wo sie in der Zeit den Master of Science und den Master of Arts sowie im Januar 2025 den Doktortitel in Philosophie an der Otto-von-Guericke-Universität Magdeburg erworben hat. Zurzeit ist sie als Cyber Security Operations Manager bei der Volkswagen AG beschäftigt.

Berufsbildung, Arbeit und Innovation –
Dissertationen und Habilitationen, 79
2024, 236 S., 49,90 € (D)
ISBN 978-3-7639-7652-2
E-Book im Open Access

Jacqueline M.-C. Schmidt

Grundlagenwissen zu Künstlicher Intelligenz von angehenden Lehrkräften

Modellbasierte Testentwicklung und Validierung

In der Dissertation von Frau Dr.in Schmidt wird ausgehend von der zunehmenden Relevanz von Künstlicher Intelligenz (KI) im Rahmen digitaler Transformationsprozesse ein Strukturmodell für KI-bezogene Kompetenzfacetten (angehender) Lehrkräfte im berufsbildenden Bereich entwickelt. Das Wissen zu KI nimmt dabei in Anlehnung an die Professionalisierungsforschung eine zentrale Rolle ein. Im Rahmen der Arbeit wird der Frage nachgegangen, wie das Grundlagenwissen (angehender) Lehrkräfte theoretisch modelliert und empirisch erfasst werden kann. Das entwickelte Testinstrument wurde anhand eines quantitativen Studiendesigns umfassend validiert.

wbv.de/bai

Berufsbildung, Arbeit und Innovation – Dissertationen und Habilitationen, 84
2024, 288 S., 49,90 € (D)
ISBN 9783763977758
E-Book im Open Access

Anne Wagner

Schulentwicklung in der digitalen Transformation

Eine fuzzy-set Qualitative Comparative Analysis schulischer Innovationsprozesse

Die digitale Transformation stellt berufliche Schulen vor erhebliche Herausforderungen. In der Dissertation von Anne Wagner wird untersucht, wie die Implementierung digitaler Bildungstechnologien durch erfolgreiche Schulentwicklungsprozesse gelingen kann. Dabei werden von ihr förderliche und hinderliche Gestaltungsfaktoren betrachtet, um Orientierungswissen für die Gestaltung von Transformationsprozessen zu liefern.

Ein innovativer methodischer Ansatz wird mit der fuzzy-set Qualitative Comparative Analysis (fsQCA) in der Berufs- und Wirtschaftspädagogik etabliert. Das ermöglicht, komplexe Kausalzusammenhänge zu analysieren und zu verstehen, welche Konstellationen von Bedingungen zu bestimmten Ergebnissen führen. Ziel ist es, notwendige und hinreichende Bedingungen für erfolgreiche Schulentwicklungsprozesse zu identifizieren.

Die Arbeit von Anne Wagner bietet wertvolle Erkenntnisse zur erfolgreichen Implementierung digitaler Technologien in Schulen. Sie hebt hervor, dass die digitale Transformation nicht nur technologische Anpassungen erfordert, sondern auch tiefgreifende organisatorische und strukturelle Veränderungen innerhalb der Schulen notwendig sind. Die Ergebnisse der Studie sind sowohl für die Wissenschaft als auch für die Bildungspolitik und schulische Praxis von Bedeutung.

wbv.de/bai

Die Dissertation von Frau Pryazhnykova beleuchtet die Wirksamkeit von Serious Games zur Förderung der Informationssicherheits-Awareness in Unternehmen. Im Fokus steht die spielerische Sensibilisierung der Generation Z bei der Volkswagen AG, um Wissen, Einstellungen und Verhalten im Bereich Cybersecurity nachhaltig zu verbessern.

Die Studie kombiniert qualitative und quantitative Methoden: Experteninterviews und Gruppendiskussionen identifizieren relevante Inhalte und Spielmechaniken. Im Anschluss wird die Wirksamkeit des entwickelten Serious Games in einer empirischen Studie getestet.

Die Publikation richtet sich u. a. IT-Sicherheitsverantwortliche sowie Wissenschaftler:innen im Bereich Informationssicherheit/Game-Based Learning.

Die Reihe **Berufsbildung, Arbeit und Innovation** bietet ein Forum für die grundlagen- und anwendungsorientierte Berufsbildungsforschung. Sie leistet einen Beitrag für den wissenschaftlichen Diskurs über Innovationspotenziale der beruflichen Bildung.

Die Reihe wird herausgegeben von Prof.in Marianne Friese (Justus-Liebig-Universität Gießen), Prof.in Susan Seeber (Georg-August-Universität Göttingen) und Prof. Lars Windelband (Karlsruher Institut für Technologie).

Dr.in Natalya Pryazhnykova, geboren in Donezk (1993), Ukraine, studierte von 2010 bis 2014 Translationswissenschaft (Englisch/Ukrainisch) an der Nationalen Universität Donezk. Seit 2014 lebt sie in Deutschland, wo sie ihren Master of Science, Master of Arts und im Januar 2025 ihren Doktor der Philosophie an der Otto-von-Guericke-Universität Magdeburg erwarb. Aktuell arbeitet sie als Cyber Security Operations Manager bei der Volkswagen AG.

ISBN: 978-3-7639-7411-5

wbv

wbv.de/bai