Fachhochschule Nordwestschweiz
Hochschule für Angewandte Psychologie

Cybersecurity-Awareness

Die spielerische Gestaltung von Cybersecurity – Untersuchung der Effektivität von spielbasierten Ansätzen am Beispiel des Escape-Rooms

BACHELORTHESIS

Juni 2023

Autorin

Malama, Annina

Betreuungsperson

Ruf, Alessia

Praxispartner*in

Breakout Basel

Valentin, Martina

Abstract

In einer zunehmend digitalen Welt ist der Schutz vertraulicher Informationen und Systeme vor Bedrohungen von entscheidender Bedeutung. Angesichts der kontinuierlichen Weiterentwicklung von Angriffsmethoden und der wachsenden Komplexität von Cyberbedrohungen sind innovative und effektive Schulungsansätze erforderlich. Diese Bachelorarbeit untersucht die Wirksamkeit von spielbasierten Ansätzen bei der Vermittlung von Cyberthemen am Beispiel eines Escape-Rooms. Durch den Einsatz qualitativer sozialwissenschaftlicher Methoden wurden sieben Cybersecurity-Experten aus der Schweiz befragt, um Einblicke in die praktische Umsetzung von Awareness-Massnahmen zu gewinnen. Der spielbasierte Ansatz bietet eine einzigartige Möglichkeit, komplexe Themen interaktiv und erlebnisorientiert zu vermitteln. Die Sensibilisierung für Cybersecurity wird von verschiedenen Faktoren beeinflusst, wobei das individuelle Sicherheitsbewusstsein einen wesentlichen Einfluss darstellt. Ausserdem zeigen die Ergebnisse die Bedeutung der Berücksichtigung dieser Faktoren bei der Konzeption und Umsetzung von Schulungsinitiativen im Bereich Cybersecurity.

Anzahl Zeichen im Bericht: 101’142

Anzahl Worte Abstract: 126

Keywords: Cybersecurity, Awareness, Gamification, Escape-Room

Inhaltsverzeichnis

1. Einleitung 5

2. Theoretischer Rahmen 7

2.1 Die Entwicklung von Cybersecurity in der Gesellschaft und im Berufsfeld 7

2.2 Schutz vor Angriffen und die Rolle des menschlichen Verhaltens 8

2.3 Einfluss auf Sicherheitsbewusstsein und -verhalten 9

2.4 Information-Security-Awareness 10

2.5 Gamification 11

2.5.1 Potenziale und Anwendungsbereiche am Beispiel des Escape-Rooms 12

2.5.2 Die Erlebnispyramide von Tarssanen 2009b 13

3. Methodik 19

3.1 Forschungsdesign 19

3.2 Experteninterviews 20

3.3 Datenerhebungsinstrument – Entwicklung Interviewleitfaden 21

3.4 Angaben zur Stichprobe 22

3.5 Ablauf der Datenerhebung 23

3.6 Datenaufbereitung: Transkription 24

3.7 Datenauswertungsmethode 24

4. Ergebnisse 27

4.1 Verständnis und Wissen zu Cybersecurity 27

4.1.1 Bedeutung Cybersecurity 27

4.1.2 Angriffsvektoren für Mitarbeitende 28

4.1.3 Meistgenannte Bedrohungen 29

4.2 Cybersecurity und Awareness 29

4.2.1 Bedeutung von Awareness-Massnahmen 29

4.2.2 Faktoren und potenzielle Einflüsse auf Cybersicherheitsverhalten 30

4.2.3 Herausforderungen bezüglich des Cybersicherheitsverhaltens 31

4.2.4 Cybersicherheitsbewusstsein/interne Vorgehensweisen in Unternehmen 32

4.3 Konkrete Massnahmen zur Awareness 33

4.3.1 Technische Massnahmen 34
4.3.2 Personelle Massnahmen 35

4.4 Gamification als Awareness-Massnahme am Beispiel des Escape-Rooms 36
4.4.1 Vorteile 36
4.4.2 Nachteile 38
4.4.3 Input 38
4.4.4 Herausforderungen 39

5. Diskussion 41

5.1 Zusammenfassung der zentralen Ergebnisse 41

5.2 Interpretation der Ergebnisse 44

5.3 Handlungsempfehlungen 47

5.4 Beschränkungen der Forschung 49

5.5 Ausblick 50

Literaturverzeichnis 52

Abbildungsverzeichnis 54

Tabellenverzeichnis 54

Anhang 56

1. Einleitung

In den letzten Jahren hat die Bedeutung von Cybersecurity aufgrund der steigenden Anzahl von Cyberangriffen und Datenschutzverletzungen erheblich zugenommen (Nationales Zentrum für Cybersicherheit NCSC, 2023). Unternehmen, unabhängig von ihrer Grösse oder Branche, sehen sich mit einem ständig wachsenden Risiko konfrontiert, Opfer von Hackerangriffen zu werden (Clinton & Barrack, 2018). Ein hypothetisches Beispiel eines mittelständischen Unternehmens verdeutlicht die verheerenden Auswirkungen eines solchen Angriffs. Trotz der Implementierung solider Sicherheitsmassnahmen und regelmässiger Schulungen zum Thema Cybersecurity wurde das Unternehmen durch das Fehlverhalten eines Mitarbeiters kompromittiert. Der Mitarbeiter wurde durch eine Phishing-E-Mail dazu verleitet, seine Zugangsdaten auf einer gefälschten Login-Seite einzugeben. Dies ermöglichte es den Hackern, auf das interne Netzwerk zuzugreifen und sensible Kundendaten, Kreditkarten sowie Geschäftsgeheimnisse zu entwenden. Die Folgen dieses Vorfalls waren gravierend: Das Unternehmen verlor das Vertrauen der Kunden, was zu Umsatzeinbussen und Kündigungen führte, zudem wurden Klagen wegen Identitätsdiebstahl und Betrug eingereicht. Dieses Beispiel verdeutlicht die hohe Relevanz der Sensibilisierung von Mitarbeitenden für das Thema Cybersecurity. Untersuchungen von DeCusatis, Gormanly, Alvarico, Dirahoui, McDonough, Sprague, Maloney, Avitable und Mah (2022) sowie von Clinton und Barrack (2018) bestätigten, dass menschliches Versagen die Hauptursache für einen Grossteil der Datenschutzverletzungen ist. Um Mitarbeitende effektiv auf potenzielle Bedrohungen hinzuweisen und ihre Sensibilisierung für Cybersecurity zu erhöhen, sind innovative Schulungsmethoden erforderlich (Löffler, Schneider, Asprion & Zanwar, 2021).

Aktuelle Berichte von Decusatis et al. (2022) deuten darauf hin, dass die derzeitigen Schulungsmethoden für das Bewusstsein von Cybersecurity zentrale Probleme aufweisen. Häufig basieren sie auf passiven Lernmethoden wie Videos oder schriftlichen Vorträgen mit begleitenden Bewertungen oder Quizfragen. Diese Art von Schulungen zeigt jedoch kaum langfristige Auswirkungen, da die Mitarbeitenden Informationen nicht behalten oder Bedrohungen ausserhalb des Schulungskontextes nicht erkennen können (DeCusatis et al., 2022). Dies legt nahe, dass der Bedarf an verbesserten Schulungen zum Thema Cybersecurity besteht, um den Mitarbeitenden zu helfen, Verhaltensweisen zu erkennen

und zu vermeiden, welche die Cybersecurity gefährden könnten (DeCusatis et al., 2022). In diesem Zusammenhang zeigen Escape-Rooms als Methode zur Schulung von Cybersecurity-Awareness vielversprechende Ergebnisse (Palmas & Niermann, 2021). Durch die Integration von realistischen Szenarien und aktuellen Bedrohungen können die Teilnehmenden ein tieferes Verständnis für die Konsequenzen von Sicherheitslücken entwickeln und lernen dadurch, diese zu vermeiden. Um die Wirksamkeit von Escape-Rooms als Methode zur Schulung von Cybersecurity-Awareness zu prüfen, sind nach Palmas und Niermann (2021) die Gestaltung des Escape-Rooms, die Auswahl der Rätsel, die Szenarien und technische Elemente von Bedeutung.

Diese Bachelorarbeit widmet sich der Fragestellung, inwieweit Escape-Rooms als Methode zur Schulung von Cybersecurity-Awareness eingesetzt werden können und welche Rahmenbedingungen zur Wirksamkeit dieser Methode beitragen. Die Arbeit kombiniert eine umfassende Literaturrecherche mit Experteninterviews, um fundierte und praxisnahe Erkenntnisse zu gewinnen. Diese Erkenntnisse sollen einerseits Unternehmen und Organisationen unterstützen, ihre Schulungsmassnahmen zur Cybersecurity zu optimieren, und andererseits dem Praxispartner Breakout Basel aktuelle und relevante Bedingungen für den Einsatz von Escape-Rooms bieten. Durch den Beitrag dieser Arbeit soll das Bewusstsein für Cybersecurity geschärft werden. Um dieses Ziel zu erreichen, wurden zwei übergeordnete Fragestellungen formuliert, die jeweils eine untergeordnete Frage beinhalten:

Fragestellung 1: Welchen Beitrag leisten Awareness-Massnahmen zur Verbesserung der Cybersecurity?

Unterfrage 1.1: Welche Faktoren beeinflussen die Wirksamkeit solcher Massnahmen?

Fragestellung 2: Inwieweit können Escape-Rooms als Methode zur Schulung von Cybersecurity-Awareness eingesetzt werden?

Unterfrage 2.2: Welche Rahmenbedingungen tragen zur Wirksamkeit dieser Methode bei?

2. Theoretischer Rahmen

Das Kapitel 2.1 widmet sich zunächst der Entwicklung von Cybersecurity in der Gesellschaft und im Berufsfeld. Im Rahmen der theoretischen Auseinandersetzung werden in Kapitel 2.2 der Begriff ‚Informationssicherheit', der Schutz vor Angriffen und die Rolle des menschlichen Verhaltens beschrieben. In Kapitel 2.3 wird auf den Gamification-Ansatz und dessen Bedeutung eingegangen. Abschliessend wird in Kapitel 2.4 der Escape-Room als gamifizierte Massnahme vorgestellt, unter der Berücksichtigung der Erlebnispyramide von Tarssanen (2009b).

2.1 Die Entwicklung von Cybersecurity in der Gesellschaft und im Berufsfeld

Die zunehmende Digitalisierung hat erhebliche Auswirkungen auf die Art und Weise, wie Unternehmen in Kontakt treten und interagieren (Löffler et al., 2021). Einerseits ist die Komplexität von Cyberangriffen rasant gestiegen, sodass herkömmliche Abwehrmechanismen nicht mehr ausreichen, um diesen Angriffen entgegenzuwirken (vgl. Beispiel in Kapitel 1). Andererseits ist die Motivation, neue Technologien einzusetzen, um beispielsweise Kosten zu senken oder Innovationen voranzutreiben, stärker denn je (Clinton & Barrack, 2018). Diese Gegebenheiten gehen jedoch auch mit neuen Herausforderungen und Risiken einher, wie Cyberbedrohungen und Cyberkriminalität. Immer mehr Daten werden digital gespeichert und über das Internet ausgetauscht. Dies stellt nach Clinton und Barrack (2018) Unternehmen und Regierungen vor neue Bedrohungen durch Cyberkriminalität.

Aufgrund der zunehmenden Anzahl von Berichten in den Medien wächst das Bewusstsein für die Risiken und Bedrohungen im Zusammenhang mit Informationssicherheit. Das Fachgebiet der Informationssicherheit befasst sich mit der Nutzung von Informationstechnologien in Bezug auf Bedrohungen und Risiken im Bereich des Cyberraums (Klipper, 2015). Der englische Begriff ‚Cybersecurity' wird in der Regel anstelle des deutschen Begriffs ‚Informationssicherheit' verwendet. Er ist in der IT-Branche und in der internationalen Gemeinschaft allgemein anerkannt und gewinnt in gesellschaftlichen und politischen Diskussionen zunehmend an Bedeutung.

Zudem ist der Begriff ‚Cybersecurity' präziser als ‚Informationssicherheit', da er Bedrohungen aus dem Cyberraum berücksichtigt (Klipper, 2015). Gemäss Klipper (2015) wird die Bezeichnung ‚Cybersecurity' häufig als Synonym für die Begriffe ‚IT-Sicherheit' und ‚Informationssicherheit' verwendet. Experten beziehen sich jedoch meist auf Informationssicherheit. Mit Cybersecurity wird, ähnlich wie mit Informationssicherheit, das Ziel verfolgt, die Sicherheit von Informationen vor Bedrohungen zu schützen. Dabei konzentriert sich Cybersecurity speziell auf den Cyberraum und die Absicherung von Computersystemen, Netzwerken und Daten vor Angriffen aus dem Internet sowie anderen digitalen Kanälen (Klipper, 2015).

Es gibt sogenannte ‚Cybersecurity-Professionals' in verschiedenen Teildisziplinen, wie im Security-Management, in der Sicherheitsarchitektur und im Datenschutz. Klipper (2015) betont, dass die Professionalisierung innerhalb der Cybersecurity bereits so weit fortgeschritten ist, dass Personen sich häufig auf eine oder wenige Teildisziplinen spezialisieren. Das klassische Bild eines IT-Sicherheitsbeauftragten im Unternehmen, wie es noch vor wenigen Jahren vorherrschte, ist heute selten anzutreffen. Die meisten Cyber-Professionals, wie sie heute genannt werden, sind Seiteneinsteiger aus verschiedenen Berufsfeldern und Branchen (Klipper, 2015).

2.2 Schutz vor Angriffen und die Rolle des menschlichen Verhaltens

Liedtke (2022) beschreibt, dass die Sicherheit von Informationen eng mit persönlichem und individuellem Verhalten verbunden ist und nicht allein auf technische Massnahmen beschränkt werden kann. Es ist entscheidend, dass jede Person sich der eigenen Verantwortung bewusst ist und entsprechend sicherheitsbewusst handelt. Dies erfordert nach Liedtke (2022) ein Verständnis für die potenziellen Risiken und die Bereitschaft, angemessene Sicherheitsvorkehrungen zu treffen.

Denn Angreifer greifen längst nicht mehr ‚nur' die Technik an (Klipper, 2015). Clinton und Barrack (2018) sind der Meinung, dass der Mensch als eine der grössten Schwachstellen in Bezug auf die Informationssicherheit angesehen wird. Weber, Schütz und Fertig (2019) versuchen sich allerdings davon zu distanzieren, Menschen als ‚Schwachstellen' zu bezeichnen, und legen stattdessen den Fokus auf die Sicherheit von

Informationen und Informationssystemen. Das nachfolgende Folgende Zitat wurde von Weber et al. (2019, S. 3) verfasst:

> *„Menschen sind keine Schwachstelle – sie sind eine unverzichtbare Stütze für das Informationssicherheitskonzept."*

Dabei wird der Mensch als Komponente eines soziotechnischen Systems betrachtet (Garz & Kraimer, 1991, S. 22). Es ist daher nicht ausreichend, sich allein auf technische Sicherheitsmassnahmen zu verlassen, um diese Systeme zu schützen. Die Autoren sehen den Menschen als eine wichtige, unverzichtbare Stütze für das Informationssicherheitskonzept. Weber et al. (2019) sind der Ansicht, dass der Mensch als Sicherheitssensor für seine wichtige Rolle als Stütze des Informationssicherheitskonzepts sensibilisiert werden muss. In der Fachsprache heisst dies ‚Information-Security-Awareness' (vgl. Beispiel in Kapitel 2.4).

2.3 Einfluss auf Sicherheitsbewusstsein und -verhalten

Es gibt viele Gründe dafür, warum sich Personen nicht immer konform zum Thema Informationssicherheit verhalten. Gemäss Weber et al. (2019) können diese Ursachen auf mangelnde Erfahrung, unzureichende Schulungen, ein fehlendes Bewusstsein für Gefahren, Zeitmangel, Unvorsichtigkeit und das Fehlen von Alternativen zurückzuführen sein. Diese Gründe sind jedoch oft subjektiv geprägt und können dazu führen, dass Personen nicht immer die notwendigen Vorkehrungen zur Gewährleistung der Sicherheit eines Unternehmens treffen. Dabei betonen die Autoren, dass es sich um individuelle und kontextabhängige Faktoren handelt, die das Sicherheitsverhalten beeinflussen.

Forschungsergebnissen zufolge gibt es Faktoren, welche das Sicherheitsbewusstsein der Endnutzenden beeinflussen. Dazu gehört unter anderem die Informationssicherheitspolitik, die als Regeln und Vorschriften für die angemessene Nutzung der Informationssicherheitsressourcen einer Organisation definiert wird (Hwang, Wakefield, Kim & Kim 2019). Neben der Informationssicherheitspolitik spielt auch das Verhalten der Nutzenden eine zentrale Rolle beim Sicherheitsbewusstsein (Han, Kim & Kim 2017). Des Weiteren haben Untersuchungen von Farooq, Isoaho, Virtanen und Isoaho (2015) gezeigt, dass Faktoren wie Alter und Erfahrung signifikant mit dem wahrgenommenen Bewusstsein für Informationssicherheit positiv korrelieren. Shouran,

Priyambodo und Ashari (2019) betrachten die Aufklärung der Mitarbeitenden über die Bedeutung des Sicherheitsbewusstseins als eine der höchsten Prioritäten der Organisation. Die Ergebnisse der Umfragen zeigen auch, dass Wissen, Erfahrung, Sichtbarkeit und Beteiligung am Sicherheitsmanagement für das Sicherheitsbewusstsein von Bedeutung sind. Die Autoren nennen zudem Aspekte der Kultur, des Arbeitsumfelds, der Regeln und der Überwachung. Es ist notwendig, dass Richtlinien zum Sicherheitsbewusstsein in der gesamten Organisation verteilt und kommuniziert werden, damit alle Beteiligten davon Kenntnis haben.

Die Ergebnisse von Shouran et al. (2019) deuten unter anderem darauf hin, dass sich das Verhalten der Peers positiv auf die Handlungsaufforderung auswirkt, was sich wiederum positiv auf die Handlungserfahrung der Mitarbeitenden auswirkt. Somit hat die Handlungserfahrung vom Mitarbeitenden einen positiven Einfluss auf ihre Bedrohungs- und Reaktionswahrnehmung. Daher stehen die Bedrohungs- und die Reaktionswahrnehmung der Mitarbeitenden in einem positiven Zusammenhang mit ihrem Cybersicherheitsverhalten (Li et al., 2016). Eindeutig wird, dass die Entwicklung und Umsetzung von Programmen zur Förderung des Sicherheitsbewusstseins für die Verbesserung der Cybersecurity unerlässlich sind.

2.4 Information-Security-Awareness

Information-Security-Awareness bezieht sich nach Richter, Straub und Lucke (2018) auf den bewussten Umgang mit Informationen im Hinblick auf Sicherheitsgefahren. Der Begriff umfasst dabei alle Medien, unabhängig davon, ob es sich um digitale oder physische Informationen handelt. Durch Information-Security-Awareness sollen Personen dazu befähigt werden, potenzielle Bedrohungen zu erkennen, angemessen zu reagieren und sich aktiv für den Schutz von Informationen einzusetzen. Das Ziel der Schaffung von Awareness-Massnahmen ist es auch, dass die Nutzenden aktiv dazu beitragen, Informationen und Systeme vor möglichen Bedrohungen zu schützen. Ein solches Verhalten wird nach Richter et al. (2018) als informationssicherheitskonformes Verhalten bezeichnet. Trotz der Implementierung von Massnahmen ist es unbestreitbar, dass Menschen sich nicht immer in Übereinstimmung mit den Anforderungen der Informationssicherheit verhalten und nicht

immer ein angemessenes Sicherheitsbewusstsein zeigen. Beispiele dazu befinden sich im Anhang A.

Sharif und Ameen (2020) definieren Sicherheitsbewusstsein als die Fähigkeit des Benutzers, Aktivitäten, die die Cybersecurity bedrohen, zu erkennen und zu vermeiden. Zudem beinhaltet es ein kluges und verantwortungsbewusstes Verhalten (Toth & Klein, 2013). Laut Weber et al. (2019) ist es wichtig, individuelle Gründe bei der Auswahl der richtigen Awareness-Massnahme zu berücksichtigen. Die Auswahl einer geeigneten Awareness-Massnahme ist nur möglich, wenn die zugrunde liegenden Ursachen für mögliches Fehlverhalten bekannt sind. Weber et al. (2019) kommen zum Schluss, dass Schulungen als Awareness-Massnahmen der effektivste Weg sind, um das Sicherheitsbewusstsein zu fördern.

2.5 Gamification

Brad Wolfenden (2019) beschreibt, dass der Einsatz von Gamification beim Cyberlernen ‚bahnbrechend' sei, wie unterschiedliche Forschungsergebnisse unterstreichen. Durch praktische Aktivitäten wird das erlernte Wissen geprüft, sodass Unternehmen Leistungslücken erkennen und Wege zur kontinuierlichen Verbesserung finden können. Darüber hinaus hilft der Learning-by-Doing-Ansatz den Anwendern, Konzepte auf reale Übungen und Szenarien anzuwenden, wodurch die Behaltensrate der Informationen auf 75 % steigt, verglichen mit 5 % bei vorlesungsbasierten, passiven Lernmethoden (Wolfenden, 2019). Solche passiven Lernmethoden schaffen es oft nicht, die Teilnehmenden zu fesseln. Die Teilnehmenden hören die Inhalte, behalten einen Teil des Gelernten, haben aber Schwierigkeiten, den Stoff nach der Rückkehr ins Büro in die Praxis umzusetzen (Sharif & Ameen, 2020). Wolfenden (2019) beschreibt weiter, dass spielähnliche Umgebungen fesselnder als das Zuschauen bei einer vorlesungsbasierten Präsentation sind. Durch realistische Übungen mit Teamkollegen kann das strategische Lösen von Problemen gefördert werden. Zudem betont Wolfenden (2019), dass in gamifizierten Lernumgebungen ein Versuch-und-Irrtum-Lernen in einem sicheren Raum möglich ist.

Gamification ist als nützliches Schulungskonzept anerkannt worden (Wolfenden, 2019). Dabei liegt der Schwerpunkt von Gamification auf der Nutzung der menschlichen

Motivation, um das Engagement, die Motivation und das Behalten von Informationen zu fördern. Diese auf den Menschen fokussierte Designmethodik versucht, die unterhaltsamsten Elemente von Spielen auf andere produktive Aktivitäten wie Bildung anzuwenden (DeCusatis et al., 2022). Palmas und Niermann (2021) stellen fest, dass Gamification das Interesse am Lernthema der Lernenden fokussieren und binden kann, um damit den Lernerfolg zu fördern. In gamifizierten Anwendungen kommen starke motivationspsychologische Effekte wie Feedback, Eskapismus, Freude, Flow-Zustand, Herausforderungen und Errungenschaften zum Einsatz und entfalten ihre Wirkung (Hamari, Koivisto & Majuri, 2018). Dieses Argument wird durch die Annahme untermauert, dass der Mensch immer danach strebt, Teil einer Gemeinschaft zu sein. Palmas und Niermann (2021) haben Studien aus dem entsprechenden Forschungsfeld analysiert und festgestellt, dass die Verwendung von gamifizierten Elementen in Lernumgebungen die Motivation und die Produktivität bei Lernenden erhöht, um das Lernergebnis zu optimieren. Dementsprechend ist Gamification ein ideales Tool, um Veränderungen anzustossen und neue Verhaltensmuster zu erlernen (Palmas & Niermann, 2021).

Sharif und Ameen (2020) sind der Meinung, dass Spiele eine ansprechende Schnittstelle zur Verbesserung der Ausbildung bieten. In den letzten Jahren haben Spiele für Schulungszwecke an Beliebtheit gewonnen, weil sie die Teilnehmenden dazu ermutigen, sich zu engagieren sowie aktiv zu beteiligen, und sie inspirieren.

2.5.1 Potenziale und Anwendungsbereiche am Beispiel des Escape-Rooms

Die Verbindung von Escape-Rooms mit Security-Awareness ist eine neue Methode zur Verbesserung des Sicherheitsbewusstseins (Palmas & Niermann, 2021). Unternehmen nutzen Gamification-Elemente, um erwünschte Verhaltensweisen zu erkennen und zu fördern. Es stellt sich die Frage, wie Escape-Rooms als gamifizierte Massnahme genutzt werden können, um das Bewusstsein für Cybersicherheit zu stärken. Ein Escape-Room ist ein Teamspiel, bei dem die Teilnehmenden durch das Lösen von Rätseln und strategisches Vorgehen innerhalb einer bestimmten Zeit aus einem begrenzten Bereich entkommen müssen. Escape-Room-Herausforderungen umfassen Aktivitäten, die eine enge Koordination und Teamarbeit erfordern, wie Situationsbewusstsein, Aufgabenteilung, Kommunikation sowie kritisches und laterales Denken (Heikkinen & Shumeyko, 2016). Ein Escape-Room kann beispielsweise eine Sammlung von Rätseln und Aufgaben zu einem

bestimmten Thema beinhalten. Oft wird ein Escape-Room von einer Geschichte begleitet, die den Spielern mithilfe eines Videos oder einer Geschichte vermittelt wird.

Tarssanen (2009b) hat ein Modell entwickelt, das als *Erlebnispyramide* bezeichnet wird. Es dient als Grundlage, um ein erfolgreiches Escape-Room-Erlebnis zu erzeugen, indem es eine Struktur für die Schaffung eines fesselnden Erlebnisses hervorbringt. Dabei sollten die Bedürfnisse der teilnehmenden Personen berücksichtigt werden, angefangen bei der Motivation, das angebotene Erlebnis auszuprobieren, bis hin zu den möglichen menschlichen Veränderungen, die als Ergebnis des Erlebnisses auftreten können (Heikkinen & Shumeyko, 2016). Nicht jede Erfahrung, die ein Gast macht, kann als sinnvoll bezeichnet werden. Letzteres ist jedoch das ultimative Ziel eines jeden Anbieters von Erlebnissen, oder sollte es zumindest sein. Die grösste Herausforderung besteht darin, dass die Sinnhaftigkeit eines Erlebnisses subjektiv ist und von einer Vielzahl von Faktoren abhängt. Dennoch gibt es Möglichkeiten und Ansatzpunkte, das Erlebnis des Gastes zu beeinflussen (Heikkinen & Shumeyko, 2016). Diese Idee wird von einigen Forschern unterstützt, darunter Shedroff (2001, S. 2), der behauptet, dass *„die Elemente, die zu besseren Erfahrungen beitragen, bekannt und reproduzierbar sind“.* Laut Tarssanen (2009b) stellt die Erlebnispyramide ein perfektes Produkt dar, bei dem alle Elemente und Ebenen des Erlebnisses berücksichtigt werden.

2.5.2 Die Erlebnispyramide

Auf der horizontalen Achse der Abbildung 1 der Erlebnispyramide von Tarssanen (2009b) werden die Elemente des Produkts dargestellt, die das Gästeerlebnis beeinflussen und vom Erlebnisanbieter moderiert werden. Folgende sechs Elemente sollten bei der Erstellung und Bewertung eines Erlebnisprodukts berücksichtigt werden: Individualität (*individuality*), Authentizität (*authenticity*), Geschichte (*story*), multisensorische Wahrnehmung (*multisensory perception*), Kontrast (*contrast*) und Interaktion (*interaction*).

Idealerweise sollten diese Elemente auf jeder Ebene der Reise eines Gastes vorhanden sein. Tarssanen (2009b) teilt die Elemente in drei Gruppen: Kern des Produkts (Individualität, Authentizität und Geschichte), Zielgruppe (Kontrast) und Erleben (multisensorische Wahrnehmung, Interaktion).

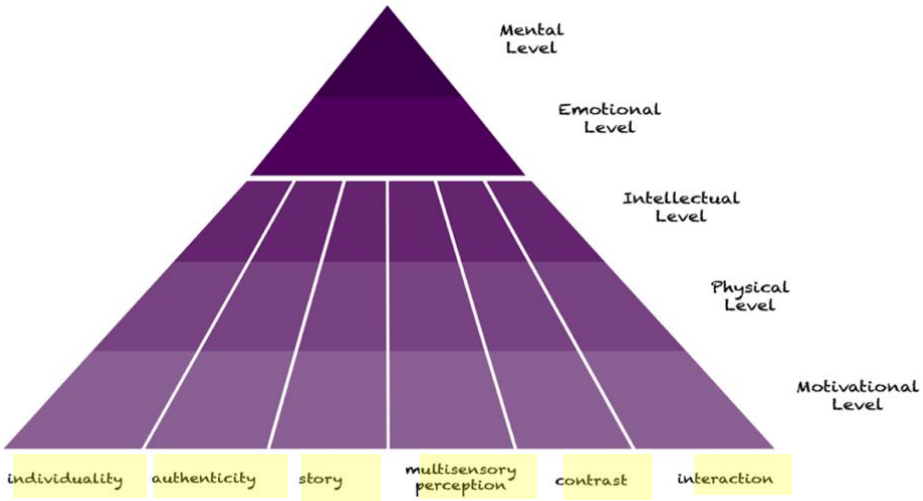

Abbildung 1: Die Erlebnispyramide von Tarssanen (2009b) horizontale Achse

Im Folgenden werden die fünf Elemente auf der horizontalen Achse näher erläutert. Das Element der Individualität bezieht sich auf die Einzigartigkeit und Flexibilität eines Erlebnisprodukts. Laut Pine und Gilmore (2011) ist die Individualität ein wichtiges Element bei der Gestaltung von bedeutsamen Erlebnissen. Denn idealerweise kann ein solches Produkt nicht anderswo gefunden werden, was den Begriff der Individualität verdeutlicht. Eine Personalisierung des Produkts kann jedoch kostspielig sein. Daher empfehlen Pine und Gilmore (2011) Unternehmen, die Lücke zwischen den Bedürfnissen der Gäste und dem, was Dienstleistungen bieten, zu verringern oder zu beseitigen, um neue Werte zu schaffen. Um eine einzigartige und ansprechende Erfahrung zu erzeugen, sollte der Gast aktiv in die Gestaltung des Erlebnisses einbezogen werden. Es ist von hoher Bedeutung, dass Unternehmen den Zielmarkt sowie die Bedürfnisse und Wünsche ihrer Kunden kennen. Nur so kann ein effektives Erlebnisprodukt gestaltet werden.

Als weitere Erlebnisebene definiert Tarssanen (2009b) die Authentizität als Grad der Glaubwürdigkeit des Produkts. Die Authentizität eines Erlebnisses wird durch persönliche Wahrnehmungen und frühere Erfahrungen des Gastes beeinflusst. Die Geschichte (Story) ist die Erzählung, die das Erlebnis durchzieht, und eng mit der Authentizität verbunden. Pine und Gilmore (2011) betonen, dass die Geschichte während des Erlebnisses kohärent, also zusammenhängend, bleiben muss, um ein erfolgreiches Erlebnisprodukt zu schaffen. White (1998, zitiert nach Heikkinen & Shumeyko, 2016) ist der Ansicht, dass auf einer Geschichte basierende Themen wirkungsvoll sein können, da sie die Gäste in eine fantasievolle, imaginäre Welt entführen.

Eine überzeugende und ausgearbeitete Geschichte kann das Erlebnis authentisch und glaubwürdig machen, wodurch eine emotionale Bindung zum Gast entstehen kann. Radoff (2011) unterstützt diese Idee und behauptet, dass Geschichten eine transformative Kraft haben, die das Denken der Menschen verändert und Bedeutung vermitteln kann. Bedeutungsvolle und denkwürdige Erlebnisse sind eng mit Emotionen verbunden, weshalb es für Erlebnisgestalter wichtig ist, diesem Element des Erlebnisses viel Aufmerksamkeit zu widmen. Die multisensorische Wahrnehmung bezieht sich darauf, alle fünf Sinne einzubeziehen, um die Erzählung des Produkts zu unterstützen und persönliche Emotionen zu verknüpfen. Das Einbeziehen persönlicher Erinnerungen und Emotionen in ein Erlebnis ist ein zentraler Faktor, der durch die Elemente der multisensorischen Wahrnehmung und Interaktion unterstützt wird. Multisensorische Wahrnehmung und Interaktion sind Elemente, die nur während des Erlebnisses existieren und es auf greifbare Weise unterstützen. Diese beiden Aspekte werden als Erfahrung betrachtet. Wenn man über Erlebnisse spricht, kann die Interaktion aus verschiedenen Perspektiven betrachtet werden. Es gibt eine Interaktion zwischen dem Gast und dem Produkt, dem Gast und dem Erlebnisanbieter sowie eine Interaktion zwischen den Gästen, die gemeinsam an dem Erlebnis teilnehmen. Alle diese Arten der Interaktion sollten berücksichtigt werden. Wenn ein Produkt gemeinsam mit anderen Gästen erlebt wird, hebt dies das Gruppengefühl und den Status des Einzelnen hervor, bindet die Teilnehmenden enger aneinander und das Erlebnis gewinnt bei richtiger Durchführung an Akzeptanz. Wenn ein Erlebnisanbieter seine Arbeit als Inszenierung für seine Darbietung behandelt, wird die Interaktion mit dem Gast lebendiger und das Erlebnis individueller, was einen Kontrast zum Alltag darstellt. Des

Weiteren haben Gespräche mit denjenigen, mit denen das Erlebnis geteilt wurde, einen Einfluss auf die Bindung von Erinnerungen sowie auf die Darstellung des Interesses und der Motivation in Bezug auf dieses Erlebnis. Denning, Lerner, Shostack und Kohno (2013) sind der Auffassung, dass gut konzipierte Spiele ein effektives Mittel darstellen können, um eine grosse Anzahl von Menschen mit einer begrenzten Menge an Sicherheitsinformationen zu erreichen. Die Autoren argumentieren, dass Spiele Spass machen und Menschen dazu motivieren, miteinander zu interagieren und daran teilzunehmen. Spiele ermöglichen auch das Erkunden von Ideen und fördern das Stellen von Fragen. Darüber hinaus sollten sie einen intrinsischen Unterhaltungswert bieten, der die Menschen dazu anregt, diese Elemente auch in ihrer Freizeit zu nutzen (Denning et al., 2013).

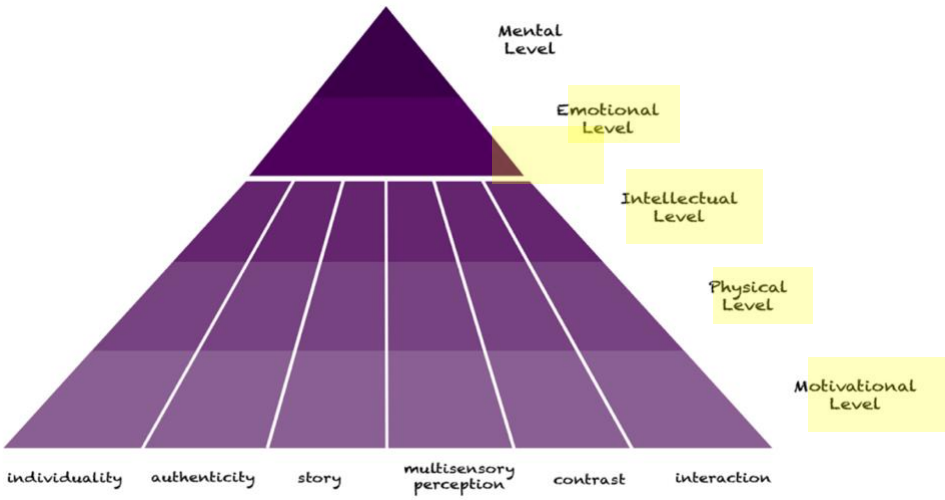

Abbildung 2: Die Erlebnispyramide von Tarssanen (2009b) vertikale Achse

Auf der vertikalen Achse der Abbildung 2 der Erlebnispyramide von Tarssanen (2009b) werden die Erlebnisebenen dargestellt, die die Reise eines Gastes durch alle Stufen repräsentieren sollten. Im Folgenden werden die fünf Elemente auf der vertikalen Achse näher erläutert, welche allerdings vom Erlebnisanbieter nur bedingt beeinflusst werden können.

Die erste Ebene, die der Autor unterscheidet, ist die Motivationsebene (*motivation level*), die der Vorerfahrungsphase entspricht. Auf dieser Ebene wird das Interesse geweckt und die Erwartungen beginnen sich in den Gedanken der Teilnehmenden zu bilden. Dabei spielen Marketinginstrumente und -techniken eine wesentliche Rolle bei der Beeinflussung dieser Erwartungen. Das Ziel besteht darin, dass die Vermarktung des Erlebnisses die Elemente auf der horizontalen Ebene widerspiegelt. Es folgt die physische Ebene, auf der

der Gast das Erlebnis in seiner materiellen Form kennenlernt. Nach Heikkinen und Shumeyko (2016) hängt der Erfolg eines Escape-Room-Spiels stark von der Qualität des physischen Raums ab, in dem es stattfindet (*physical level*). Die allgemeinen Umgebungsbedingungen spielen eine bedeutende Rolle, da die Teilnehmenden bis zu einer Stunde in dem Raum verbringen. Es ist wichtig, dass die Temperatur angenehm und der Raum gut beleuchtet sowie belüftet ist. Die Einrichtung und die Rätsel müssen zum Thema passen, um die Geschichte und Atmosphäre des Spiels zu unterstützen (Heikkinen & Shumeyko, 2016). Die auf der physischen Ebene aufgenommenen Sinnesreize werden auf der nächsten Stufe, der intellektuellen Ebene, interpretiert.

Escape-Room-Spiele bieten nicht nur Unterhaltung, sondern können laut Heikkinen und Shumeyko (2016) auch als pädagogische Erfahrung betrachtet werden: Das Lösen von Rätseln und das Grübeln über herausfordernde Aufgaben fördern das Denken, Analysieren, Argumentieren und Schlussfolgern. Auf dieser Ebene sind der Intellekt, das Denken und das Analysieren zentral. Obwohl Spiele in erster Linie Spass und Aufregung bieten, sind das Lernen und die Entwicklung von Fähigkeiten ein wesentlicher Bestandteil der Erfahrung. Erfolgreiche Escape-Room-Spiele lehren die Teilnehmenden, unkonventionell zu denken, Probleme aus verschiedenen Blickwinkeln zu betrachten und unter Druck zu arbeiten.

Wenn die zuvor beschriebenen Ebenen des Erlebnisses sorgfältig gestaltet wurden, entsteht nach Heikkinen und Shumeyko (2016) ein zusammenhängendes und bedeutungsvolles Erlebnis. Wie in Abbildung 2 zu sehen ist, sind die letzten beiden Ebenen der Erlebnispyramide von den anderen Ebenen abgetrennt. Dies liegt daran, dass der Erlebnisanbieter auf diese Ebenen keinen Einfluss hat, da die hier ablaufenden Prozesse subjektiv und persönlich sind. Die erste dieser beiden Ebenen ist die emotionale Ebene, auf der sich eine emotionale Reaktion auf das Erlebnis entwickelt. Emotionen sind ein integraler Bestandteil jeder bedeutsamen Erfahrung. Nach Pine und Gilmore (2011) können Unternehmen, die es schaffen, nicht nur die Bedürfnisse der Gäste zu befriedigen, sondern auch eine positive emotionale Reaktion auf das Erlebnis hervorzurufen, eine höhere Kundenloyalität erreichen.

Der Erfolg dieses Erlebnisses hängt massgeblich von der Gruppendynamik und den einzelnen Teilnehmenden ab. Escape-Rooms sollen auch auf der emotionalen Ebene eine Reaktion hervorrufen, indem die Teilnehmenden emotional in die Geschichte des Raums

einbezogen werden und sich so verhalten können, als wäre das Szenario real. Dies führt zu einem Zustand, der als ‚Flow' bezeichnet wird, bei dem die Zeit schnell vergeht und die Spieler sich auf die Aufgaben konzentrieren. Dabei ist der Aufbau der Rätsel zu beachten, da er einen erheblichen Einfluss auf den emotionalen Zustand der Teilnehmenden haben kann. Die letzte von den Autoren angestrebte Ebene des Gästeerlebnisses ist die mentale Ebene. Das ultimative Ziel besteht darin, eine Veränderung im Lebensstil und Denken zu bewirken. Auf der mentalen Ebene (*mental level*) kann die Erfahrung eines Escape-Rooms eine nachhaltige Wirkung haben. Logisches Denken, analytische Fähigkeiten und besseres Arbeiten in ungewohnten Situationen sind einige der möglichen Ergebnisse (Heikkinen & Shumeyko, 2016).

3. Methodik

In diesem Kapitel wird die Durchführung der empirischen Untersuchung der Bedeutung von Awareness-Massnahmen für die Verbesserung der Cybersecurity beschrieben. In den folgenden Kapiteln werden die Untersuchungsmethode und die Datenerhebung erläutert. Zudem werden Informationen zur Stichprobe und zur Auswertung des erhobenen Materials präsentiert.

3.1 Forschungsdesign

Das Forschungsdesign dieser Arbeit orientiert sich an den Prinzipien der qualitativen Sozialforschung. Als Methode zur Datenerhebung wurde das leitfadengestützte Experteninterview gewählt. Dafür wurden die Grundsätze der empirischen Sozialforschung von Atteslander (2010) berücksichtigt, die eine systematische Erfassung und Interpretation sozialer Phänomene beschreiben. Gläser und Laudel (2010) betonen, dass die empirische Forschung durch die gezielte Analyse und Auswertung von Erfahrungen und vorhandenem Wissen Erkenntnisse gewinnt. Das übergeordnete Ziel besteht darin, tiefgehende Einblicke und ein Verständnis in das untersuchte Thema zu erlangen.

Basierend auf den bisherigen Erkenntnissen wurde beschlossen, dass ein qualitatives, exploratives Vorgehen für die Datenerhebung und Analyse der Daten angemessen ist. Um den aktuellen Wissensstand zum Thema zu ermitteln und eine solide Grundlage für das Interview und die Datenanalyse zu schaffen, wurde eine umfassende Literaturrecherche durchgeführt. Um Beobachtungen und Aussagen besser in einen Zusammenhang zu bringen, wird dafür in der explorativen Forschung die bestehende Fachliteratur verwendet (Flick, 2009). Aufgrund der gesammelten Erkenntnisse wurde ein Interviewleitfaden für die geplanten Expertengespräche entwickelt. Das Forschungsdesign basiert somit auf einer qualitativen Herangehensweise, die es ermöglicht, die subjektiven Perspektiven und Erfahrungen der Experten detailliert zu erfassen und zu verstehen. Durch das leitfadengestützte Experteninterview wird ein reichhaltiges Datenmaterial generiert, das eine fundierte Analyse und Diskussion der Forschungsfragen ermöglicht. Diese Aspekte werden im nächsten Kapitel näher erläutert.

3.2 Experteninterviews

Qualitative Experteninterviews sind eine bewährte Methode, um spezifisches Wissen und Erfahrungen von Personen zu einem bestimmten Thema zu erfassen (Gläser & Laudel, 2010). Als Expertin oder Experte wird eine Person bezeichnet, die über ein Wissen verfügt, das nicht allen in diesem Fachgebiet zugänglich ist (Garz & Kraimer, 1991). In der qualitativen Sozialforschung sind Experteninterviews nützlich, da sie in kurzer Zeit eine Fülle von Informationen und Einblicken liefern können. Nach Mayring (2010) zeichnet sich dieses Verfahren dadurch aus, dass es auf einen sprachlichen Zugang setzt, um eine bestimmte Fragestellung zu untersuchen. Die Methodik der qualitativen Sozialforschung ermöglicht es den befragten Personen, ihre persönlichen Erfahrungen, Perspektiven und Einstellungen zu einem Thema darzulegen. In der Regel werden Experteninterviews als Leitfadeninterviews durchgeführt, bei denen ein vorab formulierter Fragenkatalog als Leitfaden für das Interview dient (Gläser & Laudel, 2010).

Die offene Gestaltung der Interviewsituation ermöglicht einen offenen Zugang zum Untersuchungsfeld, um Wissen, Handlungsempfehlungen und Gestaltungsmöglichkeiten auf Basis der erhobenen Daten zu gewinnen (Flick, 2009). Das Leitfadeninterview eignet sich besonders für explorative Untersuchungen, bei denen die Sichtweisen der Befragten im Mittelpunkt stehen. Da es ähnlich wie ein Gespräch gestaltet ist, muss die Reihenfolge der Fragen nicht strikt eingehalten werden. Damit das Interview erfolgreich verläuft, ist neben einem gut konzeptionierten Leitfaden auch die Kompetenz der Interviewerin oder des Interviewers entscheidend. Vorwissen und Kenntnisse über den Kontext, der besprochen wird, spielen daher eine wesentliche Rolle (Helfferich, 2011). Der Leitfaden spiegelt die theoretischen Vorannahmen wider und stellt sicher, dass alle wichtigen Punkte angesprochen werden. Der Interviewende kann im Verlauf des Gesprächs entscheiden, ob und wann er zu einem Thema detailliert nachfragt oder den Interviewten zum Leitfaden zurückführt. Dadurch wird ein Abschweifen in für die Forschungsfragen irrelevante Themen vermieden und überflüssige Daten werden minimiert. Interviews können nach Helfferich (2011) in verschiedene Grade der Strukturierung eingeteilt werden, angefangen von vollständig strukturierten über halbstrukturierte bis hin zu unstrukturierten Interviews. Für die formulierte Fragestellung ist das halbstrukturierte Leitfadeninterview eine passende Methode, da es Offenheit und Struktur miteinander verbindet. Der Leitfaden dient als

Grundlage für die Gespräche, ermöglicht aber gleichzeitig Flexibilität, um auf die spezifischen Antworten der Experten einzugehen. Das qualitative Interview hat das Ziel, durch mündliche Gespräche Wissen und Erfahrungen von Akteuren zu erheben. Dabei liegt die Steuerung des Gesprächsverlaufs weniger beim Interviewer, sondern mehr beim Befragten. Durch diese Herangehensweise werden tiefere und umfassendere Einblicke in das Forschungsthema ermöglicht (Gläser & Laudel, 2010).

3.3 Datenerhebungsinstrument – Entwicklung Interviewleitfaden

Zu Beginn der Entwicklung des Interviewleitfadens wurde eine umfassende Literaturrecherche nach relevanten Forschungsarbeiten und Publikationen durchgeführt, um einen Überblick über den aktuellen Stand der Forschung zu erhalten. Insbesondere wurden Berichte des NCSC (2023) analysiert, um die häufigsten Angriffsvektoren und deren Ursprung in Schweizer Unternehmen zu identifizieren und zu verstehen. Im Zuge dieser Recherche wurde deutlich, dass bestimmte Begriffe und Definitionen im Bereich der Cybersecurity vorherrschen und zur Fachsprache gehören. Es war daher wichtig, diese Schlüsselbegriffe zu kennen, um sich in der fachlichen Diskussion orientieren zu können. Deshalb sollten diese Begriffe nicht heruntergebrochen oder simplifiziert werden.

Auf Grundlage der gesammelten Literatur wurden geeignete Themenbereiche und Fragestellungen für den Leitfaden erarbeitet und definiert. Der Leitfaden bestand aus drei inhaltlichen Blöcken, die jeweils unterschiedliche Fragen enthielten. Zusätzlich wurden Aufrechterhaltungs- und Steuerungsfragen formuliert, um das Gespräch jederzeit lenken zu können, wenn dies nötig war. Es wurde auch eine Checkliste erarbeitet, um sicherzustellen, dass bestimmte Aspekte unbedingt angesprochen werden. Der Interviewleitfaden ist im Anhang B einsehbar.

Zu Beginn der Interviews wurde die interviewte Person gebeten, sich vorzustellen und über ihren Hintergrund, ihre Erfahrungen im Bereich der Cybersecurity sowie die Bedeutung des Themas zu berichten.

Der erste inhaltliche Block behandelte das Thema Cybersecurity und Awareness. Es wurden Fragen zur Bedeutung dieser Themenkomplexe und zu den bekanntesten Angriffsvektoren aus Sicht der Awareness gestellt.

Der zweite inhaltliche Block beinhaltet die Verbindung von Cybersecurity und Awareness. Es soll herausgefunden werden, welche potenziellen Einflüsse auf das Cybersicherheitsverhalten existieren und welche Massnahmen ergriffen werden, um die Sicherheit eines Servers zu gewährleisten. Zudem wurden Fragen zu den internen Vorgehensweisen in Unternehmen bei der Erkennung verdächtiger Aktivität gestellt.

Der dritte inhaltliche Block thematisierte Awareness und Prävention. Hierbei sollte eruiert werden, wie Mitarbeitende für das Thema sensibilisiert und geschult werden und welche Massnahmen Unternehmen ergreifen, um ihre Mitarbeitenden in diesem Bereich zu schulen. Da einige Unternehmen bereits einen Cybersecurity-Escape-Room haben, wurde bewusst ein separater Block mit Fragen zu diesem Thema erstellt. Hierbei sollte erforscht werden, wie Unternehmen Gamification in ihrer Organisation umsetzen, welche Infrastruktur dabei verwendet wird und welcher Grundgedanke der Storyline zugrunde liegt. Vor der Durchführung der eigentlichen Interviews wurde der Interviewleitfaden in Zusammenarbeit mit dem Praxispartner überprüft und einem Pretest unterzogen, um seine Praxistauglichkeit und Wirksamkeit zu gewährleisten.

3.4 Angaben zur Stichprobe

Zu Beginn einer empirischen Untersuchung ist es von zentraler Bedeutung, die Zielgruppe zu definieren, um sicherzustellen, dass die richtigen Experten ausgewählt werden. Hierbei sollte zuerst überlegt werden, welche Kompetenzen und Erfahrungen relevant sind, um das untersuchte Fachgebiet angemessen zu erfassen. Das Vorhandensein von Fachwissen über bestehende Awareness-Massnahmen und Erfahrungen im Umgang mit den aktuellen Bedrohungen, das Vorgehen zur Sensibilisierung von Mitarbeitenden wie auch ihre Einschätzungen bezüglich der Umsetzung dieser Massnahmen waren einige der wichtigsten Kompetenzen. Somit sollten Experten aus dem Bereich Cybersecurity ausgewählt werden, welche alle in einem Unternehmen in der Schweiz als deren Awareness-Spezialisten arbeiten und über umfangreiches Fachwissen und praktische Erfahrung auf dem Gebiet verfügen. Dafür wurden unterschiedliche Unternehmen in der Schweiz und deren Cybersecurity-Awareness-Experten für ein 30-minütiges Interview angefragt. Von den insgesamt sieben Unternehmen wurden zwei durch eine Kontaktperson des Praxispartners akquiriert und die restlichen fünf Unternehmen wurden von der

Studentin selbst via LinkedIn angefragt. Die Forschungsmethode ist deswegen auch qualitativ empirisch ausgewählt, um ein möglichst alltagsnahes Verständnis vom Grad der Bedrohung durch Cyberrisiken wie auch zum Cybersicherheitsbewusstsein im Unternehmen zu erlangen. Um die Anonymität und Integrität der Experten zu gewährleisten, wurden alle beteiligten Personen anonymisiert, sodass nicht nachvollziehbar ist, welche Aussagen von welcher Person oder welchem Unternehmen getätigt wurden. Aus Datenschutzgründen wird in der Arbeit nicht näher auf die Unternehmen eingegangen.

3.5 Ablauf der Datenerhebung

In diesem Abschnitt wird die Durchführung der Interviews beschrieben. Zur Gewährleistung der Gütekriterien der qualitativen Sozialforschung wurden standardisierte Bedingungen wie ein Leitfaden und ähnliche Rahmenbedingungen sichergestellt.

Im Zeitraum vom 6. bis zum 24. März 2023 wurden insgesamt sieben Experten befragt, von denen zwei online über Teams und fünf vor Ort im Unternehmen interviewt wurden. Es wurde darauf geachtet, dass eine vertrauensvolle und offene Gesprächsatmosphäre geschaffen wird.

Da die Experten bei dieser Erhebungsmethode die Richtung und Dauer des Interviews selbst bestimmen konnten, variierte die Dauer der Interviews zum Teil. Das kürzeste Interview dauerte genau 30 Minuten, während das längste knapp über eine Stunde dauerte. Zu Beginn jedes Interviews, vor der Aufnahme, hat sich die Forscherin kurz mit ihrem Namen, Alter und Beruf vorgestellt und die Einverständniserklärung mit dem Experten besprochen, welche im Anhang C zu finden ist. Es wurde somit sichergestellt, dass die Verwendung der Daten im Vorfeld mit einer Einverständniserklärung geklärt wurde, die von beiden Personen unterschrieben wurde. Dadurch sollten die Bedingungen transparent und sicher gestaltet werden.

Im ersten Teil des Interviews wurden die Expertinnen und Experten gebeten, ihre berufliche Position zu schildern. Anschliessend wurden offene Fragen gestellt, um die Expertinnen und Experten aufzufordern, ihre Einschätzungen zur aktuellen Situation im untersuchten Kontext aufgrund ihres Fachwissens abzugeben. Die abschliessenden Fragen zielten darauf ab, die Bewertungen der befragten Expertinnen und Experten abzurunden. Die Experten wurden auch dazu ermutigt, ihre Ansichten und Ideen auszudrücken und das

Gespräch in neue Richtungen zu lenken, wenn dies angebracht war. Während des Interviews versuchte die Forscherin aktiv zuzuhören und bei Bedarf nachzufragen, wenn sie etwas nicht verstand. Nach dem Interview wurden die Aufnahmen mit MAXQDA Version 2022 transkribiert. Das Programm MAXQDA kann als computergestützte qualitative Daten- und Textanalyse verwendet werden. Im nächsten Kapitel wird die Datenaufbereitung der erhobenen Daten beschrieben.

3.6 Datenaufbereitung: Transkription

Nachdem die Datenerhebungsphase beendet war, fand als nächster Schritt die Datenaufbereitung statt. Nach Flick (2009) sollte qualitatives Datenmaterial, welches ausgewertet werden soll, aufbereitet oder transkribiert werden. Die konkrete Herangehensweise hängt dabei von der Forschungsfrage ab. Die Interviews wurden mit dem Smartphone vor Ort aufgenommen, während die Online-Interviews direkt in Teams aufgezeichnet wurden. In den Transkriptionen wurden sämtliche personenbezogene Informationen über die Identitäten der interviewten Person und über die des Unternehmens anonymisiert, sodass keine Rückschlüsse auf Personen möglich sind. Für die beteiligten Unternehmen und Experten wurden Pseudonyme erstellt und mit zufälliger Nummerierung gekennzeichnet. Bei der Transkription des Materials wurden die Interviews vom Schweizerdeutschen ins Deutsche übersetzt, was zu einigen Umformulierungen führte. Alle Audioaufnahmen wurden dann mit dem Textanalyseprogramm MAXQDA transkribiert.

3.7 Datenauswertungsmethode

Die qualitative Inhaltsanalyse umfasst verschiedene Verfahren zur systematischen Analyse von Texten und kann zur Interpretation von Forschungsmaterial verwendet werden (Flick, 2009). Bei der Inhaltsanalyse wird das Material systematisch und schrittweise analysiert. Das Ziel der Analyse besteht darin, das Material gemäss vordefinierten Ordnungskriterien zu strukturieren und in einzelne Einheiten aufzuteilen. Im Fokus dieser Analyse steht das im Voraus oder während des Analyseprozesses erstellte Kategoriensystem (Mayring, 2010). In Anlehnung an Mayring (2015) erfolgt die Auswertung der Interviews mithilfe der strukturierenden Inhaltsanalyse. Durch die Verwendung eines Kategoriensystems können die Ergebnisse der Interviewanalysen vergleichbar gemacht werden.

Grundlegend bestehen zwei Möglichkeiten der Kategorienbildung nach Mayring (2010), die deduktive und die induktive Vorgehensweise, welche auch miteinander kombiniert werden können. Unter der Methode der deduktiven Kategorienbildung wird die Kodierung des Datenmaterials anhand theoretisch begründeter Analyseaspekte verstanden. Gemäss Mayring (2010) werden die Kategorien vor der Analyse des Datenmaterials festgelegt. Basierend auf dem Forschungsinteresse wurde für die Analyse ein Vorgehen gewählt, das sowohl induktive als auch deduktive Elemente beinhaltet. Durch eine ausschliesslich deduktive Vorgehensweise besteht die Gefahr, die Offenheit der Untersuchung von Anfang an einzuschränken, wobei die induktive Vorgehensweise die Offenheit für neue Aspekte fördert. Daher wurde bewusst eine Kombination von beiden gewählt. Zu Beginn wurden alle Textbestandteile anhand eines achtstufigen inhaltsanalytischen Ablaufmodells in Kategorien eingeteilt. Im Folgenden werden die einzelnen Schritte der Auswertung und Erstellung des Kategoriensystems näher erläutert.

Schritt 1: Spezifische Themen, Inhalte und Aspekte, welche für die Forschungsfrage relevant sind, wurden zu Beginn aus dem Material herausgefiltert. Ein grober Überblick über die Daten soll im ersten Schritt geschaffen werden. Dies wurde direkt im Material anhand von Notizen gemacht, für eine erste Begutachtung des Datenmaterials und um Besonderheiten und Ideen festzustellen.

Schritt 2: Da im Vorfeld theoretische Konzepte erarbeitet worden sind, wurden ausgehend von diesen Konzepten deduktiv Kategorien abgeleitet, die aufgrund der Forschungsfragen und des theoretischen Hintergrunds relevant sind. Die Grundlage für die Kategorisierung bildet der Interviewleitfaden. Danach wurde das gekennzeichnete Material herausgefiltert, zusammengefasst und aufgearbeitet. Da bei der Erstellung des Leitfadens auf eine sinnvolle Reihenfolge geachtet wurde, konnte diese zum teils übernommen werden. Somit wurde auch das Codieren erleichtert, denn gewisse Fragen zielten direkt auf eine der formulierten Hauptkategorien ab.

Schritt 3: Es wurden bei Bedarf induktiv Subkategorien gebildet, um das Material weiter zu strukturieren. Während der induktiven Analyse wurden relevante Passagen des Datenmaterials gekennzeichnet und zusammengefasst. Gemeinsame Themen und Muster konnten identifiziert werden, die auf den Daten selbst basieren.

Schritt 4: Um das Material zu kategorisieren, wurden Definitionen der Kategorien erstellt, die mit entsprechenden Ankerbeispielen und Kodierregeln versehen sind. Es wird detailliert beschrieben, welche Textelemente in eine bestimmte Kategorie fallen. Darüber hinaus werden spezifische Abschnitte aus Texten genannt, die einer bestimmten Kategorie zugeordnet wurden und als exemplarisches Beispiel für diese Kategorie dienen. Im Verlauf der Analyse konnten weitere Ankerbeispiele darin aufgenommen werden.

Schritt 5 und 6: Die identifizierten Stellen wurden gekennzeichnet und den entsprechenden Subkategorien zugeordnet. Falls es Abgrenzungsprobleme zwischen den Kategorien gab, wurden bei Bedarf klare Regeln formuliert, um eine eindeutige und schnelle Zuordnung zu ermöglichen. Das Kategoriensystem wurde dabei erprobt und überarbeitet. Die Einteilung der einzelnen Haupt- und Subkategorien ist dem Anhang D zu entnehmen.

Schritt 7: Bei der Analyse der Interviews wurden die Daten systematisch und wiederholt gesichtet, um neue Themen, Muster und Zusammenhänge zu identifizieren, welche nicht direkt aus der vorherigen Theorie oder den vordefinierten Kategorien abgeleitet wurden. Das Kategoriensystem wurde an einigen Stelle nochmals überarbeitet.

Schritt 8: Nachfolgend wurde das gesamte Material mithilfe des Kategoriensystems codiert und Textstellen wurden der entsprechenden Kategorie zugeordnet.

Schritt 9: Im Anschluss wurden jede einzelne Hauptkategorie und deren Subkategorien mithilfe des ‚Smart Coding Tools' von MAXQDA analysiert, um die wesentlichen Ergebnisse aus den Interviews zusammenzufassen. Die Kombination von deduktiver und induktiver Analyse ermöglichte eine ganzheitliche Auswertung des Datenmaterials. Die vordefinierten Hauptkategorien bieten eine theoretische Grundlage und Struktur, während die induktiv entwickelten Subkategorien neue Perspektiven und Einsichten liefern können.

4. Ergebnisse

In diesem Abschnitt werden die Ergebnisse der qualitativen Interviews unter Verwendung des Kategoriensystems der strukturierten Inhaltsanalyse vorgestellt. Es werden die Haupt- und Subkategorien verwendet, um die gewonnenen Daten zu strukturieren und zu analysieren. Die Interviewergebnisse bieten einen detaillierten Einblick in die befragten Personen und ihre Ansichten zum untersuchten Thema. Das gesamte Kategoriensystem zählt 351 codierte Segmente aus den Interviews.

4.1 Verständnis und Wissen zu Cybersecurity

Diese Kategorie beinhaltet Aussagen über das allgemeingültige Verständnis und Wissen zur Cybersecurity. Dazu gehören wichtige Begriffe und Definitionen zum Thema Cybersecurity. Die Hauptkategorie ‚Verständnis und Wissen zu Cybersecurity' hat insgesamt 83 codierte Segmente und zählt demnach zu der am zweithäufigsten vertretenen Kategorie. Diese Hauptkategorie lässt sich in die folgenden drei Subkategorien unterteilen.

4.1.1 Bedeutung Cybersecurity

In dieser Subkategorie wurden insgesamt 24 Segmente codiert. Diese Aussagen beziehen sich auf die Bedeutung von Cybersecurity in der heutigen vernetzten Welt wie auch deren Stellenwert und Relevanz. Alle Experten schätzten die Bedeutung als sehr hoch ein, wobei die Vernetzung als treibender Faktor dafür angesehen wurde. Die Experten waren sich einig, dass die Digitalisierung mit einer Zunahme von Bedrohungen und Herausforderungen einhergeht und somit den Stellenwert und die Bedeutung der Thematik steigen wird. Die zunehmende Vernetzung in der Industrie, die Abhängigkeit von der Informatik und die Professionalisierung von Betrugsmaschen sowie Bedrohungen wurden als grosse Herausforderungen betrachtet:

Experte 3: „Sie werden immer wie raffinierter, deswegen ist es notwendig, die Menschen richtig zu schulen, um sie dazu zu befähigen, sich sicher zu verhalten. Es ist auch ein Business dahinter wo entsteht, es ist immer wie besser organisiert, das stellt eine grosse Herausforderung dar."

Die Antworten der Experten deuten darauf hin, dass sich unser Alltag zunehmend digitalisiert, während viele Menschen sich nicht bewusst sind, welche Risiken damit einhergehen können. Auch die Bedeutung der Cybersecurity für Unternehmen wurde mehrfach betont. Unternehmen sind darauf angewiesen, ihre Services zu nutzen und aufrechtzuerhalten, um Daten oder Dienstleistungen bereitzustellen. Wenn diese Services allerdings nicht funktionieren, können sie ihre Dienste nicht länger aufrechterhalten.

4.1.2 Angriffsvektoren für Mitarbeitende

Diese Subkategorie umfasst 17 codierte Segmente. Aussagen beziehen sich auf Arten von Cyberangriffen (Angriffsvektoren), welche Mitarbeitenden bekannt sein sollten.

Alle Experten vertraten die Ansicht, dass Mitarbeitende in der Lage sein sollten, Phishing-E-Mails zu erkennen. Dabei beschrieb Experte 6, dass bei den meisten grossen Angriffen in der Regel eine Phishing-E-Mail am Anfang steht. Zusätzlich wurde die Klassifizierung von Informationen als wichtiger Faktor genannt. Die Aussagen der Experten deuten darauf hin, dass es von hoher Bedeutung ist, dass Menschen auch eine grundsätzliche ‚Skepsis' gegenüber der Thematik entwickeln und bei verdächtigen E-Mails kritisch sein sollten. Auch klassische Themen wie die Verwendung von einzigartigen Passwörtern wurden erwähnt. Hierbei betonten die Experten, dass diese nicht mehrfach verwendet werden sollten. Zudem wurde die Aktivierung einer Multifaktor-Authentifizierung empfohlen. Ein Experte wies zudem auf die Notwendigkeit hin, dass Mitarbeitende sich dessen bewusst sein sollten, dass sie als Einzelperson Opfer eines Hackerangriffs werden könnten, eines sogenannten ‚Social Engineering'. Der Experte bezeichnet Social Engineering als die Manipulation und Ausnutzung menschlicher Verhaltensweisen, um Zugang zu vertraulichen Informationen oder Systemen zu erlangen. Abschliessend nannten die Experten es als entscheidend, dass die Mitarbeitenden misstrauisch sind und sicherstellen, dass Informationen nur an vertrauenswürdige Quellen weitergegeben werden.

Experte 4: „Heutzutage finden gezielt Angriffe von Cyberkriminellen auf dich als Individuum statt."

Experte 6: „Personen gehen so weit, dass sie versuchen, über Monate lang eine vermeintliche Beziehung aufzubauen. Durch den persönlichen Bezug und das gezielte Ansprechen individueller Schwachstellen wird die Effektivität solcher Angriffe erhöht."

4.1.3 Meistgenannte Bedrohungen

Insgesamt 20 Aussagen wurden über die Subkategorie ‚meistgenannte Bedrohungen' getätigt. Die Aussagen beziehen sich hauptsächlich auf die am häufigsten genannten Bedrohungen. Laut den Experten sind insbesondere Phishing-E-Mails und deren Missbrauch von Daten häufig. Unternehmen betrachten dies derzeit als sehr grosse Bedrohung, ebenso wie Ransomware. Der Begriff ‚Social Engineering' wurde mehrfach erwähnt und umfasst alle Arten von Manipulationsversuche über E-Mails und andere Methoden. Experte 2 und 3 beschrieben, dass Angreifer sich teilweise monatelang im Netzwerk eines Unternehmens aufhalten können. Die E-Mail wird als der grösste und wichtigste Angriffsvektor für Privatpersonen und Unternehmen angesehen, da sie viele Möglichkeiten bietet, Dinge zu fälschen und Menschen zu manipulieren. Obwohl viele technische Massnahmen ergriffen werden können, reichen diese oft nicht aus, wenn eine mitarbeitende Person versehentlich sensible Daten preisgibt. Die grösste Bedrohung für ein Unternehmen besteht den Experten zufolge in einem Serviceausfall.

Experte 2: „Phishing gehört da halt immer mit dazu und ist oft die Grundlage für alles."

4.2 Cybersecurity und Awareness

Im Folgenden werden Aussagen über die Begriffe ‚Cybersecurity' und ‚Awareness' sowie deren Verhältnis zueinander getroffen. Zudem werden die Notwendigkeit und Bedeutung von Awareness- sowie Sensibilisierungsmassnahmen erläutert. Diese Hauptkategorie lässt sich in die folgenden vier Subkategorien unterteilen.

4.2.1 Bedeutung von Awareness-Massnahmen

Basierend auf Expertenmeinungen wurde festgestellt, dass Awareness-Massnahmen eine entscheidende Rolle spielen, um Mitarbeitende über mögliche Angriffsszenarien aufzuklären. Diese Massnahmen dienen auch dazu, die Mitarbeitenden zu

befähigen, verdächtige Aktivität zu erkennen. Laut den Experten ist der Mensch generell das schwächste Glied in der Sicherheitskette.

Experte 2: „Ja, wir sagen auch, dass der Mensch das grösste Sicherheitsrisiko ist, aber zugleich auch die grösste Chance schlussendlich. Das darf man nicht vergessen und dort sollte man eigentlich den Fokus drauf setzen, auf die grösste Chance."

Daher liegt der Schwerpunkt der Awareness-Massnahmen nicht nur auf der Sensibilisierung, sondern auch darauf, den Mitarbeitenden zu vermitteln, dass sie die grösste Chance haben, das Unternehmen zu schützen, da sie an vorderster Front stehen. Experte 6 berichtete, dass die Relevanz von Awareness-Massnahmen noch nicht die angestrebte Stufe erreicht hat. Besonders wurde die Bedeutung des CEOs für Awareness-Massnahmen hervorgehoben, da dieser die Führungskräfte in die Verantwortung nehmen sollte. Auch die Vermittlung eines Verständnisses für die Wichtigkeit von Sicherheitsmassnahmen ist entscheidend. Einem Experten zufolge haben viele Mitarbeitende das Gefühl, dass ihre Arbeit im Büro nicht wichtig sei, und sie fragen sich, warum ein Angreifer Interesse an ihren Daten haben sollte. Dies unterstreicht die Notwendigkeit, die Mitarbeitenden über die Risiken und Auswirkungen von Sicherheitsverletzungen aufzuklären.

4.2.2 Faktoren und potenzielle Einflüsse auf Cybersicherheitsverhalten

Gemäss den Experten gibt es verschiedene Faktoren, die das Cybersicherheitsverhalten von Mitarbeitenden beeinflussen können. Die Experten waren sich einig, dass Cyberkriminelle kontinuierlich neue Techniken und Methoden entwickeln, um Sicherheitsmassnahmen zu umgehen und an sensible Informationen zu gelangen. Dies erschwert die Erkennung und Abwehr von Cyberangriffen und beeinflusst nach Expertenaussage das Cybersicherheitsverhalten der Mitarbeitenden. Zusätzlich vertraten alle Experten die Meinung, dass das Sicherheitsbewusstsein einer Person eine entscheidende Rolle für ihr Cybersicherheitsverhalten spielt. Das Bildungsniveau und das Wissen über Cybersicherheit können nach Expertenmeinung ebenfalls das Verhalten einer Person beeinflussen. Ein weiterer genannter Aspekt ist das Vorhandensein klarer Sicherheitsrichtlinien und Massnahmen am Arbeitsplatz. Wenn die Organisation den Schutz

der Privatsphäre und der Daten ernst nimmt und entsprechend klare Richtlinien formuliert, sind die Mitarbeitenden eher geneigt, sich sicherheitsbewusst zu verhalten. Ein Experte beschrieb, dass es oft Menschen gibt, die sich sicher verhalten möchten, dies jedoch aufgrund fehlender Informationen oder Ressourcen, von denen sie diese Informationen erhalten können, nicht tun können. Es wurde betont, dass sicheres Verhalten in Unternehmen nicht belohnt wird und Mitarbeitende möglicherweise nicht die Zeit und Ressourcen haben, sich sicher zu verhalten. Häufig ist dies auf unklare Prozesse zurückzuführen. Somit sind neben dem Sicherheitsbewusstsein auch klar formulierte Richtlinien, die Verfügbarkeit von Informationen und die Arbeitsumgebung entscheidend. Darüber hinaus betonten die Experten, dass Bedrohungen nicht nur von externen Quellen kommen können, sondern auch interne Bedrohungen ein erhebliches Risiko darstellen können. Ein weiterer wichtiger Einflussfaktor, den ein Experte ansprach, ist die sich ändernde Aufmerksamkeitsspanne der Menschen, insbesondre durch die Nutzung von Social-Media-Plattformen wie TikTok:

Experte 1: „Früher hat man beispielsweise ein einstündiges E-Learning gemacht, wo alle Themen drin waren. Heutzutage wollen, dass die Leute nicht mehr machen, das ist viel zu lange, was ja auch logisch ist, aber ich behaupte, das wird noch mehr zunehmen. Wenn ich schaue, was Tiktok mit den Menschen und ihrer Konzentrationsfähigkeit anrichtet, im Negativen, das wird einen Einfluss haben auf die Arbeitgeber in diesem Bereich, dort wird dann Schulung und Sensibilisierung anders vorgenommen werden müssen.“

4.2.3 Herausforderungen bezüglich des Cybersicherheitsverhaltens

Laut allen Experten besteht eine der grössten Herausforderungen darin, dass Angreifer immer besser werden und automatisierte Angriffe mit geringerem Aufwand durchführen können. Es wurde betont, dass es eine zentrale Herausforderung ist, Mitarbeitende auf immer raffiniertere Angriffsszenarien vorzubereiten und entsprechend zu schulen. Eine weitere Herausforderung besteht darin, im hektischen Arbeitsalltag angemessen mit Phishing-Mails umzugehen, besonders dann, wenn im Unternehmen viel Betrieb herrscht und Mitarbeitende möglicherweise abgelenkt sind. Ein Experte beschrieb, dass die ‚gutmütige Natur‘ der Menschen und ihre tendenzielle Zurückhaltung bei der

Verteidigung als Herausforderung betrachtet werden. Experte 2 merkte an, dass sie in ihrem Unternehmen deswegen bewusst Angriffe durch das Telefon führen, und erklärte:

„Du würdest staunen, wie viele Leute da einfach vertrauen haben in eine freundliche Stimme, passendes Thema usw. Das ist das Problem, die Menschen trauen sich oft nicht sich zu wehren.“

Experte 1: „Das funktioniert halt einfach, irgendeine hierarchisch höher gestellte Person, und dann sind die Leute zu ängstlich und glauben an das Gute. Ich würde mir wünschen, dass noch mehr Leute um den Ecken denken.“

Eine weitere Herausforderung für das Cybersicherheitsverhalten ist, dass Mitarbeitende möglicherweise nicht über die erforderlichen Fähigkeiten verfügen, sei es sprachlich oder technisch, um Geräte zu bedienen und Anweisungen zu verstehen. Viele Mitarbeitende sind zum Teil lediglich mit einem Smartphone ausgestattet. Zusätzlich wurde es auch als Herausforderung dargestellt, das eher ‚trockene‘ Thema Cybersicherheit spannend und interaktiv zu gestalten.

4.2.4 Cybersicherheitsbewusstsein/interne Vorgehensweisen in Unternehmen

Aussagen in dieser Subkategorie beinhalten interne Vorgehensweisen bezüglich Cybersecurity-Richtlinien und Aussagen, wie Mitarbeitende im Unternehmen dazu ermutigt werden, sich sicherheitskonform zu verhalten. Die Experten waren sich einig, dass Unternehmen interne Prozesse für Cybersicherheitsrichtlinien einrichten sollten. Es wurde betont, dass die Mitarbeitenden kontinuierlich ermutigt werden sollten, Vorfälle zu melden, da eine frühzeitige Erkennung von Bedrohungen von grosser Bedeutung ist. Experte 7 erwähnte, dass intern ein Netzwerk von sogenannten ‚Security-Champions‘ besteht, die in jedem Arbeitsteam vertreten sind. Mitarbeitende können sich bei diesen Champions bei Problemen direkt erkundigen. Die Security-Champions werden regelmässig und detaillierter geschult. Fast alle Experten führen in ihren Unternehmen regelmässig Phishing-Tests durch, bei denen Test-E-Mails an die Mitarbeitenden verschickt werden, abhängig davon, über welchen Kenntnisstand sie verfügen. In Bezug auf Phishing-E-Mails haben die meisten

Unternehmen interne Verfahren, bei denen verdächtige E-Mails über einen Phishing-Button direkt gemeldet werden können. Abschliessend wiesen sie darauf hin, dass solche internen Vorgehensweisen repetitiv wiederholt werden sollten. Sie betonten, dass dies in angemessenen Abständen geschehen sollte, um sicherzustellen, dass das Thema wieder auftaucht und internalisiert wird. Die internen Vorgehensweisen eines Unternehmens sind davon abhängig, welchen Sensibilisierungsgrad das Unternehmen erreicht hat.

Experte 1: „Mitarbeitende bekommen Phishing-Mails, in der Hoffnung, dass sie irgendwann merken, welche Eigenschaften dahinterstecken, um auch in Zukunft das besser erkennen zu können."

Die Experten hatten unterschiedliche Ansichten darüber, wie Mitarbeitende dazu ermutigt werden können, sich sicherheitskonform zu verhalten. Eine Möglichkeit besteht laut einem Experten darin, Belohnungssysteme einzuführen, beispielsweise in Form von Ranglisten, Punkten oder Wettbewerben. Allerdings wurde auf das Problem hingewiesen, dass man nicht sagen kann, dass jemand schlecht war, nur weil sich eine Person nie gemeldet hat. Nach Meinung eines anderen Experten könnte auch ein materieller Anreiz Mitarbeitende dazu ermutigen, sich sicherheitskonform zu verhalten. Unternehmen versuchen dabei aktiv, Mitarbeitende darauf aufmerksam zu machen, dass das erlangte Wissen auch privat genutzt werden kann. Ein Experte kritisierte jedoch, dass es keinen Sinn macht, Belohnungssysteme für das Erkennen von Phishing-Mails einzuführen, da dies in der Branche als Standard angesehen wird. Nach einer Aussage eines Experten müssen solche Techniken zur Sensibilisierung in die Kultur des Unternehmens passen, wobei es schwierig ist zu sagen, ob das eine oder das andere richtig ist.

4.3 Konkrete Massnahmen zur Awareness

Diese Hauptkategorie behandelt technische und personelle Massnahmen, die anhand der durchgeführten Interviews erfasst wurden. Sie beziehen sich speziell auf Schutzmassnahmen zur Abwehr von Cyberangriffen auf Systeme.

4.3.1 Technische Massnahmen

Experten bieten in Unternehmen eine Vielzahl konkreter technischer Awareness-Massnahmen an, um das Bewusstsein der Mitarbeitenden für Informationssicherheit zu stärken. Folgende Aussagen beziehen sich auf technische Massnahmen.

Phishing-Simulationen mit Feedback: Es werden regelmässig Phishing-Simulationen durchgeführt, bei denen den Mitarbeitenden gefälschte E-Mails zugesendet werden, um ihr Verhalten bei potenziellen Phishing-Angriffen zu testen. Nach der Teilnahme erhalten die Mitarbeitenden individuelles Feedback und Hinweise, wie sie Phishing-E-Mails besser erkennen können. Zudem haben fast alle Unternehmen intern einen sogenannten ‚Phishing-Button', welchen Mitarbeitende bei verdächtigen Mails direkt anklicken können.

Service-Desk: Der Service-Desk steht den Mitarbeitenden zur Verfügung, um bei Sicherheitsfragen und Problemen zu helfen. Die Mitarbeitenden können sich an den Service-Desk wenden, um schnelle Unterstützung zu erhalten, wenn sie unsicher sind oder auf etwas Verdächtiges stossen.

E-Learning und Benutzerweisungen: Es werden Onlineschulungen und Kurse angeboten, die zum Teil aus 15 bis 16 kurzen Modulen zu verschiedenen Themen der Informationssicherheit bestehen. Das beinhaltet Test- und Quizfragen, um das Wissen der Mitarbeitenden abzufragen und zu festigen. Diese Trainings werden in regelmässigen Abständen durchgeführt. Des Weiteren werden Benutzeranweisungen bereitgestellt, welche klare Regeln und Sicherheitsrichtlinien festlegen, die von den Mitarbeitenden bei Arbeitsbeginn gelesen und unterschrieben werden müssen. Mitarbeitende haben alle Pflichtmodule, welche jährlich wiederholt werden müssen.

Sicherheitswarnungen und -hinweise: Mitarbeitende werden über aktuelle Bedrohungen und Sicherheitsvorfälle informiert. Dafür nutzt ein Unternehmen Simulationskampagnen. Das Unternehmen stellt dabei sicher, die Mitarbeitenden über potenzielle Risiken auf dem Laufenden zu halten.

Learning-Experience-Plattform/Immersive Labs: Eine Learning-Experience-Plattform kann auch in Bezug auf technische Massnahmen zur Awareness eingesetzt werden. Sie bietet interaktive und immersive Lernumgebungen, um die Fähigkeiten und das Wissen der Mitarbeitenden zu verbessern. Dies kann im Rahmen der Bereitstellung von E-Learning-Kursen, interaktiven Schulungsübungen, praktischen Übungen usw. erfolgen.

Immersive-Labs-Trainingsplattformen nutzen gamifizierte Elemente, um das Lernen unterhaltsam und motivierend zu gestalten.

Gamification: Vier der sieben befragten Unternehmen berichteten, dass sie über einen Cybersecurity-Escape-Room im Unternehmen verfügen.

4.3.2 Personelle Massnahmen

Personelle Massnahmen bezüglich Cybersecurity-Awareness beziehen sich auf Aktivitäten und Massnahmen, die darauf abzielen, das Sicherheitsbewusstsein und das Wissen der Mitarbeitenden in Bezug auf Cybersecurity zu verbessern.

Standard-Onboarding: Jede mitarbeitende Person erhält ein standardisiertes Onboarding, das die wichtigsten Aspekte der Cybersecurity abdeckt. Hier werden grundlegende Informationen zu Unternehmensrichtlinien und Sicherheitsverfahren vermittelt.

Präsenzschulungen: Es werden auch Präsenzschulungen durchgeführt, in denen spezifischere Themen behandelt werden. Diese Schulungen können beispielsweise Phishing-Prävention, sichere Internetnutzung oder den Schutz sensibler Informationen umfassen. Mitarbeitende sollten in den Schulungen die Möglichkeit haben, Fragen zu stellen.

Basisschulungen: Eine Basisschulung wird durchgeführt, um den Mitarbeitenden wichtige Begriffe und Konzepte der Cybersecurity näherzubringen.

Spezifische Schulungen: Je nach Rolle oder Abteilung können spezifische Schulungen angeboten werden, die auf die speziellen Anforderungen und Risiken dieser Position eingehen (Beispiel: Security-Champions).

Sensibilisierungskampagnen: Unter anderem werden Poster in digitaler und analoger Form erstellt, um das Bewusstsein für Sicherheitsrisiken zu schärfen. Weiter erzählte eine der Experten vom sogenannten ‚Realitätscheck'. In diesem Teil der Schulung wird den Mitarbeitenden verdeutlicht, dass es im Internet viele Angebote gibt, die zu gut sind, um wahr zu sein:

Experte 5: „Eben sowas, ich komme im Internet auf eine Seite, wo ich den neusten Bentley für 10'000 CHF kaufen kann, das kann nicht sein. Nicht denken, das will man halt

gerne, man ist der glücklichste Mensch der Welt, man ist so besonders, nein! Das nennen wir den Realitätscheck.“

Sicherheitsrichtlinien und Vorschriften: Um sicherzustellen, dass die Sicherheitsrichtlinien und Vorschriften von den Mitarbeitenden verstanden werden, erzählte ein Experte, dass er regelmässig Kommunikationen überarbeitet. Diese Texte werden vereinfacht und weniger technisch formuliert, um sie für den Mitarbeitenden verständlicher zu machen. Die meisten Experten waren der Ansicht, dass Schulungen vor Ort in der Regel besser bei den Mitarbeitenden ankommen.

Experte 6: „Vor-Ort-Schulungen kommen in der Regel besser an, vor allem, wenn man kleine Gruppen hat, wo man vor Ort schulen kann, getrauen sie sich auch mehr zu fragen und hören tendenziell auch besser zu. Auch wenn das Themen sind, wo du 1:1 bei uns im Intranet so findest und eigentlich nachlesen könntest, sind sie viel offener und nehmen das viel besser auf vor Ort…Menschen können in der Awareness noch ausgefallene Sachen machen und Themen adressieren, welche das Unternehmen direkt betrifft. Keiner hat mehr Lust auf irgendeine langweilige PowerPoint, das Wichtigste bei Awareness ist die Attraktivität im Training.“

4.4 Gamification als Awareness-Massnahme am Beispiel des Escape-Rooms

Diese Hauptkategorie umfasst Aussagen über konkrete Zusammenhänge zwischen Awareness und Gamification. Zudem folgen Vorteile, Nachteile und Inputs von den Unternehmen, welche bereits einen Cybersecurity-Escape-Room haben. Dazu gehören auch Herausforderungen und Konsequenzen der Umsetzung.

4.4.1 Vorteile

Gemäss den Expertenmeinungen gibt es mehrere konkrete Vorteile bei der Umsetzung von gamifizierten Awareness-Massnahmen in Unternehmen. Die Experten waren sich einig, dass gamifizierte Awareness-Massnahmen dazu beitragen können, das Thema Sicherheit und Datenschutz zu entmystifizieren und Mitarbeitende dazu zu ermutigen, sich aktiv damit auseinanderzusetzen. Durch interaktive und unterhaltsame Spiele oder Trainings erhalten die

Teilnehmenden eine positive Erfahrung und gewinnen Vertrauen in ihre Fähigkeiten. Dies ermöglicht eine unterhaltsame Art der Wissensvermittlung, bei der die Teilnehmenden aktiv involviert werden und Spass haben können. Gamifizierte Massnahmen sprechen die Mitarbeitenden auf einer emotionalen Ebene an und erzeugen so ein hohes Mass an Engagement. Die Mitarbeitenden erleben ein positives Erlebnis im Zusammenhang mit Cybersecurity. Dies kann ihre Einstellung zum Thema positiv beeinflussen. Ein Escape-Room verlangt oft Teamarbeit, Zusammenarbeit und Kommunikation, um Rätsel zu lösen und die Aufgaben zu bewältigen. Dies erfordert Teamgeist und stärkt die Zusammenarbeit innerhalb des Unternehmens. Zudem lernen Mitarbeitende, gemeinsam an Herausforderungen zu arbeiten. Aufgrund des interaktiven und erlebnisorientierten Charakters von gamifizierten Massnahmen bleibt das erworbene Wissen länger im Gedächtnis. Infolge der aktiven Beteiligung und des Durchlebens von Situationen im Escape-Room werden Informationen tiefer verankert und langfristig besser erinnert.

Weiter waren die Experten der Meinung, dass gamifizierte Massnahmen es den Mitarbeitenden ermöglichen, komplexe Sicherheitskonzepte auf spielerische und zugängliche Weise zu erfassen. Durch die Integration von Gamification-Elementen werden die Mitarbeitenden aktiv in den Lernprozess eingebunden. Auch bieten gamifizierte Massnahmen wie Escape-Rooms die Möglichkeit, sich ausserhalb des Arbeitsumfeldes mit dem Thema zu beschäftigen, und sie können dabei helfen, Berührungsängste abzubauen und das Thema greifbarer zu machen. Indem sich die Teilnehmenden aktiv an einer spielerischen Aufgabe beteiligen, erfahren sie, dass Cybersecurity nicht unzugänglich oder überwältigend ist, sondern etwas, dass sie verstehen und beherrschen können. Die Experten berichteten, dass diese Interaktion sehr geschätzt wird. Zudem können gamifizierte Massnahmen auch eine haptische Erfahrung darstellen, wobei die Konsequenzen einer konkreten Situation aufgezeigt werden können und Mitarbeitende vor reale Herausforderungen gestellt werden:

Experte 1: „Teilnehmenden müssen Schubladen öffnen, Gegenstände umdrehen usw. und das wird geschätzt! Ich glaube, wir erreichen mit den Personen auf allen Ebenen und mit unterschiedlichen Kompetenzen.…Gerade so Situationen, wenn sie lediglich virtuell übergebracht werden, sind viel weniger greifbar (…) Ich bin grundsätzlich der Meinung, wenn man irgendetwas spielerisch jemanden beibringen kann, dann bleibt dass auch länger.“

Experte 1: „Wir wollten auch einen Empowerment-Moment schaffen, und so ein bisschen entmystifizieren von dieser Hacker-Kultur und diesem ganzen Internet und Darknet, da es für viele

etwas sehr Mystisches ist, was sie gar nicht einordnen können, deswegen auch das Problem mit der Risikoeinschätzung, sie wissen eigentlich gar nicht, was da passiert.“

4.4.2 Nachteile

Gemäss den Expertenmeinungen gibt es bei der Umsetzung von Awareness- und gamifizierten Massnahmen einige nachteilige Aspekte für Unternehmen. Die meisten Experten waren sich einig, dass der Zeit- und Ressourcenaufwand einen Nachteil darstellt. Die Sensibilisierung einer kleinen Anzahl von Mitarbeitenden erfordert oft einen erheblichen Zeitaufwand und Ressourceneinsatz seitens des Unternehmens. Ein Experte hob hervor, dass gamifizierte Awareness-Massnahmen möglicherweise besser für Teamausflüge oder spezifische Gruppen geeignet sind als für das gesamte Unternehmen. Die Umsetzung solcher Massnahmen für alle Teams kann eine beträchtliche Herausforderung darstellen und erfordert eine angemessene Planung sowie Ressourceneinschätzung. Die Experten, welche im Unternehmen selbst schon einen Cybersecurity-Escape-Room besitzen, erwähnten, dass die Durchführung solcher Veranstaltungen vor Ort aufgrund der COVID-19-Pandemie in vielen Fällen untersagt oder stark eingeschränkt wurde. Das hat die Umsetzung von gamifizierten Massnahmen beeinträchtigt. Ein weiterer Nachteil nach Expertenmeinung besteht darin, dass die Auswirkungen und der Erfolg von gamifizierten Veranstaltungen oder Schulungen im Nachhinein schwer zu messen sind. Es kann eine Herausforderung sein, die tatsächliche Wirksamkeit solcher Massnahmen zu quantifizieren oder den Fortschritt der Mitarbeitenden zu verfolgen.

4.4.3 Input

Diese Subkategorie umfasst Aussagen, welche als Input für den selbst entwickelten Escape-Room der Unternehmen und grundsätzliche Meinungsäusserungen dienen. Letztere können Input für den Praxispartner darstellen. Es wurden demnach nur Aussagen berücksichtigt, die von Experten getätigt wurden, welche bereits selbst einen Escape-Room unterhalten. Die Experten betonten, dass zu Beginn der Planung wichtige Aspekte im Vorfeld geklärt werden sollten, die bei der Konzeption beachtet werden müssen. Dazu gehören Fragen wie: Wie viele Personen sollten teilnehmen? Soll der Escape-Room intern oder extern durchgeführt werden? Wo soll er stattfinden? Ist eine mobile Umsetzung möglich? Unternehmen berichteten, dass sie oft zu Beginn eine Fragerunde durchführen und nach Abschluss des Escape-Rooms ein Debriefing mit den Teilnehmenden vornehmen. Ein Experte erwähnte, dass die Teilnehmenden sich nach dem Spiel endlich trauen würden, Fragen zu stellen. Des Weiteren wurde bemerkt, dass Mitarbeitende oft das Gefühl haben,

‚dumme' Fragen zu stellen, und diese daher nicht äussern. Mehrere Experten berichteten, dass die meisten Teilnehmenden den Escape-Room als sehr spannend empfinden. Die Experten gaben auch Anregungen, wie die Nutzung von Mobilgeräten oder die Schaffung einer digitalen Erfahrung. Eine weitere Äusserung bezog sich auf die Verbindung mit Virtual Reality. Es wurde angemerkt, dass es interessant sein könnte, den virtuellen mit dem realen Raum zu verbinden. Zudem wurde die Integration von QR-Codes erwähnt.

Experte 2: „Und daher glaube ich, da braucht's noch viel mehr Klarheit, mehr Erklärung, mehr Storytelling und Geschichten erzählen."

4.4.4 Herausforderungen

Aus den Antworten der Experten geht hervor, dass die Einrichtung eines Escape-Rooms viele Ressourcen erfordert. Viele der Experten haben für die Entwicklung und Durchführung des Escape-Roms externe Berater hinzugezogen. Weitere genannte Herausforderungen betrafen technische Massnahmen, wie das Suchen nach geeigneten Räumlichkeiten, die über einen längeren Zeitraum bespielt werden können. Die Durchführung eines Escape-Rooms erfordert zudem einen erheblichen Zeitaufwand. Das Spiel selbst dauert in der Regel eine Stunde, hinzu kommen Transferzeiten sowie Diskussions- und Reflexionsphasen nach dem Spiel. Die Experten betonten, dass den Teilnehmenden ausreichend Zeit gegeben werden sollte, um das Erlebte zu verarbeiten und die Erfahrungen zu reflektieren. Es ist auch zu erwähnen, dass ein begrenztes Budget vorhanden ist. In Bezug auf dezentral organisierte Unternehmen stellt die Einbeziehung aller Mitarbeitenden eine Herausforderung dar. Aus diesem Grund wird die Möglichkeit in Betracht gezogen, mobile Escape-Rooms einzusetzen, um den Escape-Room an verschiedenen Standorten durchzuführen.

Eine weitere bedeutende Herausforderung besteht darin, den Escape-Room und seine Rätsel so zu gestalten, dass sie einen direkten Bezug zum Arbeitsalltag der Mitarbeitenden haben. In diesem Zusammenhang wird der Begriff ‚didaktische Anordnung' eingeführt.

Experte 6: „Spass ist ja gut, aber lernen sollten sie ja immer noch etwas."

Experte 2: „Awareness ist halt einfach ein komplexes Thema.“

5. Diskussion

Die vorliegende Bachelorarbeit umfasst eine empirische Untersuchung zum Thema Cybersecurity-Awareness. Im Rahmen dieser Untersuchung wurden sieben Experten aus verschiedenen Unternehmen in der Schweiz befragt. In diesem Zusammenhang sollte zuerst ein Grundverständnis entwickelt werden, um die Bedeutung und Relevanz der Thematik anhand einer Literaturrecherche zu entwickeln. Zudem wurde untersucht, welche Awareness-Massnahmen Unternehmen bereits anbieten, welchen Herausforderungen sie dabei begegnen und wie sich das Verhalten der Mitarbeitenden in Bezug auf Cybersecurity ändern lassen könnte.

5.1 Zusammenfassung der zentralen Ergebnisse

Bei der Analyse und Auswertung der Experteninterviews konnten vier Haupt- und zwölf Subkategorien abgeleitet werden. Durch die Verwendung eines Kategoriensystems konnten die Ergebnisse der Interviewanalysen vergleichbar gemacht werden. Dieses Vorgehen ermöglichte es, wiederkehrende Muster und Themen in den Interviewdaten zu identifizieren.

Verständnis und Wissen zu Cybersecurity

Anhand der Ergebnisse lässt sich erkennen, dass Unternehmen verstärkt auf Massnahmen zur Gewährleistung der Informationssicherheit setzen. Die Bedeutung von Cybersecurity ist in der heutigen vernetzten Welt hoch. Die wachsende Vernetzung und Digitalisierung führen zu einer Zunahme von Bedrohungen und Herausforderungen. Viele Menschen sind sich der Risiken nicht bewusst, die mit der digitalen Welt einhergehen können. Für Unternehmen ist Cybersecurity besonders wichtig, da sie von funktionierenden Services und dem Schutz von Daten sowie Dienstleistungen abhängig sind. Wenn die Sicherheit nicht gewährleistet ist, können Unternehmen ihre Dienste nicht aufrechterhalten. Insgesamt bestand ein Konsens darüber, dass die Bedeutung und Relevanz von Cybersecurity in Zukunft weiter zunehmen wird. Mitarbeitende sollten in der Lage sein, Phishing-E-Mails zu erkennen, denn diese sind meist der Auslöser für grosse Angriffe. Die Klassifizierung von Informationen spielt ebenfalls eine bedeutsame Rolle. Es ist essenziell, dass Menschen eine grundsätzliche Skepsis entwickeln und bei verdächtigen E-Mails kritisch sind. Es wurde darauf hingewiesen, dass Mitarbeitende sich bewusst sein

sollten, dass sie als Einzelperson gezielt Opfer von Hackerangriffen werden könnten, insbesondere durch Social Engineering. Misstrauen und die Weitergabe von Informationen nur an vertrauenswürdige Quellen wurden dabei als entscheidend erachtet. Es wurden verschiedene Bedrohungen im Bereich der Cybersicherheit genannt. Phishing-E-Mails, Missbrauch von Daten und Ransomware wurden als besonders grosse Bedrohungen betrachtet. Die E-Mail wird als der grösste und wichtigste Angriffsvektor für Unternehmen und Privatpersonen angesehen, da es viele Möglichkeiten gibt, Informationen zu fälschen und Menschen zu manipulieren. Der potenzielle Serviceunterbruch wurde als grösste Bedrohung für Unternehmen genannt.

Cybersecurity und Awareness – Bedeutung von Awareness-Massnahmen

Awareness-Massnahmen spielen eine entscheidende Rolle, um Mitarbeitende über mögliche Angriffsszenarien aufzuklären und sie in der Erkennung verdächtiger Aktivitäten zu schulen. Dies konnte durch die Literatur wie auch durch die Datenerhebung bestätigt werden. Der Mensch wird als das schwächste Glied in der Sicherheitskette betrachtet, daher liegt der Fokus der Massnahmen darauf, die Mitarbeitenden nicht nur zu sensibilisieren, sondern auch zu ermächtigen, das Unternehmen zu schützen. Aufgrund der Ergebnisse aus den Interviews lässt sich ableiten, dass die Relevanz von Awareness-Massnahmen noch nicht das gewünschte Niveau erreicht hat. Insbesondere wurde die Bedeutung des CEOs für diese Massnahmen hervorgehoben, da dieser die Führungskräfte in die Verantwortung nehmen und ein Verständnis für die Wichtigkeit von Sicherheitsmassnahmen vermitteln sollte. Es wurde ferner auf das Gefühl vieler Mitarbeitender hingewiesen, dass ihre Arbeit im Büro nicht wichtig genug sei, um das Interesse von Angreifern zu wecken. Daher ist es unerlässlich, die Mitarbeitenden über Risiken und Auswirkungen von Sicherheitsverletzungen aufzuklären. Es konnten verschiedene Faktoren identifiziert werden, die das Cybersicherheitsverhalten von Mitarbeitenden beeinflussen. Neue Techniken und Methoden der Cyberkriminellen erschweren die Erkennung und Abwehr von Angriffen. Das Sicherheitsbewusstsein, das Bildungsniveau und das Wissen über Cybersecurity spielen ebenfalls eine Rolle. Klare Sicherheitsrichtlinien am Arbeitsplatz fördern sicherheitsbewusstes Verhalten. Ressourcenmangel, unklare Prozesse, interne Bedrohungen und eine veränderte Aufmerksamkeitsspanne sind weitere Einflussfaktoren. Laut den Befragten kann es

schwierig sein, dass ‚trockene' Thema Cybersecurity spannend und interaktiv zu gestalten. Wichtig ist, dass die Sensibilisierungstechniken zur Unternehmenskultur passen.

Konkrete Massnahmen zur Awareness

Viele Unternehmen führen Phishing-Simulationen mit Feedback durch, haben einen Service-Desk, E-Learning und Benutzerweisungen, Sicherheitswarnungen sowie Hinweise, Learning-Experience-Plattformen/immersive Labs und Gamification, welche allesamt technische Massnahmen sind. Zu den personellen Massnahmen gehören Standard-Onboardings, Präsenzschulungen, Basisschulungen, spezifische Schulungen, Sensibilisierungskampagnen, Sicherheitsrichtlinien und Vorschriften. Die Zahl der gemeldeten und genannten Cybervorfälle zeigt, dass es immer noch viele Fälle gibt, die nicht gemeldet werden. Es ist daher wesentlich, dass Unternehmen und Mitarbeitende bei Verdacht auf einen Cyberangriff immer sofort reagieren und die entsprechenden Stellen informieren, um mögliche Schäden zu vermeiden oder zumindest zu minimieren. Es ist wichtig anzumerken, dass gamifizierte Awareness-Massnahmen allein nicht ausreichen, um eine umfassende Sicherheitskultur im Unternehmen zu etablieren. Dennoch können sie ein wirksames Instrument sein, um das Bewusstsein und das Interesse an Cybersecurity zu fördern. Indem diese Mitarbeitende spielerisch involvieren und positive Erfahrungen ermöglichen, tragen sie dazu bei, das Verständnis und die Motivation zur Umsetzung von Sicherheitsmassnahmen zu stärken. Durch die Literaturrecherche und Datenerhebung konnten verschiedene Faktoren untersucht werden, die das Verhalten der Benutzer in Bezug auf Cybersecurity beeinflussen können. Dazu gehören der Einfluss von Peers, die Informationssicherheitspolitik, das Verhalten, das Bildungsniveau und das Wissen der Benutzer selbst, Faktoren wie Alter und Erfahrung, die Sichtbarkeit und die Beteiligung am Sicherheitsmanagement sowie Aspekte der Kultur und des Arbeitsumfelds. Der Einfluss von Peers spielt eine bedeutende Rolle im Cybersicherheitsverhalten. Menschen neigen dazu, sich an den Verhaltensweisen und Meinungen ihrer Kollegen zu orientieren. Wenn Peers ein sicheres Verhalten zeigen und die Wichtigkeit von Cybersecurity betonen, steigt die Wahrscheinlichkeit, dass andere Benutzer ähnliche Verhaltensweisen übernehmen. Um diesen Einfluss zu maximieren, ist es wichtig, dass Cybersecurity in der gesamten Organisation kommuniziert und gefördert wird.

Awareness-Massnahme Gamification: Escape-Rooms

Gamifizierte Awareness-Massnahmen in Unternehmen haben laut Experten mehrere Vorteile. Sie entmystifizieren das Thema Sicherheit und Datenschutz, fördern die aktive Auseinandersetzung der Mitarbeitenden und schaffen Vertrauen in ihre Fähigkeiten. Die interaktiven Spiele und Trainings bieten eine unterhaltsame Art der Wissensvermittlung. Escape-Rooms stärken die Team- und Zusammenarbeit, während das erworbene Wissen länger im Gedächtnis bleibt. Gamifizierte Massnahmen ermöglichen es den Mitarbeitenden, komplexe Sicherheitskonzepte spielerisch zu erfassen und Berührungsängste abzubauen. Sie können zeigen, dass Cybersecurity zugänglich und beherrschbar ist. Die Interaktion und haptische Erfahrung helfen dabei, reale Herausforderungen zu verstehen und zu bewältigen. Allerdings wird die Messung von Escape-Rooms als Herausforderung betrachtet.

5.2 Interpretation der Ergebnisse

Um die zu Beginn formulierten Fragestellungen zu beantworten, werden sowohl der theoretische Hintergrund als auch die Datenerhebung herangezogen.

Fragestellung 1: *Welchen Beitrag leisten Awareness-Massnahmen zur Verbesserung der Cybersecurity?*

Awareness-Massnahmen, also die Bewusstseinsschaffung, spielen eine entscheidende Rolle bei der Verbesserung der Cybersicherheit, da sie das Sicherheitsbewusstsein der Mitarbeitenden erhöhen und ihr Verhalten positiv beeinflussen können. Diese Massnahmen informieren die Mitarbeitenden über aktuelle sowie potenzielle Bedrohungen und lenken ihre Wahrnehmung auf das Thema. Insbesondere interaktive Schulungen haben sich als wirksame Awareness-Massnahme erwiesen. Allerdings zeigen die Ergebnisse, dass diese Massnahmen nur nützlich sind, wenn die Mitarbeitenden die Schulungen und das erlernte Wissen aktiv nutzen und in ihren Alltag integrieren. Selbst im Rahmen zahlreicher Schulungen und Trainings helfen Awareness-Massnahmen nicht, wenn die Menschen das Thema nicht als relevant erachten. Die theoretischen und praktischen Ergebnisse zeigen, dass Hackerangriffe trotz der Schulungen und Trainings, die Unternehmen für ihre Mitarbeitenden anbieten, weiterhin zunehmen. Der Mensch bleibt die fehleranfälligste Stelle. Dennoch können Awareness-Massnahmen

einen bedeutenden Beitrag zur Verbesserung der Cybersecurity leisten, insbesondere wenn sie offen, spielerisch und interaktiv gestaltet sind.

Unterfragestellung 1.1: *Welche Faktoren beeinflussen die Wirksamkeit solcher Massnahmen?*

Es ist fundamental, dass Awareness-Massnahmen kontinuierlich durchgeführt und regelmässig aktualisiert werden, um den sich ständig wandelnden Bedrohungen gerecht zu werden. Um die geeignete Awareness-Massnahme auszuwählen, ist es notwendig, den aktuellen Stand der Sicherheitsfaktoren im Unternehmen zu verstehen. Die Wirksamkeit von Awareness-Massnahmen in Unternehmen kann von verschiedenen Faktoren beeinflusst werden. Zum einen ist die Relevanz der vermittelten Inhalte entscheidend, da es von Bedeutung ist, dass die Benutzer die Informationen als relevant für ihren Arbeitsbereich und ihre täglichen Aufgaben wahrnehmen. Das Engagement und die Unterstützung der Führungsebene sind ebenfalls entscheidend für den Erfolg von Awareness-Massnahmen. Wenn die Führungskräfte die Bedeutung von Cybersicherheit betonen und selbst zeigen, werden die Benutzenden eher motiviert, sich sicherheitsbewusst zu verhalten. Auch die Wahl der passenden Schulungsmethoden kann die Wirksamkeit von Awareness-Massnahmen beeinflussen. Interaktive Schulungen, Simulationen und praktische Übungen können das Lernen und die Umsetzung von Sicherheitspraktiken fördern. Es ist allerdings zu beachten, dass Unternehmen neben Awareness-Massnahmen auch eine Kultur schaffen, in der die Mitarbeitenden offen ihre Fragen stellen können und gehört werden. Abschliessend sind die individuelle Meinung und die Einstellung zum Thema weitere Faktoren, welche die Wirksamkeit solcher Massnahmen beeinflussen.

Fragestellung 2: *Inwieweit können Escape-Rooms als Methode zur Schulung von Cybersecurity-Awareness eingesetzt werden?*

Escape-Rooms können eine geeignete Methode zur Schulung von Cybersecurity-Awareness-Massnahmen darstellen. Aus der erarbeiteten Theorie und den Interviews konnte erkannt werden, dass Escape-Rooms als innovative Methode zur Schulung von Cybersecurity-Awareness eingesetzt werden können. Sie bieten den Teilnehmenden eine praxisnahe, interaktive und erlebnisorientierte Lernumgebung. Zudem fördern Escape-Rooms die Zusammenarbeit und den Teamgeist, denn die Teilnehmenden müssen zusammenarbeiten, um Rätsel zu lösen, Hinweise zu finden und Sicherheitsprobleme zu

lösen. Dies spiegelt die Bedeutung der Zusammenarbeit bei der Bewältigung von Cybersicherheitsproblemen wider, da in der realen Welt die meisten Sicherheitsvorfälle durch das Zusammenspiel von Technologie, Prozessen und Menschen verursacht werden. Auch die geschilderten Herausforderungen der Experten lassen sich zum Teil mit einem Escape-Room umgehen: Eine genannte Herausforderung war es, eine Räumlichkeit zu schlichten. Ein Escape-Room kann die Räumlichkeiten bieten, sodass Mitarbeitende ausserhalb des gewohnten Arbeitsfeldes den Escape-Room spielen können. Eine weitere Herausforderung betrifft die Ressourcenproblematik: Mit einem Escape-Room sollten grösstenteils die organisatorischen Aufwände für Unternehmen entfallen. Somit sollten auch keine Kosten für Unterkunft, Verpflegung oder Fahrten entstehen. Eine weitere genannte Herausforderung ist die Konzentrationsfähigkeit: Bei Escape-Rooms ist die Gefahr geringer, dass sich Mitarbeitende durch betriebsabhängige Störungen ablenken lassen. Für dezentrale Unternehmen könnte ein mobiler Escape-Room eingesetzt werden, um ihn an verschiedenen Standorten anzubieten. Eine weitere Herausforderung ist der kritische Alltagsbezug: In einem Escape-Room können realistische Szenarien aus der Cybersecurity-Welt integriert werden, um den Lernprozess zu stärken und dazu beizutragen, das Wissen auch ausserhalb der Schulung anzuwenden. Es sei allerdings darauf hingewiesen, dass auch andere Awareness-Massnahmen, unabhängig vom Escape-Room, durchgeführt werden müssen.

Unterfragestellung 2.2: *Welche Rahmenbedingungen tragen zur Wirksamkeit dieser Methode bei?*

Die Erlebnispyramide von Tarssanen (2009b) versucht, die verschiedenen Ebenen des Erlebens und der emotionalen Bindung von Menschen an bestimmte Aktivitäten oder Ereignisse zu beschreiben. Um die Wirksamkeit dieser Methode zu erhöhen, müssen bestimmte Rahmenbedingungen eingehalten werden. Bei der Gestaltung eines Escape-Rooms kann der Erlebnisanbieter gewisse Aspekte beeinflussen, die in der Erlebnispyramide von Tarssanen auf der horizontalen Achse dargestellt werden. In der folgenden Tabelle 1 lassen sich die zentralen Aspekte zusammenfassen:

Tabelle 1: Eigene Darstellung der Ebenen auf der horizontalen Achse von Tarssanen (2009b)

Ebene	Besonderheiten
Individualität	- Einzigartig und auf das Unternehmen zugeschnitten

	- Idealerweise lässt sich das Produkt nicht anderswo finden. - Den Gast aktiv in die Gestaltung des Erlebnisses einbeziehen
Authentizität	- Wird durch persönliche Wahrnehmungen und frühere Erfahrungen des Gastes beeinflusst - Je authentischer die Geschichte, desto realistischer das Erlebnis
Geschichte	- Eng mit der Authentizität verbunden - Geschichte soll während des Erlebnisses kohärent sein - Das Thema in eine Geschichte verpacken, welche die Gäste in eine imaginäre Welt entführen soll - Je überzeugender die Geschichte, desto authentischer und glaubwürdiger das Erlebnis - Geschichte mit Emotionen verbinden
Multisensorische Wahrnehmung	- Alle fünf Sinne sowie persönliche Erinnerungen und Emotionen einbeziehen → existiert nur während des Erlebnisses
Interaktion	- Es sollten unterschiedliche Interaktionen berücksichtigt werden, um das Gruppengefühl zu stärken. → existiert nur während des Erlebnisses
Kontrast	- Je individueller das Erlebnis, desto stärker der Kontrast zum Alltag

5.3 Handlungsempfehlungen

Da die Erlebnispyramide von Tarssanen im Jahr 2009 entwickelt wurde, war es angebracht, sie basierend auf den Ergebnissen und Implikationen der Arbeit zu überarbeiten, um die Einflussnahme des Erlebnisanbieters graphisch darzustellen. Diese aktualisierte Version wird in der nachfolgenden Abbildung 3 präsentiert.

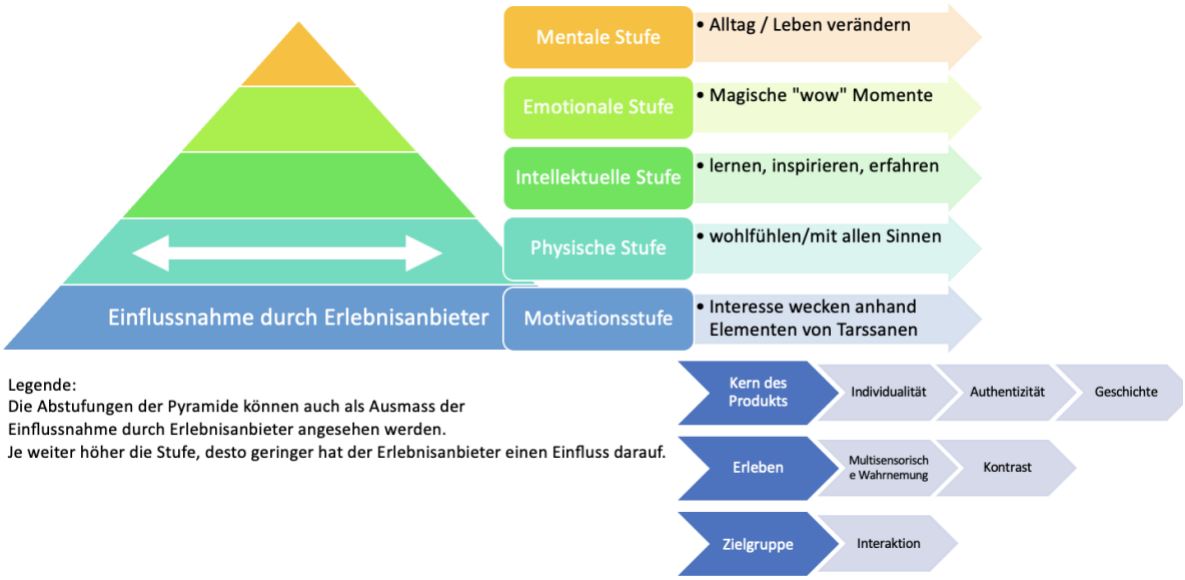

Abbildung 3: Eigene Abbildung der Erlebnispyramide in Anlehnung an Tarssanen (2009b)

Dazu gehören die Individualität, die Authentizität, die Geschichte, der Kontrast und die multisensorische Wahrnehmung, welche der Erlebnisanbieter bewusst beeinflussen kann. Der Erlebnisanbieter sollte versuchen, alle diese Ebenen zu integrieren, um ein ganzheitliches und ansprechendes Erlebnis zu schaffen. Die Ebenen auf der vertikalen Achse können vom Erlebnisanbieter nur bedingt oder gar nicht beeinflusst werden, wie der Pfeil in der Abbildung 3 verdeutlicht. Je höher eine Stufe in der Pyramide liegt, desto stärker wird sie von subjektiven Faktoren geprägt. Die Stufen auf der vertikalen Achse hängen von den individuellen Erfahrungen, Vorlieben und Persönlichkeiten der Teilnehmenden ab. Bei der Betrachtung von Erlebnissen sollen auch verschiedene Interaktionsperspektiven berücksichtigt werden, um die Wirksamkeit dieser Methode zu erhöhen. Um sicherzustellen, dass die Teilnehmerinnen und Teilnehmer von den Cybersecurity-Escape-Rooms optimal profitieren, ist es entscheidend, spannende Lehrmaterialien zu entwickeln. Diese sollten leicht verständlich und informativ gestaltet sein. Dabei sollten unterschiedliche Medien verwendet werden, um die Aufmerksamkeit der Teilnehmenden aufrechtzuerhalten. Es ist wichtig, dass die Materialien sowohl für technische als auch für nichttechnische Personen zugänglich sind, um eine umfangreiche Zielgruppe anzusprechen. Eine mögliche Massnahme, die Unternehmen in Betracht ziehen könnten, ist die Entwicklung eines Belohnungssystems, insbesondere für Mitarbeitende, die die Vorschriften

und Regeln zur Cybersecurity befolgen. Dadurch könnten andere Mitarbeitende von ihren Kollegen lernen, was wiederum Auswirkungen auf die Bedrohungs- und Reaktionswahrnehmung von Mitarbeitenden haben kann. Im Laufe der Forschung wurde festgestellt, dass das Thema Cybersecurity-Awareness möglicherweise weniger komplex ist als zunächst angenommen. Wesentliche Erkenntnisse aus den Experteninterviews legen nahe, dass bereits die Verwendung eines einmaligen und sicheren Passworts oder die Skepsis gegenüber verdächtigen E-Mails einen Einfluss auf die Cybersecurity eines Unternehmens haben können. Viele Menschen haben die Vorstellung, dass das Thema komplex ist und dass sie machtlos dagegen sind. Die Untersuchung hat jedoch gezeigt, dass dahinter machbare und einfache Prozesse stehen. Menschen sollten verstehen, dass jede einzelne Person aktiv zur Schaffung von Awareness beitragen kann.

Die Erkenntnisse dieser Arbeit legen nahe, dass es entscheidend ist, den Mythos der Unzugänglichkeit und Überwältigung im Zusammenhang mit Cybersecurity zu entkräften. Indem Menschen erkennen, dass sie selbst in der Lage sind, einen Beitrag zur Sicherheit zu leisten, kann eine positive Veränderung des Sicherheitsbewusstseins und -verhaltens herbeigeführt werden. Unternehmen sollten daher Schulungen und Sensibilisierungsmassnahmen entwickeln, die auf einfachen und verständlichen Prozessen aufbauen. Ein vielversprechender Ansatz dafür könnte die Integration eines Escape-Rooms sein. Mithilfe der Erlebnispyramide von Tarssanen und der formulierten Erlebnisstufen sollte es möglich sein, ein umfassendes und eindrucksvolles Erlebnis zu schaffen. Der Escape-Room kann so gestaltet werden, dass er die wesentlichsten Aspekte der Erlebnispyramide von Tarssanen berücksichtigt. Abschliessend soll darauf hingewiesen werden, dass es im Bereich der Cybersecurity oft schwierig ist, konkrete Handlungsempfehlungen abzuleiten. Dies ist darauf zurückzuführen, dass die Cyber-Bedrohungslandschaft ständig im Wandel ist, stetig neue Angriffsmethoden entwickelt werden.

5.4 Beschränkungen der Forschung

In der vorliegenden Arbeit wird die Forschung auf die Untersuchung der Effektivität von spielbasierten Ansätzen wie Escape-Rooms eingeschränkt. Es werden ausschliesslich Auswirkungen mit dieser spezifischen spielerischen Massnahme auf das Verhalten und die

Einstellungen der Mitarbeitenden betrachtet. Andere spielbasierte Ansätze werden in dieser Arbeit nicht berücksichtigt. Darüber hinaus ist anzumerken, dass die Forschung nicht auf eine bestimmte Organisation oder eine quantitative Datenanalyse fokussiert ist. Die Ergebnisse können daher nicht verallgemeinert werden, sondern sind auf den spezifischen Kontext des Escape-Rooms begrenzt. Diese Beschränkungen der vorliegenden Forschung bieten Raum für zukünftige Arbeiten, um die Effektivität und Anwendbarkeit spielbasierter Ansätze in verschiedenen Kontexten und Organisationen weiter zu untersuchen. Es wäre spannend, die Kosten-Nutzen-Aspekte zu berücksichtigen und die Übertragbarkeit auf andere Branchen sowie Organisationen zu erforschen.

5.5 Ausblick

Eine vielversprechende Richtung wäre die Untersuchung der langfristigen Auswirkungen solcher Ansätze auf das Verhalten und die Einstellung der Mitarbeitenden im Hinblick auf Cybersecurity. Angesichts der Herausforderungen bei der Skalierbarkeit und der Quantifizierung des Lerneffekts nach dem Escape-Room wäre es interessant zu erforschen, ob positive Veränderungen im Verhalten und in der Einstellung langfristig beibehalten werden können. Des Weiteren wäre eine Analyse der Rollen von Team- und Zusammenarbeit in spielerischen Umgebungen für die Verbesserung der Cybersecurity-Fähigkeiten der Mitarbeitenden relevant, um festzustellen, wie sich die Fähigkeiten der Mitarbeitenden verbessern könnten. Die Erlebnispyramide von Tarssanen (2009b) bietet einen möglichen Rahmen für die Gestaltung von Escape-Rooms zur Vermittlung von Cybersecurity-Wissen. Daher wäre es interessant, weitere Forschungen durchzuführen, um zu ermitteln, wie die Motivation und Belohnungssysteme in spielbasierten Ansätzen wirksam genutzt werden können. Eine weitere Fragestellung betrifft die Übertragbarkeit der Ergebnisse auf verschiedene Branchen und Organisationen.

Es wäre spannend zu untersuchen, ob die Effektivität und Wirksamkeit spielbasierter Ansätze in unterschiedlichen Kontexten ähnlich sind oder ob spezifische Anpassungen erfolgen müssen. Da einige Experten die Ressourcenplanung und die Kosten-Nutzen-Abwägung als eher gering einschätzen, wäre es interessant, eine Kosten-Nutzen-Analyse durchzuführen.

Diese Forschungsbereiche können das Verständnis und die Anwendung von spielbasierten Ansätzen zur Verbesserung der Cybersecurity in Unternehmen vorantreiben.

Literaturverzeichnis

Atteslander, P. (2010). *Methoden der empirischen Sozialforschung.* Berlin: Erich Schmidt Verlag GmbH & Co.

Clinton, L., & Barrack, S. (2018). *Management von Cyber-Risiken: Handbuch für Unternehmensvorstände und Aufsichtsräte.* Arlington, USA: Internet Security Alliance.

DeCusatis, C., Gormanly, B., Alvarico,, E., Dirahoui, O., McDonough, J., Sprague, B., (…) Mah Marist , B. (2022). *A Cybersecurity Awareness Escape Room using Gamification Design Principles.* Las Vegas: IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC).

Denning, T., Lerner, A., Shostack, A., & Kohno, T. (2013). *Control-Alt-Hack: the design and evaluation of a card game for computer security awareness and education.*

Farooq, A., Isoaho, J., Virtanen, S., & Isoaho, J. (2015). An Analysis of Students Individual Factors. *Information Security Awareness in Educational Institution*, pp. 352-359.

Flick, U. (2009). *An introduction to qualitative research.* Thousand Oaks: Sage.

Garz, D., & Kraimer, K. (1991). *Qualitativ-empirische Sozialforschung: Konzepte, Methoden, Analysen. 1. Auflage.* Opladen: Westdeutscher Verlag.

Gläser, J., & Laudel, G. (2010). *Experteninterviews und qualitative Inhaltsanalyse als Instrument rekonstruierender Untersuchungen.* Wiesbaden: VS Verlag für Sozialwissenschaften.

Hamari, J., Koivisto, J., & Majuri, J. (May 2018). Gamification of education and learning: A review of empirical literature. *GamiFIN Conference*, S. 11-19.

Han, J., Kim, Y., & Kim, H. (2017). An integrative model of information security policy compliance with psychological contract: Examining a bilateral perspective. *Computers & Security*, S. 52-65.

Heikkinen, O., & Shumeyko, J. (2016). *Designing an escape room with the Experience Pyramid model.* Haaga-Helia.

Helfferich, C. (2011). *Die Qualität qualitativer Daten. Manual für die Durchführung qualitativer Interviews.* Hamburg: VS-Verlag.

Hwang, I., Wakefield, R., Kim, S., & Kim, T. (2019). Security Awareness: The First Step in Information Security Behavior. *Journal of Computer Information Systems*, pp. 1-12.

Klipper, S. (2015). *Cyber Security.* Kiel: Springer.

Löffler, E., Schneider, B., Asprion, P., & Zanwar, T. (2021). *CySecEscape 2.0—A Virtual Escape Room To Raise Cybersecurity Awareness.* International Journal of Serious Games.

Li, L., Xu, L., Chen, Y., & Chen, H. (2016). Cyber Security Awareness and Its Impact on Employee's Behavior. In A. Tjoa, L. Xu, M. Raffai, & N. Novak, *Research and Practical Issues of Enterprise Information Systems* (pp. 110-118). Vienna, Austria: Springer.

Liedtke, T. (2022). *Informationssicherheit - Möglichkeit und Grenzen.* Remseck: Springer.

Mayring, P. (2010). *Qualitative Inhaltsanalyse. In: Mey, G., Mruck, K. (eds) Handbuch Qualitative Forschung in der Psychologie. VS Verlag für Sozialwissenschaften.* https://doi.org/10.1007/978-3-531-92052-8_42.

Mayring, P. (2015). *Einführung in die qualitative Sozialforschung (6. Aufl).* Weinheim: Beltz.

Nationales Zentrum für Cybersicherheit NCSC. (11. Mai 2023). *NCSC Halbjahresbericht 2022/II (Juli - Dezember).* Von Schweizerische Eidgenossenschaft: https://www.ncsc.admin.ch/ncsc/de/home/dokumentation/medienmitteilungen/newslist.msg-id-95071.html abgerufen am 01.05.2023

Palmas, F., & Niermann, P.-J. (2021). *Extended Reality Training.* Wiesbaden: Springer Gabler.

Pine, J., & Gilmore, J. (2011). *The Experience Economy: work is theatre and evey business a stage.* Boston: Harvard Business School Press.

Radoff, J. (2011). *Game On: Energize Your Business with Social Media Games.* Wiley.

Richter, S., Straub, T., & Lucke, C. (2018). *Information Security Awareness - eine konzeptionelle Neubetrachtung.* Lüneberg, Deutschland: Multikonferenz Wirschaftsinformatik.

Sharif, K., & Ameen, S. (2020). *A Review of Security Awareness Approaches With Special Emphasis on Gamification.* Duhok, Iraq: International Conference on Advanced Science and Engineering (ICOASE).

Shedroff, N. (2001). *Experience Design.* Indianapolis: New Riders.

Shouran, Z., Priyambodo, T., & Ashari, A. (2019, March). Information System Security: Humas Aspects. *Internatioal Journal of Scientific & Technology Research*.

Tarssanen, S. (2009b). *Handbook for Experience Stagers.5th Edition.* Rovaniemi: LEO, Lapland Center of Expertise for the Experience Industry.

Toth, P., & Klein, P. (2013). *A role-based model for federal information technology/cyber security training.* Federal Organizations: NIST Special Publication.

Weber, K., Schütz, A., & Fertig, T. (2019). *Grundlagen und Anwendung von Information Security Awareness.* Wiesbaden: Springer.

Wolfenden, B. (2019, Mai). Gamification as a winning cyber security strategy. *Computer Fraud & Security*, pp. 9-12.

Abbildungsverzeichnis

Abbildung 1: Die Erlebnispyramide von Tarssanen (2009b) horizontale Achse 14

Abbildung 2: Die Erlebnispyramide von Tarssanen (2009b) vertikale Achse……16

Abbildung 3: Eigene Abbildung der Erlebnispyramide in Anlehnung an Tarssanen (2009b)……..49

Tabellenverzeichnis

Tabelle 1: Eigene Darstellung der Ebenen auf der horizontalen Achse von Tarssanen (2009b) 46