HAW HAMBURG

Bachelorarbeit

Dominik Martin

Cyber-Sicherheitsbewusstsein im Hochschulkontext: Untersuchung von Awareness-Maßnahmen und Tool-Evaluation für eine nachhaltige Implementierung

Fakultät Technik und Informatik
Department Informatik

Faculty of Engineering and Computer Science
Department Computer Science

Dominik Martin

Cyber-Sicherheitsbewusstsein im Hochschulkontext: Untersuchung von Awareness-Maßnahmen und Tool-Evaluation für eine nachhaltige Implementierung

Bachelorarbeit eingereicht im Rahmen der Bachelorprüfung
im Studiengang *Bachelor of Science Angewandte Informatik*
am Department Informatik
der Fakultät Technik und Informatik
der Hochschule für Angewandte Wissenschaften Hamburg

Betreuender Prüfer: Prof. Dr. Klaus-Peter Kossakowski
Zweitgutachter: Prof. Dr. Olaf Zukunft

Eingereicht am: 04. Juli. 2024

Dominik Martin

Thema der Arbeit

Cyber-Sicherheitsbewusstsein im Hochschulkontext: Untersuchung von Awareness-Maßnahmen und Tool-Evaluation für eine nachhaltige Implementierung

Stichworte

IT-Sicherheit, Informationssicherheit, Informationssicherheitsbewusstsein, Sensibilisierung

Kurzzusammenfassung

Social-Engineering gehört zu den Hauptbedrohungen im Cyber-Bereich. Besonders Phishing wird in diesem Bereich häufig von Angreifern verwendet. Auch Hochschulen blieben nicht unversehrt. Eine Vielzahl an Hochschulen registrierter Informationssicherheitsvorfälle, welche wiederum zu gravierenden Konsequenzen führten, darunter der Ausfall von IT-Systemen sowie die unerlaubte Veröffentlichung sensibler Daten. Um IT-Sicherheitsvorfälle vorzubeugen und diese zu minimieren, ist es wichtig, dass sich die Nutzer sicher verhalten, denn menschliches Versagen stellt die Ursache für den Großteil der Sicherheitsvorfälle dar. Deshalb ist es von entscheidender Bedeutung, die Nutzer im Bereich der Informationssicherheit zu schulen und zu sensibilisieren. Das Ziel dieser Bachelorarbeit besteht darin, verschiedene Aspekte eines Cyber-Security-Awareness-Konzeptes zu untersuchen, um deren Eignung für den Hochschulbereich einschätzen zu können, sodass diese Arbeit von Hochschulen zur Entwicklung eines Cyber-Security-Awareness-Konzeptes genutzt werden kann.

Dominik Martin

Title of Thesis

Cyber security awareness in the university context: investigation of Awareness measures and tool evaluation for a sustainable implementation

Keywords

Cyber-Security, Cyber-Security-Awareness, Cyber-Security-Awareness-Program

Abstract

Social engineering is one of the main threats in the cyber area. Phishing in particular is frequently used by attackers in this area. Universities have not remained unscathed. A large number of universities registered information security incidents, which in turn led to serious consequences, including the failure of IT systems and the unauthorized publication of sensitive data. In order to prevent and minimize IT security incidents, it is important that users behave securely. This is because human error is often the cause of the majority of security incidents. Consequently, it is crucial to train and sensitize users in the area of information security. The aim of this bachelor thesis is to examine various aspects of a cyber security awareness concept in order to assess its suitability for the higher education sector, so that this work can be used by universities to develop a cyber security awareness concept.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

1.1 Motivation

Laut dem Threat-Landscape-Report-2023 der ENISA (European Union Agency for Cybersecurity), gehört Social-Engineering zu den Hauptbedrohungen im Cyber-Bereich [14, ENISA, 2023]. Besonders Phishing wird in diesem Bereich häufig von Angreifern verwendet. Die APWG (Anti-Phishing Working Group) zählte im Jahr 2023 1.286.208 Phishing-Angriffe [4, APWG, 2023]. Dabei haben sich die Phishing-Angriffe in den letzten zehn Jahren fast verzehnfacht (Abbildung: 1.1). Phishing-Angriffe missbrauchen das Vertrauen von Nutzern durch gefälschte Kommunikation, oft per E-Mail, wobei sich Angreifer als vertrauenswürdige Personen ausgeben. Ihr Hauptziel ist es, sensible Informationen zu stehlen und IT-Infrastrukturen zu kompromittieren.

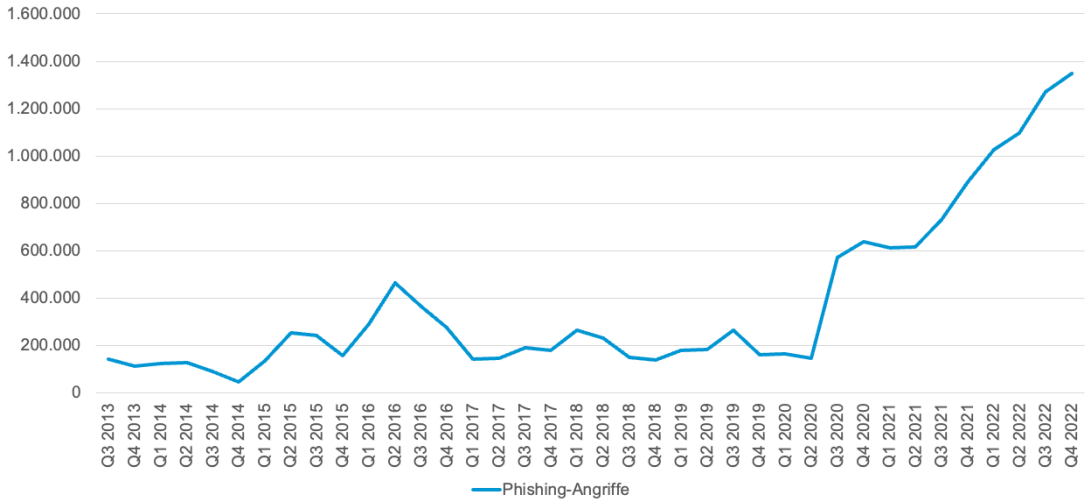

Abbildung 1.1: Phishing-Angriffe Q3 2013 - Q4 2022
Quelle: Eigene Darstellung in Anlehnung an [3, APWG, 2023]

Besonders für Hochschulen, die eine Vielzahl von persönlichen Daten und Forschungsinformationen verwalten, stellt dies ein erhebliches Risiko dar.

Wie aus der Statistik von B. Kondruss hervorgeht, wurden im Jahr 2023 weltweit über 100 Cyberangriffe auf Hochschulen registriert, wovon 16 Angriffe deutsche Hochschulen betrafen [35, Kondruss]. Diese Angriffe führten häufig zu gravierenden Konsequenzen, darunter der Ausfall von IT-Systemen sowie die unerlaubte Veröffentlichung sensibler Daten.

Um Informationssicherheitsvorfälle vorzubeugen und diese zu minimieren ist es wichtig, dass sich die Nutzer den Richtlinien ihrer Organisation konform verhalten. Doch dies ist meist nicht der Fall [5, Bada et al., 2015]. Laut Khando et al., 2021, stellt menschliches Versagen die direkte oder indirekte Ursache für den Großteil der Informationssicherheitsvorfälle dar, sowohl absichtliche als auch unabsichtliche Fehlhandlungen [24, Khando et al., 2021]. Dafür kann es viele Gründe geben. Es könnte sein, dass die Nutzer nichts von den Richtlinien wissen oder sich der Risiken nicht bewusst sind.

Folglich ist es von entscheidender Bedeutung, die Nutzer über die Risiken von Cyberangriffen, insbesondere hinsichtlich der Methoden des Social-Engineerings, aufzuklären und ihr Bewusstsein zu schärfen. Die Nutzer sollten wissen, wie sie Cyber-Angriffe wie zum Beispiel eine Phishing-Mail erkennen können und darauf reagieren oder wie sie mit sensiblen Daten in ihrer Organisation umgehen sollten.
Dabei ist es ebenfalls von hoher Bedeutung, den Nutzern zu vermitteln, wie sie erkannte Sicherheitsvorfälle innerhalb der Organisation melden. Ohne die Meldung von Sicherheitsvorfällen ist die Organisation nicht in der Lage, angemessen auf diese zu reagieren. Eine Organisation sollte klar definierte Meldewege und Prozesse festlegen, die es den Nutzern ermöglichen, Sicherheitsvorfälle zu melden und der Organisation die Auswertung dieser Meldungen zu ermöglichen. Diese Verfahren sollten innerhalb eines Cyber-Security-Awareness-Konzeptes den Nutzern vermittelt werden.

Mit welchen Methoden und Programmen die Nutzer im Hochschulbereich effektiv geschult werden oder auch welche psychologischen Einflussfaktoren wichtig sind und wie das Bewusstsein für Cyber-Security gemessen werden kann, wird Teil dieser Bachelorarbeit.

1.2 Ziel

Das Ziel dieser Bachelorarbeit besteht darin, verschiedene Aspekte eines Cyber-Security-Awareness-Konzeptes zu untersuchen, um deren Eignung für den Hochschulbereich einzu-

schätzen. Zu diesen Aspekten gehören unter anderem die Methoden, welche zur Sensibilisierung im Bereich Cyber-Security eingesetzt werden, die Faktoren, die das menschliche Verhalten in diesem Kontext beeinflussen und die Messmethoden, welche dabei helfen, das Cyber-Security-Bewusstsein der Nutzer zu messen.

Zusätzlich zur Untersuchung der Awareness-Methoden werden passende Applikationen evaluiert und auf Eignung für den Einsatz im Hochschulbereich untersucht. Das Ziel hierbei ist es, aufzuzeigen, welche Möglichkeiten bestehen, die Awareness-Methoden möglichst automatisiert zu betreiben und dabei gleichzeitig die Aspekte der Nutzerfreundlichkeit, Funktionalität und Kosten zu berücksichtigen.

Das übergeordnete Ziel besteht darin, die Informationssicherheit von Hochschulen nachhaltig zu stärken und die bestmöglichen Awareness-Methoden, Applikationen und Ansätze für den Hochschulbereich aufzuzeigen. Diese Arbeit soll dazu genutzt werden können, innerhalb einer Hochschule ein Cyber-Security-Awarenes-Konzept aufzubauen. Dabei sollen die grundlegenden Aspekte eines Cyber-Security-Awareness-Konzeptes beachtet werden. Ein umfassendes Gesamtkonzept wird jedoch nicht präsentiert, weil dieses auf die jeweilige Organisation zugeschnitten sein muss.

1.3 Zielgruppe

Diese Bachelorarbeit soll Hochschulen zur Verfügung stehen. Sie bietet eine fundierte Grundlage, auf der Hochschulen ein Cyber-Security-Awareness-Konzept aufbauen können.

Die Arbeit soll Administratoren, IT-Sicherheitsbeauftragten und Entscheidungsträgern im Hochschulbereich dienen, indem sie Einblicke in die verschiedenen Cyber-Security-Awareness-Methoden verschafft und vermittelt, wie diese angewendet werden können. Darüber hinaus richtet sie sich an Akademiker und Forschende im Bereich der Cybersicherheit, die an der Entwicklung, Evaluation und Implementierung von Cyber-Security-Awareness-Konzepten interessiert sind.

1.4 Struktur der Arbeit

Diese Bachelorarbeit gliedert sich nach der Einleitung in fünf verschiedene Kapitel.

Kapitel zwei befasst sich mit den Grundlagen und definiert Cyber-Security-Awareness. Darüber hinaus wird erläutert, wie ein Cyber-Security-Awareness-Konzept aufgebaut ist und welche Methoden genutzt werden kann, um dieses aufzubauen. Außerdem wird der Social-Engineering-Angriff als Beispiel für Cyber-Angriffe mit Menschen als Zielobjekte erklärt, um zu betonen, weshalb Cyber-Security-Awareness von großer Bedeutung ist.

Kapitel drei befasst sich mit den verschiedenen Cyber-Security-Awareness-Methoden und den psychologischen Einflussfaktoren. Hier werden die Methoden untersucht, wobei spezifische Kriterien, wie Effektivität im Sinne der Einprägung, Zeitaufwand, Nutzerfreundlichkeit, Unterhaltsamkeit und Hochschuleignung, berücksichtigt werden. Neben den Methoden werden auch psychologische Einflussfaktoren untersucht, welche Auswirkungen auf das menschliche Verhalten in Bezug auf die Informationssicherheit haben.

Im vierten Kapitel werden verschiedene Messmethoden untersucht, welche dazu dienen, das Bewusstsein der Nutzer im Cyber-Security-Bereich zu messen. Dies ist ein wichtiger Bestandteil eines jeden Cyber-Security-Awareness-Konzeptes, damit regelmäßig die Effektivität der eingesetzten Maßnahmen geprüft und diese gegebenenfalls angepasst werden können.

In Kapitel fünf erfolgt eine Evaluation relevanter Applikationen. Dabei werden im ersten Schritt Anforderungen und Bewertungskriterien für die Applikationen aufgestellt und im Anschluss anhand dieser bewertet, um einen Vergleich ziehen zu können.

Abschließend wird in Kapitel sechs die Arbeit zusammengefasst und ein Fazit mit einem Ausblick präsentiert.

Die einzelnen Kapitel, insbesondere die Kapitel drei bis fünf, dienen als einzelne Aspekte eines Cyber-Security-Awareness-Konzeptes und können von Hochschulen entsprechend genutzt werden, um ein eigenes ganzheitliches Cyber-Security-Awareness-Konzept zu entwickeln.

2 Grundlagen

In diesem Kapitel wird zunächst eine Definition der Cyber-Security-Awareness gegeben. Darüber hinaus werden grundlegende Themen erläutert, die in diesem Zusammenhang von Bedeutung sind. Es wird erklärt, wie ein Cyber-Security-Awareness-Konzept aufgebaut ist und gegen welche möglichen Cyber-Angriffe es schützen kann. Dabei wird Social-Engineering als Beispiel Angriff näher betrachtet.

Organisationen werden zunehmend Opfer von Cyber-Angriffen. Sowohl private als auch öffentliche Organisation sind Ziel solcher Angriffe. Insbesondere im Hochschulbereich wurde eine Vielzahl von Cyber-Angriffen registriert [35, Kondruss].

2.1 ISMS-Implementierung durch den PDCA-Zyklus zur Förderung der Cyber-Security-Awareness

Um den wachsenden Herausforderungen beim Schutz sensibler Informationen und IT-Infrastrukturen sowie bei der Implementierung geeigneter Schutzmaßnahmen gerecht zu werden, wurden weltweit 27.536 Organisationen in 150 Ländern nach der Norm ISO/IEC 27001 für 'Information Security Management Systems' (ISMS) zertifiziert, die von der International Organization for Standardization (ISO) und der International Electrotechnical Commission (IEC) herausgegeben wird. [48, Scholl et al., 2017]

Innerhalb eines ISMS werden Richtlinien entwickelt, welche dazu dienen die Sicherheitsrisiken der Organisation zu identifizieren, zu messen und entsprechende Maßnahmen einzuführen, um diese Risiken zu mildern oder zu beseitigen. Eine Zertifizierung des ISMS ermöglicht es der Organisation gegenüber externen Parteien glaubhaft zu belegen, dass sie sich aktiv, um die Informationssicherheit bemüht. Dies hilft dabei den externen Parteien, zum Beispiel den Studenten im Hochschulbereich, der Organisation, in dem Fall der Hochschule, ein gewisses Vertrauen aufzubauen. [47, Saint-Germain, 2005]

Die Entwicklung, Implementierung, Pflege und kontinuirliche Verbesserung des ISMS sind grundlegend für eine Zertifizierung. Um diesen Prozess zu durchlaufen, nutzen viele Organisation den Plan-Do-Check-Act (PDCA) Zyklus. Dies ist eine Vorgehensweise, um Prozesse iterativ zu betrachten und zu verbessern. Wie genau dieser angewendet wird um das ISMS zu entwickeln und kontinuirlich zu verbessern, beschreibt Tabelle 2.1. [47, Saint-Germain, 2005]

PDCA-Phase	Beschreibung
Plan (Entwicklung des ISMS)	• Definition des Geltungsbereiches des ISMS und der Informationssicherheitsrichtlinien • Identifizierung und Bewertung der Risiken • Auswahl von Kontrollzielen und Kontrollen, die zur Bewältigung dieser Risiken beitragen • Erstellung der Anwendbarkeitserklärung, in der die ausgewählten Kontrollen und deren Entscheidungen dokumentiert werden
Do (Implementierung und Durchführung des ISMS)	• Formulierung und Umsetzung eines Plans zur Risikominderung • Implementierung der zuvor ausgewählten Kontrollen, um die Kontrollziele zu erreichen
Check (Überwachung und Überprüfung des ISMS)	• Durchführung regelmäßiger Überprüfungen, um die Wirksamkeit des ISMS zu verifizieren
Act (Aufrechterhaltung und Verbesserung des ISMS)	• Ergreifen geeigneter Korrektur- und Präventivmaßnahmen sowie der ermittelten ISMS-Verbesserungen • Validierung der Verbesserungen

Tabelle 2.1: ISMS & PDCA-Zyklus

[47, Saint-Germain, 2005]

Im Rahmen des ISMS sind Organisationen verpflichtet, ihre Mitarbeiter hinsichtlich der Informationssicherheit zu sensibilisieren. Denn häufig stellt der unsachgemäße Umgang mit Informationen das größte Risiko dar. Das Bewusstsein der Mitarbeiter für die organisatorischen und persönlichen Konsequenzen eines unsachgemäßen Umgangs mit sensiblen Informationen ist entscheidend für den Erfolg einer Organisation. [48, Scholl et al., 2017]

2.2 Cyber-Security-Awareness

Nutzer, die nicht ausreichend für Informationssicherheit sensibilisiert sind, können nicht nur Fehler begehen, sondern auch Opfer verschiedener Cyber-Angriffe werden, die auf menschliches Verhalten abzielen, wie beispielsweise Phishing-Angriffe.

Laut Saad, 2021, kann Cyber-Security-Awareness als ein Zustand beschrieben werden, in dem sich die Nutzer einer Organisation im Idealfall ihrer Sicherheitsaufgabe verpflichtet fühlen. Dies bedeutet auch, dass die Nutzer den kritischen Charakter der besten Informationssicherheitspraktiken verstehen und sich der Sicherheitsaufgabe mitverantwortlich fühlen müssen. [2, Alahmari, 2021]

Ein Ziel der Cyber-Security-Awareness besteht unter anderem darin, die Zahl der Informationssicherheitsvorfälle zu reduzieren. Zudem sollte die Anzahl der von den Nutzern gemeldeten Sicherheitsvorfälle steigen. [59, Sykosch, 2022]

Dabei kann Cyber-Security-Awareness aus verschiedenen Blickwinkel betrachtet werden. Siponen, 2001, argumentiert, dass es fünf Dimensionen gibt, aus denen Cyber-Security-Awareness heraus betrachtet werden kann. Diese fünf Dimensionen sind: Die Organisatorische Dimension, die Allgemein Öffentliche Dimension, die Sozialpolitische Dimension, die Computer-Ethische Dimension und die institutionelle Bildungs Dimension. [51, Siponen, 2001]

In der Organisatorischen Dimension geht es vor allem darum, dass Level der Informationssicherheit innerhalb von Organisationenn hoch zu halten. Dies lässt sich nur gestalten, wenn die Nutzer ein Bewusstsein dafür entwickeln, wie sie mit den Technologien umgehen und wie Sie sich verhalten müssen im Bereich der Informationssicherheit. [51, Siponen, 2001]

In der Allgemein Öffentlichen Dimension geht es, um die private Informationssicherheit der einzelnen Personen. Es wird argumentiert, dass jede Person heutzutage etwas Verständnis für das Thema Informationssicherheit benötigt, im alltäglichem Umgang mit der digitalen Welt, um die eigenen Daten (wie zum Beispiel Kreditkarteninformationen) zu schützen. [51, Siponen, 2001]

Die dritte Dimension, die Sozialpolitische Dimension beschreibt die Cyber-Security-Awareness für Personen im politischen Bereich, wie zum Beispiel Staatsanwälte, Politiker oder auch die Regierung. Die Regierung eines Landes stellt digitale Lösungen für die Bevölkerung bereit. Wenn es hier zu Ausfällen aufgrund eines Cyber-Angriffes kommen sollte, könnte dies zu schwerwiegenden Konsequenzen führen. Deshalb ist eine nachhaltige Sensibilisierung in diesem Bereich wichtig. [51, Siponen, 2001]

Die Computer-Ethische Dimension verfolgt das Ziel, erstens relevante Informationen, beispielsweise technischer Natur, für Computerethiker bereitzustellen und zweitens deren Expertise zu erweitern und zu nutzen. Diese Wissenschaftler beschäftigen sich unter anderem mit ethischen Dilemmata und Problemen im IT-Bereich, wobei eine kontinuierliche Aktualisierung von Themen, einschließlich technischer Fakten, von großer Bedeutung ist. Forscher im Bereich der Informationssicherheit können wertvolle Unterstützung leisten, indem sie Informationen über Sicherheitsprobleme bereitstellen, die Computerethiker für die Analyse ihrer Kernthemen verwenden können.[51, Siponen, 2001]

Die letzte Dimension ist die institutionelle Bildungs Dimension. Aufgrund des immer stärker werdenden digitalen Wandels muss innerhalb der Bildung immer mehr IT-Wissen vermittelt werden. Dabei müssen die Bildungsinstitutionen darauf achten, den Schülern und Studenten die Gefahren mit an die Hand zu geben und wie sie mit diesen Umgehen. Bildungsinstitutionen spielen eine große Rolle, wenn es, um die Vermittlung von Wissen im IT-Bereich geht. Denn sie schaffen die Grundbausteine für die jungen Leute, welche sich im Laufe ihres Lebens weiter in eine der anderen Dimensionen bewegen werden. [51, Siponen, 2001]

In dieser Arbeit wird der Fokus insbesondere auf die organisatorische Dimension und die institutionelle Bildungsdimension gelegt. Hochschulen können aus zwei verschiedenen Perspektiven betrachtet werden: Aus der organisatorischen bzw. unternehmerischen Sicht, die Mitarbeiter wie Professoren und die Studenten als Nutzer der Organisation umfasst. Darüber hinaus können Hochschulen auch aus der institutionellen Bildungsperspektive betrachtet werden, die die Verantwortung trägt, den Lernenden Wissen zum Thema Informationssicherheit zu vermitteln und sie für deren Zukunft zu rüsten.

Das allgemeine Ziel der Cyber-Security-Awarness über alle Dimensionen hinweg ist es ein hohen Grad der Sensibilisierung bei den einzelnen Nutzern im Bereich der Informationssicherheit zu schaffen. Dafür müssen die Nutzer sowohl die Praktiken im Bereich der Informationssicherheit kennen und verstehen, aber vor allem müssen sie erst das nötige Grundwissen im Bereich der Informatik bzw. der digitalen Welt erwerben. Dieses Wissen bezieht sich auf die fundamentalen Technologie basierten Applikationen, welche im täglichen Gebrauch genutzt werden. Wie zum Beispiel Computer, das Internet oder auch E-Mail-Systeme. Ein höheres Maß an Informatikwissen trägt positiv zur Sensibilisierung im Bereich der Informationssicherheit bei. Dies ist wichtig zu wissen, denn bei der Entwicklung eines Cyber-Security-Awareness-Konzeptes muss davon ausgegangen werden, dass die verschiedenden teilnehmenden Personen unterschiedliche IT-Kentnisse haben und somit unterschiedliche Themen in den Schulungen benötigen. [2, Alahmari, 2021]

Es liegen eindeutige Belege vor, dass die Schulung im Bereich der Informationssicherheit die kosteneffektivste Methode zur Absicherung einer Organisation darstellt. In zahlreichen Experimenten wurde der Erfolg von Schulungen anhand der Reduktion der Anfälligkeit für Phishing-Angriffe gemessen. Die Ergebnisse zeigen, dass die Schulungen erfolgreich waren, da die Zahl der Personen, die auf Phishing-Betrug hereinfielen, signifikant zurückging. Worauf genau bei der Konzipierung eines Cyber-Security-Awareness-Konzeptes geachtet werden sollte, wird in den kommenden Kapiteln näher betrachtet. [2, Alahmari, 2021]

2.3 Aufbau und Implementierung eines Cyber-Security-Awareness-Konzeptes

Ein Cyber-Security-Awareness-Konzept zeigt auf wie innerhalb einer Organisation das Bewusstsein für Informationssicherheit gestärkt werden soll. Es beschreibt, welche Schritte unternommen werden sollten und wie diese umgesetzt werden können. Die jeweiligen Schritte, welche innerhalb eines Cyber-Security-Awareness-Konzeptes unternommen werden, werden Maßnahmen gennant.

Ein Cyber-Security-Awareness-Konzept setzt sich unter anderem aus folgenden Punkten zusammen:

- Den Methoden, welche den Nutzern die Inhalte präsentieren.

- Die psychologischen Einflussfaktoren, welche beachtet werden müssen, um die Nutzer zu verstehen und somit besser auf sie eingegangen werden kann.
- Den Messmethoden, welche dazu dienen das Bewusstsein für Informationssicherheit der Nutzer zu messen um somit die eigenen Maßnahmen gegebenenfalls anzupassen.
- Den Programmen, welche unter anderem für die Cyber-Security-Awareness-Schulungen genutzt werden.

Die Methoden sind die Grundbasis eines jeden Cyber-Security-Awareness-Konzeptes. Sie beschreiben die Techniken zur Schaffung oder Entwicklung ansprechneder Materialien zur Verbesserung der Cyber-Security-Awareness innerhalb einer Organisation [24, Khando et al., 2021].
Die psychologischen Einflussfaktoren helfen dabei die Nutzer zu verstehen und die passenden Methoden zu entwickeln und auf deren Bedürfnisse anzupassen. Ebenfalls helfen sie dabei, der Organisation eine Umgebung zu schaffen, die es den Nutzern erleichtert, sich mit dem Cyber-Security-Awareness-Konzept auseinanderzusetzen und die jeweiligen Richtlinien zu befolgen. [36, Leach, 2003]
Um zu Messen wie effektiv die erstellten Methoden sind, werden Messmethoden benötigt. Diese helfen dabei die Cyber-Security-Awareness der Nutzer zu messen und zu schauen wie gut das jeweilige Cyber-Security-Awareness-Konzept der Organisation von den Nutzern angenommen wird. So kann auch mithilfe der Messmethoden geschaut werden, ob evtl. Anpassungen des Cyber-Security-Awareness-Konzeptes nötig sind. Solche Messungen sind unabdingbar um ein Cyber-Security-Awareness-Konzept stetig zu verbessern.
Sowohl einige der Methoden als auch einige der Messmethoden sind nicht durchführbar ohne entsprechende Programme bzw. Tools. Es werden Tools benötigt, um zum Beispiel E-Learning-Methoden zu gestalten oder auch Phishing-Simulationen durchzuführen. Deshalb sollte auch die Entscheidung welche Tools wie zum Einsatz kommen, in einem Cyber-Security-Awareness-Konzept besprochen werden.
Alle zuvor genannten Aspekte werden in den nächsten Kapiteln dieser Bachelorarbeit behandelt, mit besonderem Fokus auf ihre Anwendung im Hochschulbereich.

Cyber-Security-Awareness wird meist in sogenannten Kampagnen durchgeführt. Dabei konzentriert sich eine Kampagne auf einen bestimmten Themenbereich der Informationssicherheit. Somit müssen mehrere Kampagnen durchgeführt werden, um die Nutzer für ein breites Spektrum der Informationssicherheit zu sensibilisieren. Außerdem ist das erlangte Bewusstsein von Informationssicherheit der Nutzer ein temporärer Zustand, wel-

cher in regelmäßigen Abständen erneruert werden muss. Somit sollten diese Kampagnen auch regelmäßig durchgeführt werden. [1, Abawajy, 2012] [6, Bauer et al. 2017]

Das regelmäßige Durchführen der Kampagnen hilft auch dabei, Feedback von den Nutzern zu sammeln und iterativ das Cyber-Security-Awareness-Konzept zu verbessern. Dabei kann die Organisation, wie auch bei der Entwicklung des ISMS, nach dem PDCA-Zyklus agieren. Die jeweiligen Kampagnen können mithilfe des PDCA-Zyklus betrachtet und verbessert werden. Somit dienen die Kampagnen als eine Iteration durch den PDCA-Zyklus. Es sollte sich also nach einer Kampagne der Erfolg der durchgeführten Maßnahmen angeschaut und bewertet werden, um diese Kentnisse bei der Planung für die nächste Kampagne zu berücksichtigen. Der Erfolg einer Kampagne kann durch verschiedene Techniken gemessen werden. Die meistgenutzte Technik ist die Durchführung einer Phishing-Simulation. Es können aber auch andere Techniken genutzt werden, wie zum Beispiel Umfragen / Quizze, welche die Nutzer beantworten müssen, oder auch das Überwachen der gemeldeten Informationssicherheitsvorfälle, um zu schauen, ob sich diese erhöht haben bzw. ob sich die erfolgreichen Informationssicherheitsvorfälle verringert haben. Bei all diesen Methoden geht es darum, herauszufinden ob die Nutzer aufmerksam bei den Cyber-Security-Awareness-Schulungen teilgenommen und die dort vermittelten Praktiken aufgenommen haben und diese im Alltag einsetzen. [48, Scholl et al., 2017] [59, Sykosch, 2022]
Nachdem die Kampagnen bewertet wurden sind, können entsprechende Maßnahmen zur Verbesserung eingeleitet werden, um die nächste Kampagne so zu gestalten, dass diese einen höheren Erfolg erzielt. Einige Maßnahmen wären die Vermittlung unterschiedlicher Belohnungen für die Nutzer oder die ansprechendere Gestlatung des Material. Der PDCA-Zyklus kann dann bei jeder Kampagne wiederholt werden, um ein optimales Ergebnis des Cyber-Security-Awarenes-Konzeptes zu erreichen.

Um ein ganzheitliches Cyber-Security-Awareness-Konzept zu konzipieren, müssen unter anderem zwei Aspekte besonders hervorgehoben werden. Der erste Aspekt sind die eingesetzten Methoden. Sie bestimmen wie die Inhalte des Konzeptes präsentiert werden. Gemäß Khando et al. bezeichnen Methoden im Kontext der Cyber-Security-Awareness jene Techniken, die darauf abzielen, ansprechende und angemessene Materialien zu entwickeln, um das Niveau der Informationssicherheit bei den Nutzern zu verbessern [24, Khando et al., 2021]. Dabei ist die Auswahl der Methoden ein wichtiger Faktor für ein erfolgreiches Cyber-Security-Awareness-Konzept. Folgende Methoden werden innerhalb dieser Arbeit untersucht:

- Traditionelles Lernen (Präsentationen)
- Interaktives Lernen (Workshops / Dialoge)
- Passives Lernen (E-Mail-Erinnerungen / Flyer / Plakate)
- Asynchrones Lernen (E-Learning)
- Spielerisches Lernen (Lernspiele)

Der zweite Themenbereich, welcher mit ausschlaggebend für ein erfolgreiches Cyber-Security-Awareness-Konzept ist, sind die sogenannten Faktoren. Die Faktoren beziehen sich auf die psychologischen Verhaltensweisen der Nutzer und liefern Aufschluss darüber, wie diese das Thema Cyber-Security wahrnehmen und darüber denken. Dabei teilen sich die Faktoren in zwei Hauptgruppen auf. Die erste Gruppe der Faktoren bezieht sich auf das Verständnis des Nutzers dafür, welches Verhalten von ihm erwartet wird. Die zweite Gruppe der Faktoren thematisiert die Bereitschaft des Nutzers ein, sein Verhalten einzuschränken, um die akzeptierten Normen einzuhalten. [36, Leach, 2003]

Es ist wichtig diese beiden Themenbereiche zu kennen und zu verstehen, um das Cyber-Security-Awareness-Konzept erfolgreich zu gestalten. Denn zum einen wird das Wissen über die jeweiligen Methoden benötigt, um ansprechendes Material für die Cyber-Security-Awanress-Schulungen zu gestalten und zum anderen ist das Verständnis der Faktoren wichtig, um die Motivation der Nutzer aufrechtzuerhalten. [1, Abawajy, 2012][24, Khando et al., 2021] [36, Leach, 2003]

Um die bereits gennanten Aspekte umzusetzen, werden Programme benötigt, um diese digital zu implementieren und den manuellen Aufwand gering zu halten. Die Programme können dabei helfen, die Schulungen für die Nutzer zu gestalten und diese durchzuführen, aber auch, um das Bewusstsein für Informationssicherheit der Nutzer zu messen, indem zum Beispiel digitale Tests oder Phishing-Simulationen durchgeführt werden. So können einige hier vorgestellte Methoden (z.B. E-Learning) oder auch Messmethoden (z.B. Phishing-Simulationen) nicht ohne geeignete Programme implementiert und druchgeführt werden.

2.4 Menschen als Zielobjekte von Cyber-Angriffen

Zahlreiche Sicherheitsrisiken, darunter Viren, Denial-of-Service-Angriffe, gestohlene Passwörter und Verletzungen von Autorität sowie Autorisierungen, resultieren häufig aus einem mangelnden Sicherheitsbewusstsein. Ein mangelndes Sicherheitsbewusstsein führt oft zu Fehlverhalten der Nutzer, welches wiederrum einfach von Cyber-Angriffen ausgenutzt werden kann. ENISA (2019) ermittelte, dass etwa 77 % der Datenschutzverletzungen in Unternehmen auf die Ausnutzung menschlicher Schwächen zurückzuführen sind [13, ENISA, 2019]. Es wurde auch festgestellt dass mehr als die Hälfte aller Verstöße gegen die Informationssicherheit der Informationssicherheitsverletzungen auf die mangelnde Einhaltung der Vorschriften durch die Mitarbeiter zurückzuführen sind. [24, Khando et al., 2021] [10, Chen et al., 2006]

Unter den vielen möglichen Cyber-Angriffen die auf das menschliche Fehlverhalten abzielen gehört Social-Engineering zu den Hauptbedrohungen im Cyber-Bereich [14, ENISA, 2023] [23, Jimoh, 2022]. Insbesondere wird die Taktik der Phishing-Angriffe innerhalb des Social-Engineerings häufig von Cyberkriminellen genutzt. Dies wird durch Daten der APWG (Anti-Phishing Working Group) bestätigt, die einen Anstieg der Phishing-Vorfälle in den letzten zehn Jahren um nahezu das Zehnfache verzeichnet. [4, APWG, 2023]

Angesichts seiner hohen Relevanz wird der Social-Engineering-Angriff hier erörtert und dient als Beispiel für eine Art von Cyber-Angriff, die gezielt menschliches Fehlverhalten ausnutzt. Es ist von entscheidender Bedeutung, dass ein Cyber-Security-Awareness-Konzept den Nutzern unter anderem vermittelt, wie sie derartige Angriffe erkennen und melden können.

Social-Engineering kann definiert werden als die Täuschung einer Person, sei es von Angesicht zu Angesicht, per Telefon oder mithilfe eines Computersystems (Phishing-Emails), mit dem Ziel, ein bestimmtes Sicherheitsniveau zu durchbrechen. [23, Jimoh, 2022]

So ruft beispielsweise ein Hacker beim Kundendienst an, um sich als echter Kunde auszugeben, und verwendet verschiedene Social-Engineering-Techniken, um an die privaten Daten eines Kunden des Opfers zu gelangen. Zu den möglichen Techniken des Social-Engineering zählt unter anderem die gezielte Recherche von Informationen, die es dem Angreifer ermöglicht, dem Nutzer glaubhaft zu vermitteln, er sei eine andere Person. Auch das Ausüben von Druck auf den Nutzer ist eine häufig verwendete Technik. Dies sorgt dafür, dass der Nutzer nicht die Identität des Angreifers hinterfragt oder die Anfrage eingehender prüft. Eine weitere häufig verwendete Technik ist es den Nutzer Aufregung

oder Freude spüren zu lassen. Durch falsche Behauptungen wie ”Sie haben eine Million Euro gewonnen, bitte verraten Sie mir nur noch Ihre Bankdaten....”, sorgen die Angreifer für Aufregung und Freude bei den Nutzern, welches dazu führen kann, dass der Nutzer vor Aufregung den Aufforderungen des Angreifers folge leistet. Diese Techniken dienen hier nur als Beispiel, es gibt noch viele andere Techniken und Herangehensweisen von Hackern, welche oft auf die jeweilige Situation angepasst ist. Diese Techniken können durch gezielte Sensibilisierung und einfache Maßnahmen unterbrochen werden. Ist der Nutzer angemessen geschult, kann er gelassen und kritisch auf eine verdächtige Anfrage reagieren und diese sorgfältig prüfen, um die Authentizität zu verifizieren. Deshalb ist Social-Engineering als Angriff ein gutes Beispiel, um den Nutzen und die Wichtigkeit von Cyber-Security-Awareness aufzuzeigen. [50, Shetty, 2017]

Zwar sind Social-Engineering Angriffe oft auf die jeweilige Situation angepast, jedoch lässt sich ein ungefährer Ablauf (Abbildung: 2.1) zeichnen:

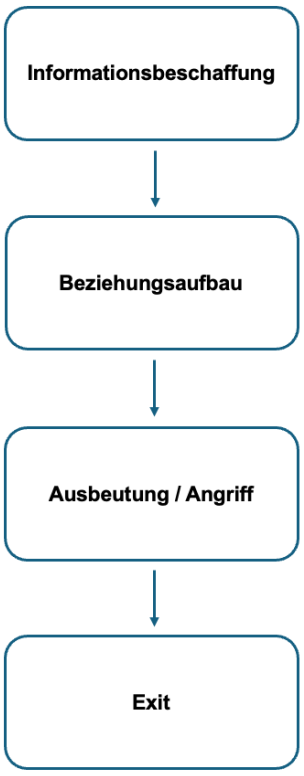

Abbildung 2.1: Social-Engineering-Schema
Quelle: Eigene Darstellung in Anlehnung an [23, Jimoh, 2022]

Die erste Phase ist eine Vorangriffsphase, die in der Regel Methoden der Informationsbeschaffung erfordert. Der Angreifer findet eine für ihn optimale Person oder Organisation als Opfer, um den Angriff zu starten. In der zweiten Phase baut der Angreifer eine positive Beziehung zum Opfer auf. Der Angreifer sorgt dafür, dass das Opfer sein Vertrauen gewinnt, indem er das Opfer per E-Mail oder Telefon kontaktiert. Ziel ist es, eine gute Beziehung zum Opfer aufzubauen. Die dritte Phase ist die direkte Aktion, in der der Täter das Opfer ausnutzt, indem er das Vertrauen des Opfers manipuliert. In dieser Phase werden fast alle privaten Informationen des Opfers extrahiert und der Angriff ausgeführt. Schließlich versucht der Angreifer, seine Spuren zu verwischen. Er stellt sicher, dass er keine Beweise für seinen Besuch hinterlässt, die eine Rückverfolgung zu seiner wahren Identität ermöglichen oder ihn mit dem unbefugten Eindringen in das Zielsystem in Verbindung bringen könnten. in Verbindung bringen könnten.

Ein tiefgehendes Verständnis dieser Angriffsarten ist entscheidend, um den Wert eines Cyber-Security-Awareness-Konzeptes vollständig zu erfassen. [23, Jimoh, 2022] [50, Shetty, 2017]

3 Methoden und psychologische Einflussfaktoren im Bereich der Cyber-Security-Awareness

Khando et al., 2021, argumentiert, dass es zwei wichtige Aspekte gibt, welche ein erfolgreiches Cyber-Security-Awareness-Konzept ausmachen. Zum einen sind es die eingesetzten Methoden, welche die Inhalte präsentieren und den Nutzern das Wissen im Informationssicherheits Bereich vermitteln. Sie beschreiben die Techniken zur Schaffung oder Entwicklung ansprechender Materialien zur Verbesserung des Bewusstseins für Informationssicherheit der Nutzer. Und zum anderen sind es die psychologischen Einflussfaktoren welche Aufschluss über die denkweisen der Nutzer zum Thema Informationssicherheit geben. Die Methoden und Faktoren sind eng miteinander verbunden. Beide Aspekte müssen in die Entwicklung des Cyber-Security-Awareness-Konzeptes mit einbezogen werden, um das Bewusstsein für Informationssicherheit zu erhöhen. [24, Khando et al., 2021]

3.1 Cyber-Security-Awareness-Methoden

Zur Vermittlung des Bewusstseins für Cyber-Security gibt es zahlreiche Methoden, die von der Verteilung von Nachrichten (z. B. Poster) bis hin zu formellen Präsentationen reichen, um die Cyber-Security-Awareness der Benutzer zu verbessern. Neben dem vermittelten Inhalt ist auch die Art und Weise der Vermittlung von hoher Bedeutung für den Erfolg eines Cyber-Security-Awareness-Konzepts. Aus diesem Grund werden in diesem Abschnitt die gängisten und bewährten Cyber-Security-Awareness-Methoden vorgestellt und anschließend untersucht. Dabei wird ebenfalls auf die Hochschuleignung der jeweiligen Methoden eingegangen. [1, Abawajy, 2012]

Laut dem BSI (Bundesamt für Sicherheit in der Informationstechnik) sind Cyber-Security-Awareness-Maßnahmen dann erfolgreich, wenn sie die Zielgruppen befähigen und den

einzelnen Menschen für mehr Cyber-Security motivieren [22, BSI]. Mit Cyber-Security-Awareness-Maßnahmen sind die Schritte gemeint, die innerhalb eines Cyber-Security-Awareness-Konzeptes unternommen werden, um die Nutzer zu sensibilisieren, welche auch über die Cyber-Security-Awareness-Methoden hinaus gehen. Darunter könnten die Cyber-Security-Awareness-Methoden gehören, wie zum Beispiel Präsentationen oder auch die Messmethoden wie zum Beispiel Phishing-Simulationen. Cyber-Security-Awareness-Methoden hingegen beziehen sich auf die spezifischen Ansätze, die verwendet werden, um die Inhalte zu präsentieren und das Wissen an die Nutzer zu vermitteln [1, Abawajy, 2012] [24, Khando et al., 2021].

Das Ziel besteht nicht darin, den Nutzern umfassendes Fachwissen im Bereich Cyber-Security zu vermitteln, sondern vielmehr deren Bewusstsein für das Thema zu schärfen und sie über die damit verbundenen Gefahren, Risiken sowie mögliche Präventionsmaßnahmen aufzuklären. Darunter gehört auch, wie die Nutzer Informationssicherheitsvorfälle erkennen und diese melden.

Für einige Cyber-Security-Awareness-Methoden (z.B. E-Learning) werden entsprechende Tools benötigt, um diese umsetzen zu können. Die möglichen Tools für diesen Zweck werden in Kapitel fünf (5) behandelt.

Folgende Methoden werden innerhalb dieser Arbeit untersucht:

Traditionelles Lernen (Präsentationen)

Beim traditionellen Lernen im Cyber-Security-Awareness Kontext werden Präsentationen nach den allgemeinen Unterrichtsformalien gehalten. Dabei richtet sich der Inhalt an ein ausgewähltes Publikum. Es wird ein bestimmtes Thema im Bereich Cyber-Security von einem Experten vorgestellt. Dies kann sowohl in Präsenz als auch Online stattfinden. Hier wird eine größere Zielgruppe adressiert. Im Nachgang können Fragen an den jeweiligen Experten gestellt werden.

Interaktives Lernen (Workshops & Dialoge)

Interaktives Lernen (Workshops und Dialoge) wird in einer kleineren Gruppe durchgeführt, wobei es in diesem Rahmen möglich ist, Diskussionen zu führen oder Erfahrungen im Bereich der Informationssicherheit auszutauschen. Sie werden von einem Moderator geleitet und gemeinsam können verschiedene Aufgaben bearbeitet werden, um das Verständnis und Wissen zu vertiefen. Diese Methode zielt auf eine eher kleinere Anzahl an Teilnehmern ab, um die Interaktion groß zu halten. [24, Khando et al., 2021]

Passives Lernen (E-Mail-Erinnerungen / Flyer / Plakate)

Beim Passiven Lernen geht es darum den Nutzern durch bestimmte Erinnerungen auf das Thema Cyber-Security aufmerksam zu machen. Dies kann zum Beispiel durch Plakate entstehen, welche eine Kurzanleitung haben, wie Phishing-E-Mails erkannt werden können oder auch durch Bildschirmschoner oder Bildschirmhintergründe auf den Computern der Organisation, welche bestimmte Hinweise zum Thema geben. Diese Methode zeichnet sich durch ihre Beliebtheit aus, begründet in der Einfachheit ihrer Anwendung und den kostengünstigen Implementierungsmöglichkeiten. Die Tatsache, dass der Nutzer nicht aktiv an einer Schulung teilnehmen oder Aufgaben bearbeiten muss, kennzeichnet diese Methoden als passives Lernen. [2, Alahmari, 2021] [9, Chaudhary et al., 2022]

Asynchrones Lernen (E-Learning)

Im Bereich des E-Learning gibt es viele Programme und Plattformen welche den Nutzern zum Thema Cyber-Security verschiedene Inhalte verschiedener Formen näherbringen. In der Regel stehen Lernmaterialien wie Textdokumente, Videomaterialien oder kurze Tests zur Verfügung, die beispielsweise das Erkennen von Phishing-E-Mails thematisieren. Hierbei erfolgt das Lernen asynchron, sodass die Nutzer Ort und Zeitpunkt des Lernprozesses eigenständig festlegen können. [49, Schütz et al., 2019]

Spielerisches Lernen (Lernspiele)

Unter Lernspielen wird verstanden, dass die Inhalte des Cyber-Security-Awareness-Konzeptes so dargestellt werden, dass diese das Erlebnis und die Motivation von Spielen repliziert. Dies wird auch "Gamification" genannt. Hier gibt es verschiedene Programme und Plattformen die zum Beispiel das Erkennen von Phishing-E-Mails interaktiv in einem Spiel gestalten. Meist wird dies zusammen mit der Methode des E-Learnings kombiniert oder auch innerhalb des E-Learnings integriert. [24, Kahndo et al., 2021] [2, Alahmari, 2021]

Die zuvor vorgestellten Awareness Methoden werden in dieser Arbeit mit Hinblick auf den Einsatz im Hochschulbereich Untersucht. Dabei wird darauf eingegangen wie die jeweiligen Methoden von den Nutzern angenommen werden und wie praktikabel diese im Hochschulbereich sind. Es wird auch darauf geschaut, mit welchen Methoden die Personen am effektivsten Lernen können, sodass die Inhalte effektiv aufgenommen und umgesetzt werden. In diesem Zusammenhang stützt sich die Untersuchung auf die in der referenzierten Literatur vorhandenen Erkenntnisse. Eine eigenständige Studie oder eine Befragung zur Effektivität wurde nicht vorgenommen. Des Weiteren wird auf die verschiedenen Personengruppen im Hochschulbereich eingegangen, welche unterschiedliche Kenntnisse im Bereich der Informationssicherheit aufweisen und eine unterschiedliche Organisation der Methoden benötigen. Die Betrachtung der unterschiedlichen Gruppen innerhalb der Hochschulorganisation ist notwendig, um eine optimale Verteilung der jeweiligen Methoden und Trainingsinhalte innerhalb einer Cyber-Security-Awareness-Schulung zu gewährleisten.

3.1.1 Traditionelles Lernen (Präsentationen)

Traditionelles Lernen wie Präsentationen bzw. von einem Dozenten geführter Unterricht wird noch häufig im Bereich der Cyber-Security-Awareness eingesetzt. Dabei richtet sich der Unterricht meist an eine größere Zielgruppe und wird statisch durchgeführt. Hier präsentiert ein Dozent Inhalte zu einem bestimmten Thema, woraufhin die Teilnehmenden die Möglichkeit haben, anschließend Fragen zu stellen.

Ein Vorteil dieser Methode ist, dass die Teilnehmenden direkt Fragen stellen können oder auch Feedback an den Dozenten geben können. Dies bietet dem Dozenten die Möglichkeit seinen Unterricht anzupassen und direkt auf die Fragen einzugehen.
Jedoch finden viele Nutzer diese Lern Methode eher langweilig und ineffektiv [1, Abawajy, 2012].

Der wichtigste Aspekt bei dieser Methode ist der Dozent. Der Erfolg dieser Methode hängt von den Fähigkeiten des Dozenten ab, ob dieser in der Lage ist, das Publikum zum vorgestelltem Thema zu begeistern. Insbesondere bei traditionellen Methoden gestaltet es sich als Herausforderung, die Aufmerksamkeit der Nutzer über einen längeren Zeitraum hinweg aufrechtzuerhalten.

Häufig scheitert diese Methode daran, dass von den Nutzern erwartet wird, Inhalte auswendig zu lernen, anstatt sie dazu anzuregen, über die verschiedenen Aspekte der Informationssicherheit nachzudenken sowie diese praktisch anzuwenden oder zu trainieren. [1, Abawajy, 2012]

Hochschuleignung:
Der Einsatz dieser Methode im Hochschulbereich ist durchaus möglich, jedoch mit erhöhtem Aufwand verbunden. Da durch die Studenten in einer Hochschule größere Zielgruppen existieren, wäre es möglich diese mithilfe der traditionellen Lernmethode zu schulen. Hierfür wäre etwas organisatorischer Aufwand nötig. Es würde ein Dozent benötigt werden und sollte der Unterricht in Präsenz stattfinden auch ein geeigneter Raum. Beides wäre kein allzu großer Aufwand für eine Hochschule, da diese mit diesem Lernkonzept bereits geeignete Erfahrungen haben, durch die eigenen Vorlesungen, welche jede Hochschule anbietet. Dabei wäre es möglich so einen Unterricht für Studierende in den Vorlesungsplan mit einzuarbeiten.
Für Mitarbeiter und Lehrkräfte einer Hochschule müsste wiederrum eine seperate Lösung gefunden werden. Mitarbeiter haben feste Arbeitszeiten, diese müssen bei der Planung der Veranstaltungen berücksichtigt werden. Außerdem können auch nicht alle Mitarbeiter gleichzeitig geschult werden, aufgrund des dadurch verusachten Arbeitsausfall. Bei den Lehrkräften, wie den Professoren, sieht es ähnlich aus.
Des Weiteren müsste darauf geschaut werden, wie die jeweiligen Themen und die Komplexität der Veranstaltungen verteilt werden. Hier weisen zum Beispiel Professoren aus dem IT-Bereich mehr Wissen in der Informationssicherheit auf als Studierende aus dem Studiengang Soziale Arbeit. Daher benötigt diese Methode eine gewisse Koordination und Organisation, welches den Aufwand wiederrum erhöht.

Die Effizienz dieser Methode erweist sich jedoch als unzureichend, um eine konkrete Empfehlung auszusprechen. Solch eine Schulung wäre durch die große Anzahl an Teilnehmenden sehr allgemein gehalten, dabei würde die Reduzierung der Teilnehmenden den Organisatorischen Aufwand erhöhen. Ein individueller Unterricht ist hier nicht möglich, welcher jedoch die Effektivität deutlich steigern würde. Zudem besteht das Risiko, dass der Dozent nicht in der Lage ist, die Teilnehmenden ausreichend abzuholen, sodass sich die Teilnehmenden schnell langweilen und sich nicht aufmerksam mit dem Thema beschäftigen werden.

Eine Möglichkeit wäre, dass diese Methode in Form von einzelnen Veranstaltungen angeboten wird, für interessierte Personen. Dies müsste dann mit einer weiteren verpflich-

tenden Methode kombiniert werden, um alle Nutzer aus der Hochschul Organisation zu erreichen.

Die Vor- und Nachteile dieser Methode werden nochmal in Tabelle 3.1 zusammenfassend aufgeführt.

Vorteile (Allgemein)	**Nachteile (Allgemein)**
Direkter Kontakt zum Dozenten.	Erfolg stark abhängig vom Dozenten.
Durch eine große Zielgruppe können viele Nutzer aufeinmal erreicht werden.	Geringer Lerneffekt aufgrund mangelnder interaktivität und hohes auswendig lernen der Nutzer.
	Allgemeingehaltener Inhalt, nicht individuell.
Vorteile (Hochschulbezogen)	**Nachteile (Hochschulbezogen)**
Hochschulen haben bereits Erfahrung mit dem Konzept der Vorlesung (Infrastruktur vorhanden).	Hoher Organisationsaufwand (Terminplanung).
	Themen und Komplexität des Inhaltes korrekt an die richtigen Nutzer zu verteilen sorgt für erhöhten Organisatorischen Aufwand.

Tabelle 3.1: Vor- & Nachteile: Traditionelles Lernen

3.1.2 Interaktives Lernen (Workshops & Dialoge)

Khando, 2021, betont die Bedeutung der aktiven Teilnahme von Nutzern an Cyber-Security-Awareness-Schulungen. Forschungsergebnisse zeigen, dass Workshops und Dialoge eine positive Auswirkung auf das Verhalten der Teilnehmenden im Hinblick auf die Informationssicherheit haben. Durch die aktive Teilnahme der Nutzer fühlen sich diese mitverantwortlich für das Thema, was wiederrum eine positive Auswirkung auf deren Bewusstsein und Verhalten im Bereich der Informationssicherheit haben kann. Vor allem im öffentlichen Sektor wird diese Methode gerne genutzt, bei der die Nutzer ihre Erfahrungen und ihr Wissen miteinander teilen können. [24, Khando et al., 2021]

Es ist wichtig, dass bei dieser Methode passende Themen für die jeweiligen Zielgruppen besprochen werden. Zum Beispiel ist für eine Gruppe voller IT-Administratoren das Thema Umgang mit Kritischen Systemen spannender als für Servicemitarbeiter der Mensa. Deshalb sollte der Inhalt und die besprochenen Themen vorher sorgfältig ausgewählt werden.

Jedoch fordert diese Methode einige organisatorische Hürden. Solche Workshops und Dialoge benötigen einen geeigneten Raum, wenn diese in Präsenz geführt werden. Zusätzlich wird ein Informationssicherheit Experte benötigt, welcher als Moderator fungiert. Doch wie bereits bei der Traditionellen Methode erwähnt, wäre dies keine allzu große Hürde für eine Hochschule, da dies meist bereits vorhanden ist oder beschafft werden kann. Zudem sollten solche Workshops und Dialoge im Gegensatz zur traditionellen Methode in kleineren Gruppen geführt werden, um eine hohe Beteiligung der Teilnehmenden zu ermöglichen. Denn bei einer hohen Anzahl an Teilnehmenden, ist es möglich, dass nicht jeder zu Wort kommt, aus beispielsweise zeitlichen Gründen. Es kann auch sein, dass sich Personen in großen Gruppen nicht wohl fühlen und sich dann zurückziehen, welches wiederrum dazu führen würde, dass sich die Nutzer unwohl fühlen würden. Kleine Gruppen implizieren auch mehrere Veranstaltungstermine, um alle Personen der Organisation zu erreichen.

Hochschuleignung:
Im Hochschulkontext existieren diverse Personengruppen von unterschiedlicher Größe. Daher wäre es erforderlich mehrere Workshops und Dialoge zu organisieren, um alle Zielgruppen angemessen zu erreichen. Außerdem sollten auch die verschiedenen Wissensstände im Bereich der Informationssicherheit der unterschiedlichen Personengruppen beachtet werden. Innerhalb eines Workshops sollten im Optimalfall Personen sein, welche einen ungefähr gleichen Wissensstand in der Informationssicherheit aufweisesen können, damit die jeweiligen Personen nicht über- oder unterfordert sind. Im Hochschulbereich existieren drei Hauptgruppen, Professoren und Lehrende, Mitarbeiter der Hochschule (z.b. Servicekräfte der Mensa) und die Studierende. Wobei sich die Gruppen der Studierende und Professoren und Lehrenden noch weiter aufteilen in die jeweiligen Fachrichtungen. Aus diesem Grund benötigt werden im Hochschulbereich viele solcher Termine für die Workshops und Dialoge benötigt, um alle Personen zu erreichen. Ein weiterer Aspekt, welcher zu beachten ist, ist das Zeitmanagement. Bei einer hohen Anzahl an Personen, wird es oft Personen geben, welche zu bestimmten Terminen nicht erscheinen können. Dies erschwert es diese Methode in dieser Größe innerhalb einer Hochschule zu implementieren.

Ähnlich, wie bei der traditionellen Lernmethode wäre der Vorschlag, diese Methode im kleineren Kreis anzugehen. Zum Beispiel könnten Termine zum Thema Informationssicherheit auf freiwilliger Basis innerhalb der Hochschule angeboten werden und dies dann zielgerichtet an die jeweiligen Personengruppen. Dies würde den organisatorischen Aufwand deutlich verringern und zusätzlich eine Möglichkeit bieten ein Bewusstsein für

Informationssicherheit zu schaffen. Diese freiwilligen Termine müssten ebenfalls mit einer verpflichtenden Methode kombiniert werden, um das Bewusstsein für Informationssicherheit hochschulweit zu implementieren.

Die Vor- und Nachteile dieser Methode werden nochmal in Tabelle 3.2 zusammenfassend aufgeführt.

Vorteile (Allgemein)	**Nachteile (Allgemein)**
Hohe Interaktion fördert den Lernerfolg.	Durch eine kleine Zielgruppe können nur wenige Nutzer aufeinmal erreicht werden.
Durch kleine Gruppen ist der Inhalt individueller an die Nutzer gerichtet.	Viele Termine / Veranstaltungen nötig, was wiederum den Organisatorischen aufwand erhöht.
Vorteile (Hochschulbezogen)	**Nachteile (Hochschulbezogen)**
Infrasturktur für Umsetzung vorhanden (Räumlichkeiten vorhanden & Dozenten welche die Kurse leiten könnten sind meist ebenfalls vorhanden).	Hoher Organisationsaufwand (Terminplanung / Zeitmanagement).
	Themen und Komplexität des Inhaltes korrekt an die richtigen Nutzer zu verteilen sorgt für erhöhten Organisatorischen Aufwand.

Tabelle 3.2: Vor- & Nachteile: Interaktives Lernen

3.1.3 Passives Lernen (E-Mail-Erinnerungen / Broschüren / Plakate)

Bei der passiven Lernmethode geht es darum durch bestimmte Erinnerungen, die Nutzer auf das Thema Informationssicherheit aufmerksam zu machen. Dabei werden verschiedene Medienformate und Kommunikationskanäle genutzt, um die jeweiligen Zielgruppen zu erreichen und über Cyber-Security zu informieren. Es können Plakate, E-Mails, Infografiken, Comics, Broschüren, und Flugblätter genutzt werden, die spezifische Informationen zu Cyber-Security vermitteln. Da der Nutzer nicht aktiv mitarbeiten muss, handelt es sich hierbei, um eine passive Lernmethode. Als Beispiel ließe sich eine kompakte Broschüre erstellen, die als Kurzanleitung dient und erläutert, wie eine Phishing-E-Mail identifiziert werden kann, oder auch ein Plakat entwerfen kann, welches die wichtigkeit von sicheren Passwörtern aufzeigt.
Durch die Integration digitaler Technologien lässt sich der Informationsgehalt von Plakaten signifikant aufwerten. Beispielsweise können Plakate durch die Einbindung eines

QR-Codes ergänzt werden, der Interessierte direkt zu einer Webseite mit umfassenden Informationen zum Thema oder einem Feedback-Formular führt. Zudem ermöglicht die Verbreitung solcher Plakate über Massenkommunikationsmittel wie E-Mail, soziale Medien und Websites oder auch das einfache Aufhängen der Plakate eine effiziente Verteilung der Botschaft an ein breites Publikum. [1, Abawjy, 2012] [9, Chaudhary et al., 2022]

Es ist jedoch wirksam, diese Medienformate ansprechend zu gestalten. Chaudhary et al., 2022, hat sechs Eigenschaften herausgearbeitet, welche Plakate etc. beinhalten sollten, um als effektive Informationsvermittler für die Sensibilisierung im Informationssicherheits Bereich zu dienen. [9, Chaudhary et al., 2022]

- **Thema:** Es sollte sich auf ein für die Zielgruppe relevantes Thema fokussieren.
- **Qualität der Information:** Die jeweiligen Informationen sollten konsistent und aktuell sein.
- **Botschaftsgestaltung:** Die Nachricht sollte direkt und explizit an die Zielgruppe gerichtet sein, dabei sollte sie auch positiv gestaltet sein (z.b. "Was muss man tun", statt "Was man nicht tun sollte")
- **Empfehlungen:** Die Empfehlungen sollten durch den Nutzer ohne Einschränkungen anwendbar sein.
- **Präsentation des Inhalts:** Der Inhalt sollte informatik strukutiert sein. Außerdem sollte der Inhalt präzise formuliert sein und auf den Punkt gebracht sein. Des Weiteren ist die Nutzung von verschiedenen Darstellungen wie Grafiken, Diagramme von Vorteil.
- **Formatierung:** Bei der Formatierung sollte darauf geachtet werden, dass die Hauptaussage schon von weiter distanz zu lesen ist, außerdem sollte die Hauptbotschaft so platziert sein, dass diese nicht untergeht. Zudem sollte Farbe, das Logo der Organisation, Bilder und die richtige Schriftart verwendet werden, um ein Plakat ansprechend zu gestalten.

Der letzte Punkt der sechs Eigenschaften bezieht sich explizit auf das Medienformat Plakat. Jedoch lassen sich die anderen Eigenschaften auch auf andere Medienformate wie zum Beispiel Broschüren anwenden.

Ein großer Vorteil dieser passiven Methode ist, dass es wenig Aufwand benötigt, diese Methode zu implementieren. Sie ist kostengünstig und schnell umgesetzt. Hierbei kann

auch auf die Materialien von verschiedenen Organisationen zurückgegriffen werden, wie zum Beispiel ENISA, EUROPOL, oder das SANS Institute. Somit würden nur noch die Ressourcen für den eventuellen Druck der jeweiligen Materialien benötigt. [9, Chaudhary et al., 2022]

Hochschuleignung:
Vor allem, um die Zielgruppe der Studierende zu erreichen, kann diese Methode gut im Hochschulbereich angewendet werden. Plakate können an strategisch ausgewählten Standorten innerhalb der Hochschule platziert werden, die einen hohen Personenverkehr aufweisen (zum Beispiel am Mensa Eingang). Außerdem ist die einfache und kostengünstige Umsetzung von großen Vorteil für Hochschulen. Hochschulen haben begrenzte personelle und finanzielle Mittel, diese Methode wäre gut, um mit einfachen Mitteln auf das Thema Cyber-Security aufmerksam zu machen. Jedoch kann auch ein nachteil sein, dass wenn zum Beispiel die Materialien nicht ansprechend gestaltet sind, diese von den Studenten und Mitarbeitern ignoriert werden.

Wichtig ist, dass einem bewusst ist, das mithilfe dieser Methode kein tiefes Wissen für die Informationssicherheit aufgebaut wird und, dass diese Methode auch kein ersatz für eine Cyber-Security-Awareness-Schulung ist. Doch durch den Einsatz dieser Methode lässt sich das Bewusstsein für das Thema Cyber-Security effektiv steigern, da die Nutzer regelmäßig durch Plakate etc. an das Thema erinnert werden.

Die Vor- und Nachteile dieser Methode werden nochmal in Tabelle 3.3 zusammenfassend aufgeführt.

Vorteile (Allgemein)	**Nachteile (Allgemein)**
Durch Massenkommunikation werden viele Nutzer erreicht.	Kein (individuelles) training der Nutzer, es wird lediglich auf das Thema aufmerksam gemacht.
Geringer Organisatorischer Aufwand.	Korrekte Gestaltung der Materialien kann schwierig sein.
Kostengünstig.	
Vorteile (Hochschulbezogen)	**Nachteile (Hochschulbezogen)**
Schnelle, simple und kostengünstige Umsetzung gut für den Hochschulbereich.	Gefahr, dass nicht auf die Materialien geachtet wird.
Erhöhter Personenverkehr an Hochschulen führt zur Erreichung vieler Nutzer.	

Tabelle 3.3: Vor- & Nachteile: Passives Lernen

3.1.4 Asynchrones Lernen (E-Learning)

Im Bereich des Asynchronem Lernens wird das Lernen auf Distanz behandelt. Dies wird mithilfe des E-Learnings verwirklicht. Hier wird asynchron von den Nutzern verschiedene Kampagnen zum Thema Informationssicherheit absolviert. Innerhalb einer Kampagne gibt es meist verschiedene Module zu unterschiedlichen Theman (z.b. Phishing, Passwort Sicherheit etc.). Diese Module werden üblicherweise mittels diverser Medienformate (Text, Videos, Interaktiv, Spielerisch (3.1.5)) umgesetzt, um die Themen den Nutzern verständlich zu vermitteln.

Forschungen zufolge ist die Kombination von Medienformaten und Lerntechniken besser geeignet als der Einsatz einer einzelnen Methode [2, Alahmari, 2021] [6, Bauer et al., 2017]. Dies berücksichtigt die Tatsache, dass Menschen aufgrund verschiedener Lerntypen auf unterschiedliche Weisen effektiver lernen. So gibt es Personen welche besser mit textueller Beschreibung lernen können oder wiederrum andere welche besser visuell mit Videomaterial lernen.

Durch den Asynchronen Ansatz beim Lernen, können die Nutzer selbst entscheiden, wann sie das jeweilige Modul absolvieren. Dies bietet den Nutzern mehr Flexibilität und sie können es einfacher in deren Alltag integrieren [49, Schütz et al., 2019].

Der Hauptaspekt des E-Learnings ist das Aufbauen von Wissen. Deshalb ist diese Methode gut für den Einsatz bei der Sensibilisierung von Informationssicherheit geeignet. Um hier das individuelle Lernen des Nutzers zu fördern und Inhalte zu vermitteln, die für den Nutzer relevant sind, sollten die zu behandelnden Themen an das Vorwissen des Nutzers angepasst werden. Um das Vorwissen des Nutzers zu ermitteln, lässt sich zu Beginn ein kurzer Test durchführen, den der Nutzer absolvieren muss. Anhand dessen können dann die jeweiligen Themen für die Nutzer ausgewählt werden. [49, Schütz et al., 2019]

Nach Auswertung der Wissensstände der Nutzer, können die nötigen Module den jeweiligen Nutzern einzelnd oder gruppenweise zugeordnet werden. Da diese Methode auf einer technischen Plattform passiert, kann dies auch automatisiert werden. Die Auswertung, Modulzurodnung und die Verteilung der Inhalte können automatisiert ablaufen.
Der automatisierte Ablauf sorgt dafür, dass nur wenig Personal benötigt wird, um solch ein Training durchzuführen.

Ein weiterer Vorteil ist die Möglichkeit den Inhalt der verschiednen Module zu individualisieren. Die jeweiligen Module können eigenständig erstellt werden oder es kann auch aus bereits vorhanden Modulen ausgewählt werden.

Um E-Learning effektiv einzusetzen, kann dies in Kombination mit traditionellen Methoden wie Präsentationen oder Workshops ergänzt werden. Dies argumentiert auch [49, Schütz et al., 2019]. So kann das E-Learning als Hauptlernmethode agieren und die traditionellen Methoden können ergänzend für Interessierte als Events angeboten werden, wie schon bei den interaktiven und traditionellen Lernmethoden vorgeschlagen.

Ein wichtiger Aspekt der beim E-Learning zu beachten ist, sind die Ressourcen und Kosten. Es wird eine E-Learning Plattform mit den Modulen zum Thema Informationssicherheit benötigt. Dies selbst zu entwickeln und zu programmieren ist ein hoher Aufwand. Zur technischen Konzeption und Programmierung der Plattform sind Entwickler sowie Hardware-Ressourcen erforderlich. Des Weiteren wird Personal welche sich Thematisch mit dem Thema auskennen benötigt, um die Inhalte für die Plattform zu erstellen.
Eine weitere Möglichkeit wäre das Einkaufen solch einer Plattform (Verschiedene Plattformen und deren Evaluation werden in einem Späteren Kapitel behandelt. Kapitel: 5). Beim Einkauf solch einer Plattform wird Aufwand gespart, da die externen Anbieter, welche die Plattform anbieten, meist auch Hosten und betreiben. Somit ist nur noch wenig Personal nötig, um die Plattform zu benutzen (Trainings auswählen, Trainings an Nutzer verteilen, Auswertung). Außerdem bieten die Plattformen direkt die jeweiligen Inhalte für die Module mit an.

Hochschuleignung:
Die Methode des asynchronen Lernens ist gut für ein Cyber-Security-Awareness-Konzept innerhalb des Hochschulbereiches geeignet. Angesichts der hohen Nutzeranzahl und der Diversität an einer Hochschule gibt es verschiedene Lerntypen, die jeweils unterschiedlich gut auf unterschiedliche Formate reagieren. Diese Methode bietet durch E-Learning die Unterstützung verschiedener Formate wie Texte, Videos und interaktives Lernmaterial. Dies stellt einen Vorteil für den Hochschulbereich dar, da es die Lerneffizienz der einzelnen Nutzer steigern kann.
Außerdem ist der asynchrone Ansatz vor allem im Hochschulbereich von Vorteil. In Hochschulen gibt es viele verschiedene Zeitpläne und Tagesabläufe, da die Studierende zum Beispiel verschiedene Stundenpläne haben, die Professoren verschiedene Vorlesungen etc. Deshalb ist es hier besonders von Vorteil, dass beim Ausrollen solcher Trainings keinen besonderen Wert auf die Zeitpläne der einzelnen Persone legen muss. Dies senkt den or-

ganisatorischen Aufwand enorm.
Ein wichtiger Aspekt für Hochschulen ist der Impelemtierungsaufwand bei solch einer Methode. Die technische Implementierung des E-Learnings erfordert Personal, Zeit und finanzielle Mittel. Welches oft vor allem im Hochschulbereich nur begrenzt zur Verfügung steht.

Deshalb ist eine Evaluierung nötig, welche implementierungsmethode sich für die jeweilige Organisation besser rentiert. Dennoch lässt sich sagen, dass die hohe Skalierbarkeit, die Flexibilität, der geringe organisatorische Aufwand beim laufenden Betrieb und die Effizienz im Lernprozess dieser Methode für den Einsatz im Hochschulbereich gut geeignet ist.

Die Vor- und Nachteile dieser Methode werden nochmal in Tabelle 3.4 zusammenfassend aufgeführt.

Vorteile (Allgemein)	**Nachteile (Allgemein)**
Stärkerer Lernerfolg durch Kombination von Medienformaten.	Aufwändig beim Implementieren.
Nutzer haben die Freiheit selbst Zeitpunkt und Tempo ihres Lernens zu entscheiden.	
Hohe Skalierbarkeit und Individualle Trainings möglich.	
Vorteile (Hochschulbezogen)	**Nachteile (Hochschulbezogen)**
Durch den Asynchronen Ansatz gibt es kaum Probleme beim Zeitmanagement (Stundenpläne, Arbeitszeiten etc.).	Durch den hohen Implementierungsaufwand werden Personal, Zeit und finanzielle Mittel benötigt.
Durch technische Lösungen ist ein hoher Automatisierungsgrad möglich, dadurch kann sich der Arbeitsaufwand während des Betriebes enorm senken.	

Tabelle 3.4: Vor- & Nachteile: Asynchrones Lernen

3.1.5 Spielerisches Lernen (Lernspiele)

Bei Lernspielen zur Förderung des IT-Sicherheitsbewusstseins liegt der Fokus insbesondere auf interaktiven Videospielen, die über Themen wie Phishing, Social-Engineering oder weitere Aspekte der Informationssicherheit informieren. Diese Spiele gehen über die bloße Aufklärung hinaus, indem sie interaktive Trainingsmodule bieten, durch die Nutzer lernen, potenzielle Gefahren zu erkennen und adäquat darauf zu reagieren.

Wichtig zu erwähnen ist auch, dass wenn in diesem Kontext von Lernspielen die Rede ist, bezieht sich dies auf Videospiele in digitaler Form.

Es wurde gezeigt, dass sich das Bewusstsein für Informationssicherheit der Nutzer nach Spielen dieser Lernspiele erhöht hat. Dies lässt sich vor allem darauf zurückführen, dass die Nutzer spaß beim Spielen und somit auch Spaß beim Lernen hatten. Durch den Spaß am Lernen und die hohe Interaktivität zeigten die Nutzer Bereitschaft am Informationssicherheittraining teilzunehmen. Die Beliebtheit eines Lernspiels ist jedoch ein höchst subjektives Thema und hängt maßgeblich von dem jeweiligen Spiel selbst ab. Die Attraktivität eines solchen Lernspiels kann variieren, abhängig von der Zielgruppe sowie der Gestaltung und Aufmachung des Spiels.
Außerdem zwingt die Interaktivität solcher Lernspiele die Nutzer dazu, aktiv an der Schulung bzw. am Training teilzunehmen und auch aktiv darüber nachzudenken. Schon bei der interaktiven Lernmethode wurde die Wichtigkeit der aktiven Teilnahme betont. [1, Abawajy, 2012] [24, Khando et al., 2021]

Ein weiterer Vorteil bei dieser Methode ist, dass sie die Nutzer herausfordern, motivieren und engagieren kann. Denn wenn Menschen Spiele spielen, haben sie oft das Gefühl der Beherschung, der Kompetenz, des Vergnügens, des Eintauchens in die Materie, alles Eigenschaften, die das motivierte menschliche Verhalten ausmachen. [2, Alahmari, 2021]

Zudem können die Nutzer bei dieser Methode die jeweiligen Spiele alleine absolvieren und dies von überall aus wo sie einen Computer und eine Internetverbindung haben. Es wird hier also kein spezieller Ort und auch kein persönlicher Experte für Informtaionssicherheit benötigt.

Ein Solches Lernspiel lässt sich mit der richtigen technischen Umsetzung in das E-Learning-Programm integieren. Auch hier bietet sich eine vorherige Wissensabfrage der

Nutzer gut an, um die Inhalte der Lernspiele individuell an die jeweiligen Personen zuzuweisen.

Doch, um ein Training mittels Lerspiel bereitstellen zu können, wird erst ein Spiel benötigt. Bei der Implementierung gibt es vor allem zwei Methoden: Es kann selbst entwickelt und programmiert werden, oder es wird sich eine Lernplattform gekauft welches so ein Spiel im Bereich der Informationssicherheit anbietet.

Die Entwicklung und Programmierung eines solchen Lernspiels stellt einen erheblichen Aufwand dar. Es gilt zu berücksichtigen, dass nicht nur die Erstellung und Programmierung des Spiels selbst erforderlich ist, sondern auch die Entwicklung einer Software für die Verteilung und die Auswertung der Spieldaten notwendig ist, um beispielsweise zu erfassen, wer das Training bereits abgeschlossen hat. Dabei ist ebenfalls zu berücksichtigen, dass die Entlohnung der eigenen Entwickler sowie potenziell anfallende weitere Kosten, beispielsweise für Hardware, zu tragen sind.

Demgegenüber ist der Erwerb eines solchen Lernspiels mit einem geringeren Aufwand verbunden. Allerdings ist hierbei wichtig, die damit einhergehenden Kosten zu berücksichtigen.

In beiden Szenarien ist qualifiziertes Personal erforderlich, um die Verwaltung des Spiels zu gewährleisten. Es bedarf einer verantwortlichen Person, die die Verteilung des Spiels überwacht, die Auswertungen analysiert und bei Bedarf notwendige Anpassungen durchführt.

Hochschuleignung:
Insbesondere im Hochschulbereich bietet dieser Ansatz erhebliche Vorteile. Verschiedenen Personen, die ein Training mittels Spiel absolvieren sollen, kann der Zugang bereitgestellt werden. Zusätzlich lässt sich eine Erläuterung des Zwecks und des Inhalts des Spiels übermitteln, um den Teilnehmenden einen umfassenden Überblick zu gewähren. Dadurch, dass jeder das Spiel für sich spielt, kann es auch jeder in seinem eigenem Tempo spielen und sich den Zeitpunkt des Spielens frei wählen. Somit haben die Nutzer recht viel Freiraum und Selbstbestimmung beim Training. Im laufendem Betrieb hat die Hochschule einen geringen Organisatorischen Aufwand. Durch den Asynchronen Ansatz muss nicht stark auf zeitliche Termine geachtet werden.
Dadurch, dass die Nutzer einerseits das Spiel im eigenem Tempo spielen können und andererseits die jeweiligen Spielinhalte an die verschiedenen Personengruppen der Hochschulen angepasst werden kann, fördert dies den individuellen Charakter und stärkt den

Lernerfolg bei den Nutzern.
Doch genau wie bei der asynchronen Methode ist auch hier eine sorgfältige evaluierung des jeweiligen Implementierungsverfahrens nötig. Die technische Implementierung eines einzelnen Lernspiels erfordert hohen aufwand.

Das Sicherheitsbewusstsein der Nutzer wird durch den Einsatz von Lernspielen positiv beeinflusst. Wie beim E-Learning ist auch hier die Flexibilität, die hohe Skalierbarkeit, der geringe organisatorische Aufwand und das nachhaltige Training der Nutzer von Vorteil und somit gut für den Einsatz im Hochschulbereich geeignet. Die Methode zur Implementierung solcher Spiele erfordert jedoch eine sorgfältige Abwägung.

Die Vor- und Nachteile dieser Methode werden nochmal in Tabelle 3.5 zusammenfassend aufgeführt.

Vorteile (Allgemein)	**Nachteile (Allgemein)**
Lernerfolg durch Spaß am lernen und hohe interaktion.	Beliebtheit des Lernspiels ist subjektiv und abhängig vom Spiel.
Nutzer werden motiviert zu lernen.	Hoher implementierungsaufwand und hohe implementierungskosten (kann je nach implementierung variieren).
Hohe Skalierbarkeit.	
Vorteile (Hochschulbezogen)	**Nachteile (Hochschulbezogen)**
Durch den Asynchronen Ansatz gibt es kaum Probleme beim Zeitmanagement (Stundenpläne, Arbeitszeiten etc.).	Durch den hohen Implementierungsaufwand werden Personal, Zeit und finanzielle Mittel benötigt.
Durch technische Lösungen ist ein hoher Automatisierungsgrad möglich, dadurch kann sich der Arbeitsaufwand während des Betriebes enorm senken.	

Tabelle 3.5: Vor- & Nachteile: Spielerisches Lernen

3.1.6 Auswertung der Methoden Untersuchung

In den vorherigen Abschnitten wurden die gängisten Methoden welche im Bereich Cyber-Security-Awareness eingesetzt werden, untersucht. Dabei wurde besonders auf die folgenden Aspekte eingegangen:

- Organisatorischer Aufwand.
- Eignung für den Einsatz im Hochschulbereich.
- Lernerfolg der Nutzer bzw. Annahme des Lerninhaltes durch den Nutzer.

Die Erkenntnisse dieser Untersuchung basieren auf der referenzierten Literatur. Darüber hinaus wurden verschiedene Aspekte eigenständig analysiert und spezifisch auf den Hochschulbereich angewendet.

Eine hohe aktive Teilnahme und Interaktivität der Nutzer ist ausschlaggebend für den Lernerfolg im Cyber-Security-Awareness Bereich [24, Khando et al., 2021]. Deshalb sind vor allem Methoden für ein Cyber-Security-Awareness-Konzept auszuwählen, die diese Aspekte berücksichtigen. Dies wären die interaktive Methoden (Workshops und Dialoge) und die asynchrone (E-Learning) Methode in Kombination mit der Methode des spielerischem Lernen.

Obwohl die Methode des interaktiven Lernens einen positiven Einfluss auf das Verständnis und Verhalten der Nutzer im Bereich der Informationssicherheit ausübt, gestaltet sich der organisatorische Aufwand, insbesondere bei der Implementierung im Hochschulbereich, als sehr umfangreich. Darüber hinaus ist diese Methode nicht kostenfrei, da, wie bereits erwähnt, Aufwendungen für Personal und die Bereitstellung von Räumlichkeiten anfallen und vor allem finanzielle Mittel begrenzt im Hochschulbereich zur verfügung stehen.

Dahingegen ist die Methode des asynchronen Lernens (E-Learning) in Kombination mit dem spielerischen Lernen für den Einsatz im Hochschulbereich zu empfehlen. Diese Methode gewährleistet durch die Förderung aktiver Teilnahme und hoher Nutzeraktivität einen nachhaltigen Lernerfolg. Außerdem werden noch weitere Aspekte berücksichtigt, es werden verschiedene Medienformate verwendet, um verschiedene Lerntypen zu adressieren, welches wiederrum auch einen positiven Einfluss auf den Lernerfolg hat [6, Bauer et al., 2017]. Ein weiterer positiver Aspekt, ist dass bei dieser Methode die Inhalte an

die Nutzer angepasst werden können. Es lässt sich zu Beginn ein kurzer Test durchführen, anhand dessen können dann die jeweiligen Themen für die Nutzer ausgewählt werden. Denn das Level des IT-Wissens der Nutzer ist ein wichtiger Faktor in Bezug auf die Cyber-Security-Awareness. Nutzer mit fortgeschrittenen IT-Kentnissen besitzen ein gesteigertes Bewusstsein für Cyber-Security [2, Alahmari, 2021]. Vor allem im Hochschulbereich indem die Diversität der Nutzer hoch ist, ist dies ein wichtiger Aspekt welcher zu beachten und mit dieser Cyber-Security-Awareness-Methode gut umsetzbar ist.

Im Gegensatz zu den Workshops und Dialogen ist bei dieser Methoden Kombination der Organisatorische Aufwand für Hochschulen relativ gering. Es muss nicht stark auf Zeitpläne der Nutzer geachtet werden, es müssen keine Räume zur Verfügung gestellt werden, und auch für die Nutzer ist es deutlich einfacher, denn diese können das Training in einem eigenem Tempo und in selbst ausgewählten Räumlichkeiten durchführen. Wie bei allen Methoden ist auch diese nicht kostenfrei, es kommen Aufwendungen für die Implementierung der E-Learning Plattform und das Personal, welches dieses administriert. Eine ausführliche Vorstellung von verfügbaren Produkten und Plattformen in diesem bereich einschließlich einer Evaluierung dieser wird in Kapitel fünf (5) stattfinden.

Zusätzlich zur Methode des asynchronen Lernens (E-Learning) in Kombination mit dem spielerischen Lernen ist die passive Methode eine gute Möglichkeit die Nutzer an das Thema Cyber-Security zu erinnern und deren Aufmerksamkeit darauf zu lenken. Vor allem im Hochschulbereich können gut Plakate etc. platziert werden, um Werbung für Cyber-Security zu machen und somit den Nutzer zu sensibilisieren. Die einfache und kostengünstige Umsetzung ist ein überzeugendes Argument für den Einsatz im Hochschulbereich, denn sie ist ohne großen Organisatorischen Aufwand umzusetzen und die Kosten begrenzen sich auf geringe Personal- und Materialkosten.

Des Weiteren können nach belieben die anderen Methoden auf freiwilliger Basis als Events angeboten werden. Jedoch sollte darauf geachtet werden, dass die Hauptmethoden bereits implementiert und optimiert sind, bevor sich auf die Nebenmethoden konzentriert wird. Die freiwilligen Methoden sind optional und sollten nur in Betracht gezogen werden, falls die Organisation einen deutlichen Bedarf seitens der Nutzer für diese Angebote feststellt.

Ein weiterer Aspekt, der bei der Implementierung dieser Methoden beachtet werden sollte, ist die Wiederholung und Häufigkeit der Kampagnen. Wie bereits erwähnt, ist das erlangte Wissen im Cyber-Security Bereich ein temporärer Zustand welcher in Regelmäßigen Abständen erneuert werden sollte. Zudem kommen im Hochschulbereich häufig

neue Studierende hinzu (mind. ein mal im Semester bzw. alle sechs Monate). Dies bedeutet, dass die Kampagnen mit Themen zum Grundwissen der Informationssicherheit alle sechs Monate stattfinden sollten und das an die neuen Nutzer der Hochschulorganisation gerichtet sein sollte. Allgemein kann gesagt werden, dass darauf geachtet werden muss, dass Schulungen in Regelmäßigen Abständen durchgeführt werden sollten, alle Nutzer der Organisation sollten die Schulungen erhalten und dabei ist es wichtig ein gesundes Maß einzubehalten, damit die einzelnen Nutzer nicht mit zu vielen Cyber-Security-Schulungen überhäuft werden.

3.2 Psychologische Einflussfaktoren der Cyber-Security-Awareness

Wie bereits erwähnt gibt es neben den Methoden auch Faktoren, welche das Verhalten der Menschen im Bereich der Cyber-Security beeinflusst. Dieser Abschnitt beschreibt diese Faktoren und wie sich diese von Vorteil gemacht werden können, um das Verhalten der Nutzer positiv im Sinne der Informationssicherheit zu beeinflussen.

Zu verstehen wie sich Nutzer verhalten und welche Faktoren sie beeinflussen, ist ein wichtiger Aspekt, um ein erfolgreiches Cyber-Security-Awareness-Konzept zu erstellen.

Leach John, 2003, sagt aus, dass die beeinflussenden Faktoren in zwei Gruppen unterteilt werden könnnen. Die erste Gruppe, welche das Verständnis des Nutzers bezüglich der vom Unternehmen erwarteten Verhaltensweisen umfasst, differenziert sich von der zweiten Gruppe, die auf die persönliche Bereitschaft des Nutzers abzielt, sein Verhalten anzupassen, um sich innerhalb akzeptierter und anerkannter Normen zu bewegen. [36, Leach, 2003] Die Gruppierung und die dazugehörigen Faktoren werden in Abbildung 3.1 gezeigt.

Abbildung 3.1: Beeinflussende Faktoren Sicherheitsverhalten
Quelle: Eigene Darstellung in Anlehnung an [36, Leach, 2003]

3.2.1 Erwartete Verhaltensweisen und Nutzerverständnis

Die erste Gruppe beinhaltet drei Faktoren, welche das Verständnis des Nutzers bezüglich der erwarteten Verhaltensweisen beschreibt. Der erste Faktor beschäftigt sich mit dem Wissen, also dem, was dem Nutzer gesagt und gelehrt wird. Dies beinhaltet zum Beispiel die verschiedenen Informationssicherheits Richtlinien aber auch die Zugänglichkeit zu diesen Dokumenten. [36, Leach, 2003]

Der zweite Faktor behandelt das "was sieht der Nutzer". Dies bedeutet, dass es hier um die Wahrnehmung des Nutzers bezüglich der Verhaltensweisen von Führungskräften und Kollegen geht. Im Hochschulbereich könnte dies auch auf die Studierenden und Professoren abgeleitet werden oder auch Studenten zu Studenten. Die Verhaltensweisen eines Menschen sind stark beeinflussbar durch die der anderen. Es ist also wichtig, dass Verhaltensweisen von anderen konform zu den Richtlinien sind, damit diese als Vorbild dienen. Vor allem die Führungskräfte bzw. Autoritätspersonen sollten als vorbild voranschreiten, um ein Bewusstsein für Informationssicherheit innerhalb einer Organisation zu bilden. [36, Leach, 2003] [24, Khando et al., 2021]

Der letzte Faktor aus der ersten Gruppe bezieht sich auf die Entscheidungen des Nutzers, welche dieser selbst treffen muss. Entscheidungen welche nicht in einer Richtlinie oder Leitfaden beschrieben sind. So baut sich der jeweilige Nutzer über die Zeit seine eigenen Erfahrungen auf und lernt aus diesen. Hierbei ist es wichtig, dass die Nutzer nach einer wichtigen Entscheidung Feedback erhalten um zu wissen, ob Ihre Entscheidung korrekt war oder ob sie etwas hätten anders machen können. [36, Leach, 2003]

3.2.2 Persönliche Anpassungsbereitschaft

Die zweite Gruppe bezieht sich auf die Faktoren, welches die Bereitschaft des Nutzers, sein verhalten einzuschränken, um die akzeptierten Normen einzuahlten, beeinflusst.

Der erste dieser Faktoren bezieht sich auf die persönlichen Werte der Nutzer. J. Leach argumentiert, dass es zu inneren Konflikten bei Personen kommen kann, wenn die persönlichen Werte nicht mit denen der Organisation übereinstimmen. Hierbei erweist es sich als schwierig, diese zu adressieren und zu eliminieren. Meistens führt dies dazu, dass die Person ihre Werte anpasst oder die Organisation verlässt. Im Hochschulbereich und vor allem in der Thematik der Informationssicherheit ist dieser Faktor nicht allzu relevant, denn hier geht es um das Schützen der Organisation vor Cyber-Angriffen und somit auch um das schützen der Arbeitstelle (bei Mitarbeitern & Professoren) und um das Schützen der Hochschule (bei Studenten) welches beides im Interesse aller liegt. Es stellt sich jedoch die Frage, inwieweit die Nutzer bereit sind, sich für die Erreichung des Ziels zu engagieren.[36, Leach, 2003]

Beim zweiten Faktor geht es, um den psychologischen Vertrag den jeder Mitarbeiter mit seiner Organisation hat. Hierbei handelt es sich um einen nicht schriftlichen Vertrag der besagt, dass der Mitarbeiter gute Arbeit leistet und sich den Richtlinien der Organisation konform verhält während der Arbeitgeber die Mitarbeiter gut behandelt. Die muss nicht nur in einem Arbeitsverhältniss der Fall sein, dies kann auch auf das Verhältnis der Studierende - Hochschule bezogen werden. Das bedeutet also, dass wenn sich Studenten oder Mitarbeiter gut behandelt fühlen, werden diese auch eher im interesse der Organisation handeln und somit auch eher ein Sicherheitskonformes verhalten aufzeigen. [36, Leach, 2003]

Der letzte Faktor der zweiten Gruppe bezieht sich auf den Aufwand welcher der Nutzer betreiben muss, um den Informationssicherheits Richtlinien konform zu handeln. Wenn

eine Organisation es den Nutzern einfach und unkompliziert macht, sich Sicherheitskonform zu verhalten, werden diese das auch eher tun. Wenn die Sicherheitsmaßnahmen zu kompliziert sind oder zu viel Aufwand für den Nutzer bedeuten, werden diese eher nicht eingehalten. [36, Leach, 2003]

3.2.3 Auswertung der psychologischen Einflussfaktoren

Folgende drei Faktoren und die daraus resultierenden Erkenntnisse sind wichtig, um ein positives Informationssicherheits verhalten der Nutzer zu erzielen [36, Leach, 2003]. Diese sollten auch bei der Planung und Implementierung eiens Cyber-Security-Awareness-Konzeptes beachtet werden.

Positives Verhalten von Kollegen & Führungskräften: Es ist wichtig, dass sich die Kollegen und die Führungskräfte bzw. Autoritätspersonen korrekt verhalten und als Vorbilder voran gehen, damit sich andere leichter an ihnen orienteren können. Vor allem für neue Personen in der Organisation ist dies ein wichtiger Aspekt, welche sich am Anfang viel am Verhalten der anderen orientieren. [36, Leach, 2003] [24, Khando et al., 2021]

Verständliche & zugängliche Informationssicherheits Richtlinien: Die Maßnahmen im Cyber-Security Bereich sollten einfach und unkompliziert sein. Die Nutzer sollten die Maßnahmen / Richtlinien kennen und wissen wo sie diese finden können. Eine Person sollte für eventuelle Fragen zu Verfügung stehen. [36, Leach, 2003]

Wissen der Nutzer: Die Nutzer sollten im Bereich Cyber-Security geschult und trainiert sein, um sichere und Richtlinien konforme Entscheidungen treffen zu können. Außerdem sollten diese nach einer Schulung oder Entscheidung Feedback erhalten, damit sich die Nutzer einen eigenen Wissensstand und Erfahrungsstand aufbauen können. [36, Leach, 2003] [24, Khando et al., 2021] [5, Bada et al., 2015]

Hochschulbezug:

Durch die immer wieder startenden Semester in einer Hochschule, gibt es viele regelmäßige neue Nutzer, welche dazu neigen, sich an den älteren Studenten oder Professoren zu orienteren. Deshalb ist der Aspekt des Positiven Verhaltens von Kollegen und Führungskräften besonders wichtig. Neue Studierenden orientieren sich am Anfang gern an Studierenden aus höheren Semestern oder an Professoren. Es sollte darauf geachtet werden, dass diese Personen mit einem Vorbild voran gehen, damit die neuen Nutzer bzw.

Studierende direkt das korrekte Verhalten in Bezug zur Informationssicherheit mitbekommen und adaptieren können.
Es ist auch wichtig, dass die Studierenden und aber auch die Mitarbeiter einer Hochschule, nach den Cyber-Security-Awareness-Kampagnen Feedback erhalten, wie sie diese durchgeführt haben. So können sie sich einen eigenen Wissenstand aufbauen, nachdem sie in Ernstfällen handeln können.
Allgemein kann gesagt werden, dass sich die zuvor vorgestellten Einflussfaktoren auf die Nutzer im Hochschulbereich ableiten lassen.

Diese Faktoren müssen beachtet werden, um ein positives Erscheinungsbild für das Cyber-Security-Awareness-Konzept innerhalb der Hochschule aufzubauen. Denn wenn die Nutzer positiv gegenüber dem Konzept gestimmt sind, werden diese auch aktiv mitarbeiten und gegebenfalls helfen. Und eine Mitarbeit der Nutzer sorgt wiederrum für den Erfolg der jeweiligen eingesetzten Methoden des Cyber-Security-Awareness-Konzeptes.

4 Untersuchung von Methoden zur Messung des Bewusstseins für Informationssicherheit

Dieses Kapitel behandelt, wie das Informationssicherheits Bewusstsein der jeweiligen Nutzer gemessen werden kann, um die angewandten Methoden innerhalb eines Cyber-Security-Awareness-Konzeptes zu prüfen und zu schauen, ob diese das Cyber-Security Bewusstsein der Personen nachhaltig verbessert haben.

Das Thema Messung sollte integraler Bestandteil eines jeden Cyber-Security-Awareness-Konzeptes sein. Die Erfassung des Cyber-Security-Bewusstseins der Nutzer ermöglicht es der jeweiligen Organisation, die Effektivität ihres Cyber-Security-Awareness-Konzeptes zu bewerten und erforderliche Anpassungen vorzunehmen.

In Kapitel zwei (2) wurde der PDCA-Zyklus vorgestellt und erläutert wie dieser im Kontext Cyber-Security angewendet wird. Es wurde auch erläutert wie dieser für den Erfolg eines Cyber-Security-Awareness-Konzeptes eingesetzt werden kann. Um den PDCA-Zyklus anwenden zu können, wird ein gewisses Feedback am Ende einer Cyber-Security-Awareness-Kampagne benötigt. Um solch ein Feedback einzuholen und zu schauen wie die verschiedenen Cyber-Security-Awareness-Methoden von den Nutzern angenommen werden sowie zu prüfen, ob die Awareness-Maßnahmen zu einer positiven Beeinflussung ihres Cyber-Security-Verhaltens beitragen, können verschiedene Methoden zur Messung des Bewusstseins für Informationssicherheit angewandt werden.

Laut Sykosch Arnold, 2022, gibt es vier verschiedene Methoden um das Cyber-Security Bewusstsein zu messen. [59, Sykosch, 2022]
In den folgenden Abschnitten wird erläutert wie diese vier Methoden funktionieren, zusätzlich wird untersucht wie gut diese im Hochschulbereich angewendet werden können.

4.1 Befragungen / Fragebogen

Die erste Methode umfasst Befragungen und Fragebögen. Hier geht es darum, dass die jeweiligen Personen welche eine Cyber-Security-Awareness-Schulung absolviert haben, eine Befragung oder einen Fragebogen durchlaufen sollen. Diese Messmethode ist die am häufigsten eingesetzte Methode [59, Sykosch, 2022].

Eine Befragung lässt sich als eine Art mündliche Evaluation verstehen. Hier werden der geschulten Person von einem Experten Fragen gestellt, wie in einem Interview. Die Person muss diese beantworten und dabei ihre Gedankengänge erläutern.

Bei einem Fragebogen ist der Ablauf sehr ähnlich, jedoch läuft dies asynchron ab. Hier wird kein Experte benötigt, welcher Fragen stellt. Die geschulte Person führt diesen Fragebogen eigenständig durch, welcher auch in Form eines Online-Tests stattfinden kann. Dabei werden theoretische Fragen gestellt, ähnlich wie bei der Befragung.

Dadurch, dass beim Fragebogen kein Interviewer bzw. Experte dabei ist, weist dieser eine höhere Objektivität der Messergebnisse auf als die einer Befragung. Um jedoch die Objektivität bei einer Befragung zu gewährleisten, ist es erforderlich, dass die Interviewer bzw. Experten über einheitliche Fachkenntnisse sowie eine konsistente Aufmerksamkeitsleistung in allen Befragungen verfügen. [59, Sykosch, 2022]

Mittels dieser Methode lässt sich gut das Wissen abfragen und prüfen, jedoch ist es schwer anhand dieser Methode zu sagen, wie die geschulten Personen im Ernstfall reagieren und handeln würden. Denn eine Befragung oder ein Fragebogen berücksichtigt nicht die emotionalen und psychologischen Aspekte, welche zum Beispiel bei einem Phishing-Angriff eine große Rolle spielen. Während einer Befragung oder eines Fragebogens wird die befragte Person nicht künstlich unter Druck gesetzt, sie befindet sich in einer sicheren Umgebung und ist sich bewusst, dass fehlerhafte Antworten keine gravierenden Auswirkungen auf sie selbst oder ihre Organisation haben, wie es bei einem Phishing-Angriff der Fall wäre.
Deshalb spiegeln die Messergebnisse dieser Methode nicht das reale Verhalten einer Person im Falle eines realen Angriffes.

Hochschuleignung:

Die Durchführung von Befragungen innerhalb einer Hochschule gestaltet sich aufwendig, wenn die Befragungen persönlich und Regelmäßig durchgeführt werden sollen und dies

bei allen Nutzern der Hochschule. Eine Hochschule hat durch Studierende und Mitarbeiter meist mehrere Tausend Nutzer, dies würde bedeuten, dass eine enorme Anzahl an Terminen angesetzt werden müssten und auch eine hohe Anzahl an Experten bzw. Interviewer zur Verfügung stehen müsste. Dies würde einen erheblichen organisatorischen Aufwand erfordern.
Jedoch gibt es dafür eine Lösung, die Durchführung von asynchronen Fragebögen, zur Messung des Cyber-Security Bewusstseins, lässt sich deutlich einfacher gestalten. Solche Fragebögen lassen sich, in Form eines Tests, einfach mittels einer online Plattformen erstellen und an die jeweiligen Personen innerhalb der Hochschule verteilen. Diese Funktion wird auch bei einigen E-Learning-Plattformen im Cyber-Security-Awarness Bereich angeboten. So würde sich diese Methode für den Einsatz im Hochschulbereich eigenen, wenn diese asynchron und digital implementiert ist, um den organisatorischen Aufwand gering zu halten.

Die Vor- und Nachteile dieser Messmethode werden in nachfolgender Tabelle (Tabelle: 4.1) zusammenfassend aufgeführt.

Vorteile	**Nachteile**
Objektivität der Messergebnisse gegeben	Messergebnisse spiegeln nicht das reale Verhalten der Nutzer wieder
Geeignnet für Wissensabfrage	
Selbstüberprüfung der Nutzer	
Hochschulbezug:	
Vorteile	**Nachteile**
Asynchrone Fragebögen einfach zu gestalten	Befragung (in Person) aufwendig
Digitale Lösungen senken den Arbeitsaufwand	

Tabelle 4.1: Untersuchung der Messmethode: Fragebögen

4.2 Laborexperimente (Bearbeitung von Aufgaben)

Bei den sogennanten Laborexperimenten geht es darum, das Cyber-Security Bewusstsein anhand von gestellten Aufgaben in einer bestimmten Umgebung zu testen. Ein mögliches Szenario könnte beinhalten, dass die zu testende Person aufgefordert wird, sich vorzustellen, sie wäre Mitarbeiter in der betreffenden Organisation und müsste die eingehenden

E-Mails sichten. In diesem Rahmen würden ihr verschiedene E-Mails präsentiert, wobei sie entscheiden soll, welche der Nachrichten als Phishing-Versuch zu klassifizieren ist und welche als legitime E-Mail betrachtet werden kann. Die Messung erfolgt dann mittels Auswertung anhand der Anzahl der korrekt klassifizierten E-Mails [59, Sykosch, 2022].
Es ist nicht zwingend erforderlich, dass sich die Personen als Mitarbeiter oder in einer ähnlichen Rolle vorstellen. Insbesondere im Hochschulbereich können die zu testenden Personen authentisch sein, da genau dies das Ziel der Messung ist: Das Cyber-Security-Bewusstsein der Personen in ihrer natürlichen Verfassung zu erfassen.

Es ist wichtig, dass den Nutzern unmittelbares Feedback bereitgestellt wird beim lösen der Aufgaben. Die Bedeutung von Feedback wurde bereits in Kapitel drei (3.2) hervorgehoben, um den Nutzern Aufschluss darüber zu geben, welche Entscheidungen richtig und welche falsch waren. Dies ermöglicht den Aufbau einer Erfahrungsbasis, auf die in Zukunft zurückgegriffen werden kann. [36, Leach, 2003]
Diese Methode kann für eine Wissensabfrage der Nutzer genutzt werden und dient diesen auch für eine Selbsprüfung ihrer eigenen Kentnisse.

Experimente konnten zeigen, dass die Tatsache, ob Personen vom Ziel des Experimentes wussten, einen Einfluss auf die Klassifikation von Phishing-E-Mails hat. Personen welche vom Ziel des Experimentes Bescheid wussten, haben sich mehr Zeit gelassen bei der Klassifizierung und konnten die Phishing-E-Mails auch deutlich genauer klassifizieren als Personen, welche nicht vom Ziel des Experimentes Bescheid wussten.
Dies verdeutlicht, dass die Anwendung dieser Methode zur Messung des Cyber-Security-Bewusstseins nur bedingt auf den Alltag einer Person übertragbar ist, denn die jeweiligen Personen passen ihr Verhalten durch die Testsituation an. Außerdem haben Personen im Alltag unterschiedliche Aufgaben, auf die sie sich konzentrieren müssen. Zudem haben sie verschiedene mögliche Stresssituationen, welche in einem Laborexperiment nicht berücksichtigt werden. [59, Sykosch, 2022]

Hochschuleignung:

Die Durchführung solcher Laborexperimente innerhalb einer Hochschule gestaltet sich als solches schwierig. Durch die hohe Nutzeranzahl wäre auch hier, genau wie bei den Befragungen, ein hoher Organisatorischer Aufwand nötig. Doch hierfür wäre die Lösung, dass diese Laborexperimente automatisiert werden und digital stattfinden, mittels einer geeigneten Applikation bzw. Plattform. Die jeweilige Applikation kann Aufgabenstellungen simulieren, welche der Nutzer bearbeiten muss. Es wäre möglich, diese Methode als Tests digital in die Schulung zu integrieren.

Als digitale Lösung, wäre diese Methode für den Einsatz im Hochschulbereich geeignet. Jedoch muss auch beachtet werden, dass mittels dieser Methode nicht das reale bzw. alltägliche Verhalten der Nutzer in Bezug zur Informationssicherheit gemessen wird. Ein weiterer Aspekt ist, dass die Nutzer vor allem im Hochschulbereich viele verschiedene Programme benutzen, die eventuell auch nicht alle bekannt sind. Deshalb lässt sich das reale bzw. alltägliche Verhalten der Nutzer schwer Messen, wenn das Szenario des Laborexperimentes nicht genau die alltäglichen Situationen abbildet. Diese Methode dient somit lediglich als eine Wissensabfrage.

Die Vor- und Nachteile dieser Messmethode werden in nachfolgender Tabelle (Tabelle: 4.2) zusammenfassend aufgeführt.

Vorteile	**Nachteile**
Direktes Feedback für den Aufbau einer Erfahrungsbasis für spätere reale Entscheidungen.	Nutzer passen ihr Verhalten bei simulierten Aufgabenstellungen an. Was dazu führt, das die Ergebnisse nicht auf den Alltag übertragbar sind.
Geeignnet für Wissensabfrage.	
Selbstüberprüfung der Nutzer.	
Hochschulbezug:	
Vorteile	**Nachteile**
Digitale Lösungen senken den Arbeitsaufwand.	Laborexperimente in Person sehr aufwendig.
	Es ist schwierig den Alltag eines Nutzers im Hochschulbereiches mittels Simulierter Aufgaben abzubilden.

Tabelle 4.2: Untersuchung der Messmethode: Laborexperimente

4.3 Phishing-Simulationen

Bei einer Phishing-Simulation geht es darum, dass ein realer Phishing-Angriff simuliert wird. Dabei werden Phishing-E-Mails von der Organisation an die Nutzer verschickt. Je nach Größe der Organisation und Anzahl der Nutzer werden verschiedene Vorlagen von Phishing-E-Mails versendet innerhalb eines bestimmten Zeitraumes. Dabei sollten die Phishing-E-Mails in zeitlichen Abständen versendet werden. Die Kommunikation zwischen den Nutzern einer Organisation kann Misstrauen hervorrufen, sollten alle Phishing-E-Mails gleichzeitig versandt werden. Zudem darf der Zeitraum der Simulation nicht zu

ausgedehnt sein, da sich die Information über potenzielle Phishing-E-Mails innerhalb der Organisation verbreiten könnte, was wiederum das Ergebnis der Simulation verzerren würde.

Anschließend wird die Reaktion auf diese Phishing-E-Mails überwacht. Dabei können verschiedene Reaktions-Metriken aufgezeichnet und zur Auswertung genutzt werden:

- Öffnen der Phishing-E-Mail
- Klick auf den Phishing-Link innerhalb der E-Mail
- Mehfacher Klick auf den Phishing-Link innerhalb der E-Mail
- Weitergabe sensibler Information (z.b. Passwort) als Reaktion auf die Phishing-E-Mail
- Melden der Phishing-E-Mail

Das Versenden von Phishing-E-Mails und die Sammlung der verschiedenen Metriken lässt sich mittels verschiedener Applikationen und Plattformen automatisieren, welches dazu führt, dass diese Messmethode einen geringen Personellen Aufwand benötigt.
Die Metrik "Melden der Phishing-E-Mail" benötigt jedoch einen erhöhten Aufwand. Hier gibt es verschiedene Methoden dies zu messen, entweder besitzt der E-Mail-Client die Möglichkeit, dass der Nutzer diese E-Mail melden kann, oder es werden die Antworten auf die Phishing-E-Mail (zum Beispiel Antworten auf die E-Mail mit einem Ausdruck des Unglaubens, oder auch weiterleitungen an die verantwortlichen Administratoren der Organisation) überwacht. [59, Sykosch, 2022]

Ohne eines geeigneten Tools lassen sich keine Phishing-Simulationen durchführen. Es ist also abzuwägen, welches Tool bzw. Produkt dafür genutzt werden soll. Je nachdem welches Tool für die Phishing-Simulationen verwendet wird, kann er Implementierungsaufwand höher ausfallen. Doch dies wird ausführlicher im nächsten Kapitel besprochen.

Dadurch, dass die Nutzer während der Simulation ihren alltäglichen Aufgaben nachgehen und nichts von dem simulierten Angriff wissen, erfasst diese Methode das tatsächliche Verhalten der Nutzer und zeigt dabei auch auf, wie die Organisation bei einem realen Angriff abschneiden würde. [59, Sykosch, 2022]

Es ist auch möglich, dass die Nutzer am ende einer Phishing-Simulation Feedback erhalten, so können die Nutzer ebenfalls davon profitieren und die Ergebnisse als Selbstprüfung ansehen.

Hochschuleignung:

Durch die Möglichkeit diesen Prozess zu automatisieren, ist diese Messmethode gut für den Einsatz im Hochschulbereich geeignet. Außerdem ist es möglich an verschiedene Personengruppen (Professoren, Studenten, Mitarbeiter etc.) verschiedene Phishing-E-Mails mit unterschiedlichen Vorlagen zu schicken, angepasst an deren Bedürfnisse und Situation. Hinzu kommen die generellen Vorteile dieser Messmethode, wie zum Beispiel das Testen bzw. Messen des realen Verhaltens der Nutzer.

Die Vor- und Nachteile dieser Messmethode werden in nachfolgender Tabelle (Tabelle: 4.3) zusammenfassend aufgeführt.

Vorteile	**Nachteile**
Reales Verhalten der Nutzer kann geprüft werden.	Je nach Tool kann der Implementierungsaufwand höher ausfallen.
Selbstüberprüfung der Nutzer.	
Hochschulbezug:	
Vorteile	**Nachteile**
Digitale Lösungen senken den Arbeitsaufwand.	Kosten und Aufwand für Tools müssen beachtet werden.
Individuelle Vorlagen können an verschiedene Personengruppen und deren Bedürfnisse angepasst werden, um die Phishing-E-Mails realer zu gestalten.	

Tabelle 4.3: Untersuchung der Messmethode: Phishing-Simulationen

4.4 Meldung von Sicherheitsvorfällen

Die letzte mögliche Messmethode welche von Skosch Arnold, 2022, erläutert wird, sind die jeweiligen Sicherheitsmetriken innerhalb einer Organisation bzw. die gemeldeten IT-Sicherheits Vorfälle. [59, Sykosch, 2022]

Die Idee dabei ist, dass wenn ein erhöhtes Informationssicherheits Bewusstsein innerhalb einer Organisation etabliert ist, eine Reduktion der Informationssicherheitsrelevanten Vorfälle einhergeht, bzw. auch eine Steigerung der durch den Nutzer gemeldeten Informationsicherheitsvorfälle. Denn das ist unter anderem ein Ziel, welches durch ein Cyber-Security-Awareness-Konzept verfolgt wird. [59, Sykosch, 2022]

Es ist wichtig, die Meldung von Sicherheitsvorfällen zu Überwachen und diese als eine der Metriken zu nehmen, wenn es um Anpassungsentscheidungen des Cyber-Security-Awareness-Konzeptes geht. Zu sehen, dass die Meldungen von Sicherheitsvorfällen gestiegen sind, zeigt, dass die Nutzer die Relevanz von Cyber-Security verstanden haben und das die vermittelten Inhalte innerhalb der Cyber-Security-Awareness-Schulungen aufgenommen wurden sind.

Ein weiterer Vorteil ist, dass sich durch diese Methode das reale Verhalten der Nutzer im Alltag prüfen lässt. Und durch entsprechendes Feedback können die Nutzer Erfahren, ob ihre Meldung korrekt war oder nicht, dies sorgt für eine optimale Selbsprüfung der Nutzer.

Jedoch weist diese Messmethode einige Hürden auf, wenn es um die Testökonomie (also der Aufwand der für diese Messung benötigt wird) der Skalierbarkeit und der Validität geht. Die Anzahl der Informationssicherheitsvorfälle ist abhängig von der jeweilig aktuellen Bedrohungslage. Auch lässt sich diese Methode schwer skalieren, denn wenn einige wenige Nutzer Sicherheitsvorfälle melden, lässt sich dies nicht auf andere Nutzer abbilden. Zudem würde ein ausfühlrich dokumentierter Datensatz aus der Vergangenheit gebraucht werden, um einen vorher - nachher Vergleich durchzuführen. Ein weiterer Aspekt ist, dass jeder gemeldete Sicherheitsvorfall von entsprechend geschultem Personal geprüft werden muss. Dies ist zwar aufwändig, aber im Falle eines tatsächlichen Sicherheitsvorfalls von entscheidender Bedeutung. [59, Sykosch, 2022]

Es ist jedoch trotzdem wichtig, die gemeldeten Sicherheitsvorfälle zu überwachen, um einen ungefähren Überblick darüber zu erhalten, ob das Cyber-Security-Awareness-Konzept effektiv umgesetzt wurden ist. Außerdem hilft diese Metrik dabei die aktuelle Bedrohungslage einzuschätzen. Zusätzlich lässt sich mittels dieser Methode prüfen, ob die meldewege und Prozesse passend etabliert sind innerhalb der Organisation, um gegebenenfalls nötige Anpassungen zu tätigen.

Hochschuleignung:

Es wäre möglich und von hoher Relevanz geeignete Prozesse für Hochschulen zu definieren und zu implementieren die einen solchen Meldeweg vorsehen und damit diese Messemethode unterstützen. Digitale Lösungen senken zwar den Aufwand und sind auch unabdingbar, jedoch müssen die Kosten und der Implementierungsaufwand hier beachtet werden. Eine Hürde speziell für Hochschulen wäre, dass sich die Studenten nicht ihrer Hochschule verpflichtet fühlen, durch zum Beispiel nur kurze aufenthalte etc., und somit

nicht den Sinn darin sehen, Sicherheitsvorfälle zu melden. Deshalb ist es Ziel eines Cyber-Securtiy-Awareness-Konzept diese Hürde zu überkommen und den Nutzern die Relevanz dieses Themas klar zu vermitteln.

Die Überwachung der Meldungen von Sicherheitsvorfällen als Messmethode ist zwar Aufwändig, aber von großer Bedeutung.

Die Vor- und Nachteile dieser Messmethode werden in nachfolgender Tabelle (Tabelle: 4.4) zusammenfassend aufgeführt.

Vorteile	**Nachteile**
Reales Verhalten der Nutzer kann geprüft werden.	Geringe Skalierbarkeit, da abhängig von aktueller Bedrohungslage.
Selbstüberprüfung der Nutzer.	Aufwändig: Prozesse werden benötigt, geschultes Personal zur Prüfung der Meldungen und gut dokumentierte Datensätze.
Hochschulbezug:	
Vorteile	**Nachteile**
Digitale Lösungen senken den Arbeitsaufwand.	Kosten und Aufwand für Prozesse und entsprechende Tools müssen beachtet werden.
	Hürde, dass sich Studenten nicht ihrer Hochschule verpflichtet fühlen, muss überkommen werden.

Tabelle 4.4: Untersuchung der Messmethode: Meldung von Sicherheitsvorfällen

4.5 Auswertung der Messmethoden

Die Implementierung der Messmethode mittels Fragebögen (asynchron und digital in Form von Tests) ist für den Hochschulbereich zu empfehlen. Durch diese Messmethode kann das Wissen der Nutzer abgefragt werden und zusätzlich können die Nutzer ihr eigenes Wissen prüfen.

Es wurde auch gezeigt, dass sich die Implementierung der Phishing-Simulationen empfiehlt. Mittels dieser Methode lässt sich effektiv das reale Verhalten der Nutzer innerhalb

des Hochschulbereiches testen und wie diese im Ernstfall reagieren. Durch Phishing-Simulationen könnte ein guter Einblick in den Erfolg des Cyber-Security-Awareness-Konzeptes gegeben werden.

Die Vorteile dieser beiden Methoden lassen darauf schließen, dass ein Hybrider Ansatz bzw. eine Kombination beider Methoden zu empfehlen wäre, um die Stärken der jeweiligen Methoden einzusetzen. So deckt die Phishing-Simulation den Faktor des realen Verhaltens der Nutzer ab, während die Fragebögen den Wissenschatz der Nutzer abfragen. [59, Sykosch, 2022]

Außerdem ist es wichtig, dass die Meldung der Sicherheitsvorfälle überwacht und ausgewertet wird. Dies bringt aufschluss darüber, ob die Nutzer die Relevanz von Cyber-Security verstanden haben und auch ob die Meldewege und Prozesse optimal implementiert sind.

Die Methoden lassen sich durch entsprechende Applikationen und Plattformen automatisieren und auch die Ergebnisse können einfach ausgewertet werden, so, dass der ökonomische Aufwand gering bleibt.
Somit ist eine Implementierung ohne geeignete Tools nicht möglich. Welche genauen Produkte dafür in frage kämen, wird im nächsten Kapitel besprochen.

Im Hochschulbereich können Fragebögen bzw. Tests direkt im Anschluss einer Cyber-Security-Awareness-Schulung gemacht werden, so, dass das Erlernte überprüft werden kann, sowohl als Messeung für die Organisation als auch als Selbstüberprüfung für den jeweiligen Nutzer. Dabei können die Fragebögen als Tests gestaltet werden oder interaktiv wie bei einem Laborexperiment. Durch die technische Umsetzung mittels einer geeigneten Plattform, sind hier nur wenig Grenzen gegeben. Dies lässt sich unabhängig von den verschiedenen Personengruppen innerhalb einer Hochschulorganisation gestalten.

Um dann das tatsächliche Verhalten zu messen kann eine Phishing-Simulation durchgeführt werden, hier sollte auf die Inhalte der Phishing-E-Mails geachtet werden. Es wäre sinnvoll unterschiedliche Vorlagen von E-Mails an die jeweilig unterschiedlichen Personengruppen zuschicken, damit die Phishing-E-Mails individueller sind und somit auch ansprechender für die jeweiligen Nutzer. So könnte zum Beispiel eine Phishing-E-Mail über ein Marketing Seminar eher an Studierenden aus dem Bereich Marketing gesendet werden und eine Phishing-E-Mail zum Thema neue Arbeitszeiten eher an Mitarbeiter der Hochschule. Es ist von entscheidender Bedeutung, dass Phishing-Simulationen nicht in zu kurzen Zeitabständen durchgeführt werden, um zu vermeiden, dass Nutzer von ihren

eigentlichen Aufgaben abgelenkt werden. Eine solche Vorgehensweise könnte sich negativ auf die psychologische Einstellung der Nutzer gegenüber dem Cyber-Security-Awareness-Konzept auswirken.

Die Auswertung dieser Messungen wird Aufschluss darüber geben, wie wirksam und einprägsam die jeweiligen Kampagnen der jeweiligen Cyber-Security-Awareness-Konzepte sind bzw. wie gut die jeweilig ausgewählten Methoden innerhalb des Konzeptes angenommen werden. Im Anschluss besteht die Möglichkeit das Konzept entsprechend anzupassen, falls erkennbar wird, dass die Nutzer in bestimmten Bereichen Defizite aufweisen. Dieser Prozess sollte auch iterativ und in geregelten Zeitabständen durchgeführt werden, um eine stetige Verbesserung des Cyber-Security-Awareness-Konzeptes und der allgemeineinen Sensibilisierung im Bereich der Informationssicherheit der Nutzer zu gewährleisten.

5 Evaluation von Cyber-Security-Awareness-Tools

In Kapitel drei (3) wurden verschiedene Methoden im Bereich der Cyber-Security-Awareness untersucht. In diesem Kapitel soll es darum gehen, wie Prozesse innerhalb eines Cyber-Security-Awareness-Konzeptes automatisiert werden können mithilfe von Applikationen und Plattformen, um Methoden wie zum Beispiel E-Learning umzusetzen. Dabei werden sich nicht nur auf die Methoden sondern auch auf die Prozesse welche in Kapitel vier (4) vorgestellt wurden sind, konzentriert, um zu schauen, wie diese mittels digitaler Lösungen umsetzbar sind. Denn ein erfolgreiches Cyber-Security-Awareness-Konzept ist ohne entsprechende Tools nicht realisierbar. Insbesondere für Methoden wie E-Learning oder Phishing-Simulationen sind geeignete Programme erforderlich, um diese effektiv umzusetzen.

Innerhalb der Arbeit im Cyber-Security-Awareness gibt es zwei Hauptaufgaben, welche einfach und effizient automatisiert und elektronisch verarbeitet werden können. Dies ist die Vermittlung des Inhaltes und die Testung der Nutzer. Für die Wissensvermittlung setzen die Applikationen sowohl auf Methoden des E-Learnings als auch auf Lernspiele, da sich diese mittels entsprechender Programme effektiv realisieren lassen. Für die Testung der Nutzer können innerhalb des E-Learning kurze Quizze genutzt werden oder auch wie bereits in Kapitel vier (4) vorgestellt Phishing-Simulationen durchgeführt werden. Darüber hinaus gibt es zusätzlich kleinere Aufgaben, welche mit diesen Applikationen und Plattform einhergehen, die automatisiert werden können bzw. digital umgesetzt werden, wie zum Beispiel Aufgaben im Bereich der Nutzerverwaltung oder auch im Bereich der Berichtserstattung.

Das Kapitel strukturiert sich wie folgt: Erst werden Anforderungen an die Applikationen und Plattformen definiert, mit Hinblick auf den Einsatz im Hochschulbereich. Anschließend werden verfügbare Produkte vorgestellt, sowohl frei verfügbare Produkte als auch

kommerzielle. Abschließend werden diese Produkte anhand der vordefinierten Anforderungen verglichen, um eine finale Bewertung zu präsentieren.

5.1 Anforderungen

Um die verfügbaren Produkte vergleichen zu können und anhand von bestimmten Metriken bzw. Bewertungskriterien bewerten zu können, werden Anforderungen benötigt, aus denen sich die Bewertungskriterien ableiten lassen. Die Anforderungen beinhalten sowohl Anforderungen aus der Sicht des Endnutzers, also die Personen welche die jeweiligen Produkte zum Lernen nutzen sollen, als auch Anforderungen aus der Sicht der Organisation bzw. der jeweiligen Administratoren, welche die Produkte nutzen, um den Nutzern der Organisation das Thema der Informationssicherheit näher zu bringen.

In diesem Abschnitt erfolgt die Vorstellung der Anforderungen, ergänzt um eine detaillierte Begründung für deren Auswahl. Dabei wird bei den Anforderungen immer vom Optimalprodukt ausgegangen. Die Bewertungskriterien werden jedoch auch abgestufte Anpassungen der Anforderungen berücksichtigen. Die Bewertungskriterien abgeleitet von den Anforderungen werden im nächsten Abschnitt tabellarisch dargestellt.

Die Anforderungen teilen sich in sechs verschiedene Kategorien auf:

- A1: Schulungskampagnen
- A2: Training und Inhalt
- A3: Phishing
- A4: Nutzerverwaltung
- A5: Nutzerfreundlichkeit
- A6: Datenverarbeitung

Es ist wichtig zu beachten, dass sich die Anforderungen nur auf technische, inhaltliche und regulatorische Aspekte beziehen. Finanzielle Anforderungen bzw. preisliche Anforderungen werden hier außenvor gelassen. Dies hat den Grund, dass die Ermittlung der verschiedenen Produktpreise sich als herausfordernd erweist. Zudem sind die Preise nicht immer konstant und können aufgrund zeitlich begrenzter Angebote oder Abmachungen variieren.

A1 Schulungskampagnen

A1.1 Kampagnen erstellen: Es lassen sich Schulungskampagnen erstellen. Es können verschiedene Kurse bzw. Lerninhalte zu einer Kampagne gebündelt werden und diese den verschiedenen Nutzern zugeordnet werden. Den Nutzern wird eine Einladungsmail zu den Kampagnen automatisch vom System versendet mit entsprechender Information. Es können auch Erinnerungsmails versendet werden, bei nicht abschließen einer Schulungskampagne. Schulungskampagnen sind das Grundgerüst des Cyber-Security-Awareness-Trainings im E-Learning. Es dient dazu die Inhalte zu bündeln und in regelmäßigen Abständen auszurollen. [1, Abawajy, 2012] [6, Bauer et al., 2017]

A2 Training und Inhalt

A2.1 Lerninhalte sind inkludiert: Das Produkt hat verschiedene Lerninhalte für die Schulungen und Trainings einer Cyber-Security-Awareness-Kampagne inkludiert. Dabei sollten Inhalte zu verschiedenen Cyber-Security Themen zur Verfügung stehen. Dies würde der Organisation einiges an Aufwand einsparen, diese Inhalte selbst zu gestalten oder aus freien Ressourcen zusammenzusuchen. Wie bereits in Kapitel drei (3) erläutert, ist es von Vorteil mittels verschiedener Formate zu lernen. Deshalb sollten auch die Inhalte der jeweiligen Plattform in verschiedenen Formaten inkludiert sein (zum Beispiel Lernvideos, Texte, Interaktive Module) [2, Alahmari, 2021] [6, Bauer et al., 2017] .

A2.2 Mulitlinguale Einstellungen der Lerninhalte möglich: Angesichts der hohen Frequenz im Hochschulbereich internationaler Studierender, ist es wichtig, dass das jeweilige Produkt die Trainingsinhalte in unterschiedlichen Sprachen anbietet. Hierbei sind vor allem Deutsch, als Standortsprache, als auch Englisch als Weltsprache sehr wichtig. Doch auch weitere Sprachen wären sehr von Vorteil.

A2.3 Quizze / Tests sind inkludiert: Bereits in vorherigen Kapiteln wurde erläutert, dass Feedback wichtig für ein höheres Informationssicherheits Bewusstsein der Nutzer ist, deshalb sollte das jeweilige Produkt Quizze oder Tests anbieten zu den verschiedenen Trainingsinhalten. Damit die Nutzer am Ende einer Cyber-Security-Awareness-Kampagne Feedback erhalten und wie gut sie das Wissen verinerlicht haben [36, Leach, 2003]. Des Weiteren argumentiert Chaudhary et al., 2022, dass es für die Organisation wichtig ist, das Wissen der Nutzer regelmäßig zu messen

um zu schauen, inwieweit sich das Cyber-Security-Awareness-Training das Wissen erweitert. Dabei wird vorgeschlagen, Tests vor und nach einem Training zu durchzuführen.[8, Chaudhary et al., 2022]

A2.4 Berichterstattung zum E-Learning ist inkludiert: Das Produkt sollte umfassende Auswertungen der Ergebnisse des E-Learnings bereitstellen, einschließlich der Teilnahme der Nutzer an Schulungen sowie der Testergebnisse. Dies ermöglicht es der jeweiligen Hochschulorganisation, Feedback darüber zu erhalten, wie die Maßnahmen und Kampagnen von den Nutzern angenommen werden, um gegebenenfalls Anpassungen vorzunehmen. Mithilfe dieser Auswertungen lässt sich das Interesse und Engagement der Nutzer messen. Solche Metriken sind entscheidend, um das eigene Cyber-Security-Awareness-Konzept effektiv zu bewerten. [8, Chaudhary et al., 2022]

A2.5 Exportierung der E-Learning Berichterstattung ist möglich: Die Auswertungen innerhalb der Berichterstattung sollten sich in Form von Reports exportieren lassen und auch automatisch vom System verschicken lassen. Dies unterstützt Administratoren bzw. Verantwortliche für die Informationssicherheit dabei, den aktuellen Status den beteiligten Personen vorzustellen. Dadurch können gemeinsam Entscheidungen über weitere Maßnahmen oder Anpassungen der Cyber-Security-Awareness-Strategien getroffen werden.

A2.6 Lerninhalte sind Anpassbar: Das System sollte die Möglichkeit bieten das eigene Lerninhalte importiert werden können und die inkludierten Lerninhalte exportiert werden können. Zudem sollten die Lerninhalte innerhalb des Systems anpassbar sein. Dies ermöglicht eine höhere Individualisierung der Lerninhalte, um diese an die eigenen Bedürfnisse der Hochschulorganisation anzupasen oder auch an die aktuelle Lage. Wichtig ist auch, dass die Lerninhalte so effektiv wie möglich an das Vorwissen der Nutzer und an die aktuelle Situation angepasst sind, um eine höhere Lerneffizienz zu erreichen [49, Schütz et al., 2019] [6, Bauer et al., 2017].

A3 Phishing

A3.1 Phishing-Simulationen durchführbar: Sykosch und Chaudhary et al., 2022, zeigen auf, dass simulierte Angriffe, wie zum Beispiel Phishing-Simulationen eine nützliche Methode ist, die Cyber-Security-Awareness innerhalb der Organisation zu messen und dies auch als eine Metrik zu nutzen, um das Cyber-Securtiy-Awareness-Konzept zu evaluieren. Deshalb sollte das Produkt in der Lage sein, Phishing-Simulationen

zu erstellen und durchzuführen. Um der Organisation mehr Freiraum und Spielraum zu bieten bei der Erstellung der Phishing-Simulationen ist es von Vorteil, wenn das Produkt verschiedene Templates mitbringt für die Phishing-Simulationen welche auch anpassbar sind. So können die jeweiligen Administratoren die Phishing-Simulationen auf die aktuelle Lage der Organisation anpassen. Zum Beispiel können Hochschul spezifische Phishing-E-Mails versendet werden. [59, Sykosch, 2022] [8, Chaudhary et al., 2022]

A3.2 Phishing-Berichterstattung ist inklduiert: Das Produkt ist in der Lage verschiedene Auswertungen der Phishing-Simulationen anzuzeigen in verschiedenen Formaten. Es sollten Daten wie die Klickrate auf den Phishing-Link innerhalb der Phishing-E-Mail dargestellt werden. Genau wie beim E-Learning dienen diese Auswertungen der Organisation als Feedback über die eigenen Cyber-Security-Awareness-Maßnahmen und die allgemeine Sensibilisierung der Nutzer in diesem Bereich. [8, Chaudhary et al., 2022]

A3.3 Exportierung der Phishing-Berichterstattung ist möglich: Die Phishing Auswertungen sollten sich auch exportieren lassen und automatisch per E-Mail als Report vom System verschicken lassen. Dies hilft den Administratoren bzw. den Verantwortlichen für Informationssicherheit den jeweilig aktuellen Stand den beteiligten Personen vorzustellen, um gemeinsam über Entscheidungen und über weitere Maßnahmen oder Anpassungen zu sprechen.

A4 Nutzerverwaltung

A4.1 Nutzerimport ist über verschiedene Methoden möglich: Das Produkt sollte einen Nutzerimport anbieten, um mehrere Nutzer gleichzeitig anzulegen und auch wieder zu entfernen. Zum Beispiel über einen Dateiimport oder mittels einer Synchronisation des Active-Directories. Diese Automatisierung hilft den Administratoren enorm die jeweiligen Nutzer schnell und einfach anzulegen oder zu entfernen. Da diese Aufgabe im Hochschulbereich mindestens jedes Semester gemacht werden muss, durch die neuen und die abgehenden Studierenden, ist es von Vorteil, dass dies so weit wie möglich automatisiert werden kann.

A4.2 Nutzer Gruppierung ist möglich: Es sollte möglich sein verschiedene Nutzergruppen anzulegen. So können die Hochschulen die Nutzer in die verschiedenen Fakultäten oder Rollen gruppieren (z.B. Professoren, Mitarbeiter, Fakultät-Informatik,...

etc.). Dies vereinfacht den Prozess beim verteilen der E-Learning Trainings oder Phishing-Simulationen, um den Inhalt individuellerund gezielter zu Verteilen.

A5 Nutzerfreundlichkeit

A5.1 Einfache Dokumentation: Es ist wichtig, dass die Dokumentation des jeweiligen Produktes einfach aufzufinden ist, verständlich geschrieben und vollständig ist. So können die Administratoren bei Unklarheiten schnell und einfach verschiedene Informationen in Erfahrung bringen. Außerdem wäre es von Vorteil, wenn ein Ansprechpartner der Firma des Produktes zur verfügung steht, für eventuelle Fragen. Auch Ganchev, 2007, sagt aus, dass die Dokumentation ein wichtiger Bestanddteil einer E-Learning-Software ist und diese in die Bewertungskriterien mit einfließen sollte. [15, Ganchev et al., 2007]

A5.2 Intuitive Nutzung: Das Produkt sollte sowohl von den Administratoren als auch von den Endnutzern unabhängig und intuitiv genutzt werden können. [15, Ganchev et al., 2007]

A6 Datenverarbeitung

A6.1 Frei verfügbar: Im Hochschulbereich hat es verschiedene Vorteile, wenn die genutzten Produkte frei verfügbar sind. Vor allem aber der finanzielle Aspekt spielt hier eine entscheidende Rolle. Hochschulen haben keine unbegrenzten finanziellen Mittel um beliebig viel Software einzukaufen. Wenn ein Produkt frei verfügbar ist, kann dieses meist auch frei genutzt werden. Außerdem bringt dies noch andere Vorteile mit sich, wie zum Beispiel eine hohe Anpassbarkeit oder auch eine mögliche Prüfung auf Sicherheit der Anwendung, durch direkten Zugang zum Quellcode.

A6.2 DSGVO Konform: Diese Anforderung bezieht sich speziell auf deutsche Hochschulen. Da es sich beim E-Learning um die Verarbeitung von Personenbezogenen Daten handelt, ist es wichtig, dass das Produkt der DSGVO Richtlinie konform ist.

5.2 Bewertungskriterien

Die zuvor genannten Anforderungen werden nun innerhalb einer Tabelle als Bewertungskriterien dargestellt, um die Produkte vergleichen und bewerten zu können. Dabei sind die Anforderungen innerhalb der Tabelle immer in drei verschiedenen Abstufungen zu

finden. Von Erwartungen übertroffen bis zu unter den Erwartungen. Sollte ein Produkt eine Anforderung übertreffen, wird für diese Anforderung drei Punkte vergeben. Sollte ein Produkt die Anforderung erfüllen, werden zwei Punkte vergeben und sollte das Produkt die Erwartungen für die Anforderung nicht erfüllen, wird ein Punkt vergeben. Sollte eine Anforderung überhaupt nicht erfüllt sein, wird für diese null Punkte vergeben. Beispiel: Wenn das Produkt keine Lerninhalte inkludiert, dann können diese auch nicht in verschiedenen Sprachen eingestellt werden. Daher würde für die Anforderung A1.2 null Punkte vergeben werden. Die gesamt bewertung des Produktes misst sich dann anhand der gesamt vergebenen Punktzahl. Dabei sind maximal 46 Punkte möglich. Die Gesamtpunktzahl des jeweiligen Produktes ermöglicht einen Vergleich mit anderen Produkten anhand derselben Bewertungskriterien.

Bewertungskriterien		
≙ 3 Punkte	**≙ 2 Punkte**	**≙ 1 Punkt**
Erwartungen Übertroffen	**Erwartungen Erfüllt**	**Unter den Erwartungen**
A1 Schulungs Kampagnen		
Es lassen sich regelmäßig verschiedene Schulungskampagnen erstellen, welche verschiedene Module bzw. Lerninhalte bündeln. Den Kampagnen können verschiedene Nutzer zugeordnet werden. Die Nutzer erhalten eine Einladungsmail zur Kampagne und ggf. Erinnerungsmails bei noch nicht abgeschlossener Kampagne.	Es lassen sich regelmäßig verschiedene Schulungskampagnen erstellen, welche verschiedene Module bzw. Lerninhalte bündelt. Den Kampagnen können verschiedene Nutzer zugewiesen werden. Die Nutzer erhalten eine Benachrichtigung über den Start einer Kampagne.	Es lassen sich regelmäßig verschiedene Schulungskampagnen erstellen, welche verschiedene Module bzw. Lerninhalte bündeln.

Bewertungskriterien		
≙ 3 Punkte	**≙ 2 Punkte**	**≙ 1 Punkt**
Erwartungen Übertroffen	**Erwartungen Erfüllt**	**Unter den Erwartungen**
A2 Training & Inhalt		
Das Produkt inkludiert Lerninhalte zu verschiedenen Themen der Informationssicherheit verschiedener Formate (Text, Video, Spielerisch).	Das Produkt inkludiert Lerninhalte zu verschiedenen Themen der Informationssicherheit mindestens eines Formates.	Das Produkt inkludiert keine Lerninhalte.
Die Lerninhalte sind in verschiedenen Sprachen verfügbar (Zusätzlich zu Deutsch und Englisch).	Die inkludierten Lerninhalte sind in Deutsch und Englisch verfügbar.	Die inkludierten Lerninhalte sind nur in einer Sprache (Englisch oder Deutsch) verfügbar.
Das Produkt bietet Quizze zu verschiedenen Themen der Informationssicherheit an (Passend zu den Trainings).	Das Produkt bietet ein Quiz zum Thema Informationssicherheit an.	Das Produkt bietet keine Quizze an.
Das Produkt ermöglicht eine Berichterstattung und zeigt Informationen zum E-Learning an. Sowohl über die Teilnahmestatistiken der Schulungen als auch über die Ergebnisse der Tests. Dabei werden die verschiedenen Statistiken grafisch in verschiedenen Formaten angezeigt.	Das Produkt zeigt eine Übersicht der Statistiken der E-Learning Kampagnen (Schulungen und Tests) an.	Das Produkt zeigt keine Übersichten über das E-Learning an.

Bewertungskriterien		
≙ 3 Punkte	**≙ 2 Punkte**	**≙ 1 Punkt**
Erwartungen Übertroffen	**Erwartungen Erfüllt**	**Unter den Erwartungen**
Auswertungen der E-Learning Kampagnen lassen sich exportieren und autoamtisch vom System als Report per Mail verschicken lassen.	Auswertungen der E-Learning Kampagnen lassen sich als Report exportieren.	Auswertungen der E-Learning Kampagnen kann nicht exportiert werden.
Lerninhalte können importiert / exportiert werden und innerhalb der Plattform angepasst werden.	Lerninhalte verschiedener Formate können exportiert und importiert, jedoch nicht angepast werden.	Lerninhalte können nicht importiert / exportiert oder angepasst werden.
A3 Phishing		
Es lassen sich Phishing Kampagnen erstellen und durchführen. Dabei sind unterschiedliche Templates inkludiert, welche individuell angepasst werden können und innerhalb der Kampagnen verwendet werden können.	Es lassen sich Phishing Kampagnen erstellen und durchführen.	Es können keine Phishing Kampagnen erstellt und durchgeführt werden.
Es lässt sich eine detaillierte Auswertung der jeweiligen Phishing-Kampagnen in verschiedenen Formaten (Visuell, Tabellarisch etc.) anzeigen.	Es lässt sich eine einfache Auswertung der jeweiligen Phishing-Kampagnen anzeigen (X nutzer haben auf Phishing-Link geklickt).	Es lässt sich keine Auswertung der Phishing-Kampagnen anzeigen.

Bewertungskriterien		
≙ 3 Punkte	**≙ 2 Punkte**	**≙ 1 Punkt**
Erwartungen Übertroffen	**Erwartungen Erfüllt**	**Unter den Erwartungen**
Auswertungen der Phishing-Kampagnen lassen sich exportieren und automatisch vom System per Mail versenden.	Auswertungen der Phishing-Kampagnen lassen sich exportieren.	Auswertungen lassen sich nicht exportieren.
A4 Nutzerverwaltung		
Mehrere Nutzer können gleichzeitig über Dateien importiert und somit angelegt werden (Excel Import) und auch mittels einer Synchronisation des Active Directories importiert werden. Dabei können Nutzer sowohl angelegt als auch gelöscht werden.	Mehrere Nutzer können gleichzeitig über ein Dateiimport importiert und somit angelegt werden und auch gelöscht werden.	Nutzer können angelegt werden und gelöscht werden.
Es können mehrere Gruppen angelegt werden. Nutzer können in diese Gruppen eingeteilt werden. Nutzer können beim Import verschiedene ”Gruppen Attribute” mitgegeben werden, sodass diese autoamtisch beim Erstellen gruppiert werden.	Es können mehrere Gruppen angelegt werden. Nutzer können in diese Gruppen eingeteilt werden.	Es können keine Gruppen angelegt werden.

Bewertungskriterien		
≙ 3 Punkte	**≙ 2 Punkte**	**≙ 1 Punkt**
Erwartungen Übertroffen	**Erwartungen Erfüllt**	**Unter den Erwartungen**
A5 Nutzerfreundlichkeit		
Die Erklärung / Dokumentation ist einfach und das Produkt enthält Bedienungshilfen.	Die Erklärung / Dokumentation ist einfach.	Die Erklärung / Dokumentation ist herausfordernd.
Unabhängige und intuitive Nutzung.	Nutzung des Produktes mit minimaler Unterstützung.	Nutzung nur mit hohem Unterstützungsaufwand.
A6 Datenverarbeitung		
N. A.	Das Produkt ist frei verfügbar.	Das Produkt ist nicht frei verfügbar.
N. A.	Das Produkt ist DSGVO Konform.	Das Produkt ist nicht DSGVO konform.

Tabelle 5.1: Bewertungskriterien

5.3 Verfügbare Produkte

Hier werden nun einige verfügbare Produkte vorgestellt. Die Pordukte wurden mittels online Recherche ausgewählt. Der Markt bietet selbstverständlich noch mehr Produkte zum Thema Cyber-Security-Awareness an, doch alle hier abzudecken, würde den Rahmen einer Bachelorarbeit sprengen. Deshalb wurde sich hier nur auf einige bekannte Produkte aus dem frei verfügbarem und dem kommerziellen Bereich beschränkt.

5.3.1 Frei Verfügbare Produkte

Mit frei verfügbaren Produkte ist gemeint, dass die jeweiligen Lösungen frei und kostenlos zur Verfügung stehen und der Quellcode gegebenenfalls einsehbar ist.

BITS (Behörden IT-Sicherheitstraining): BITS ist eine frei verfügbare Web-basierende Lernsoftware, welche vor allem den Mitarbeitern in den Verwaltungen Deutschlands als Cyber-Security-Awareness Plattform dient. BITS basiert auf Textdateien in der Markdown Sprache und kann beliebig angepasst werden. Durch die Ordnerstruktur, kann BITS in die eigenen Systeme (z.B. Intranet) integriert werden. Zudem kann es online direkt ohne weitere Anpassungen genutzt werden. Die Herausgeber von BITS sind die Kommunal Agentur NRW GmbH und Herr Dr. Lutz Golan vom Landesbetrieb Verkehr Hamburg. [12, BITS Webseite]

ZibaSec Awareness Training: ZibaSec ist ein Open Source Projekt, dessen Ziel es ist Lernmaterial für den Cyber-Security Bereich bereitzustellen. ZibaSec bietet zu verschiedenen Themen wie zum Beispiel Phishing-Angriffen oder Malware Lerninhalte an. Die Lerninhalte stehen online auf der Webseite zur Verfügung. Die Inhalte können runtergeladen und in eigene Systeme integriert werden. [11, ZibaSec Webseite]

Pagerduty: Pagerduty ist ein amerikanisches Unternehmen, welches sich im Cloud Bereich auf eine SaaS Incident Response Plattform für den IT Bereich spezialisiert hat. Dabei bietet Pagerduty einen Teil seiner internenen Cyber-Security-Awareness Lerninahlte als frei verfügbare Kurse an. Die verschiedenen Inhalte können als PDF Dateien heruntergeladen werden und für eigene Zwecke genutzt werden. [46, Pagerduty Webseite]

MoodleLMS: Laut der Online-Zeitschrift Forbes zählt MoodleLMS zu den führenden Open Source Plattformen im Bereich der Lernmanagement-Systeme bzw. E-Learning Plattformen [20, Haan, 2024]. Moodle bietet den Nutzern vielfältige Individualisierungsmöglichkeiten und stellt zusätzlich eine kommerzielle Cloud-Lösung zur Verfügung. Die Open Source Software wird von über 200 deutschen Hochschulen verwendet und hat somit eine große Community im Hochschulbereich mit vielen Erfahrungswerten. [38, Moodle Webseite] [21, Moodle an Hochschulen e.v.]

GoPhish: Eine bekannte Open Source Phishing-Applikation ist GoPhish. Es bietet den Nutzern die Möglichkeit ihre Organisation mittels Phishing-E-Mails zu testen. [19, GoPhish Webseite]

5.3.2 Kommerziell

Mit kommerziellen Produkten ist gemeint, dass die jeweiligen Lösungen kostenpflichtig sind, welche erworben werden müssen bzw. für deren Nutzung Lizenzgebühren anfallen. Der Quellcode dieser Produkte ist nicht einsehbar.

KnowBe4: KnowBe4 ist ein Unternehmen aus den Vereinigten Staaten von Amerika mit einer Zweigstelle in Berlin, Deutschland. KnowBe4 hat viele Auszeichnungen, unter anderem wird KnowBe4 als sogenannter Leader von der renomierten Zeitschrift Forrester Wave im Jahr 2022 ausgezeichnet [7, Budge, 2022]. Wie viele kommerziell ausgerichtete Unternehmen in diesem Bereich, bietet KnowBe4 eine von denen verwaltete Cyber-Security-Awareness Plattform an, mit verschiedenen Möglichkeiten, dass Cyber-Security-Awareness Training zu gestalten. [30]

SoSafe: SoSafe GmbH ist ein deutsches Unternehmen welches eine Cyber-Security-Awareness Plattform als einen Managed-Service anbietet. Dabei hat sich SoSafe unter anderem auf Kunden des öffentliches Sektors (z.B. Universitäten) spezialisiert. Die Plattform bietet eine breite Palette an Optionen im Bereich der Cyber-Security-Awareness. Ziel von SoSafe ist es, den Kunden möglichst viel Arbeit abzunehmen und viele Prozesse zu automatisieren bzw. als einen Managed-Service anzubieten. [54, SoSafe Webseite]

5.4 Untersuchung der Produkte

Für die Untersuchung der verschiedenen Applikationen und Produkte wurden die Informationen aus den jeweiligen Webseiten und Dokumentationen der Hersteller entnommen. Des Weiteren wurde für das MoodleLMS und für die Applikation von SoSafe ein Demo Zugang verwendet, um das Produkt näher kennen zu lernen. Zusätzlich wurden mehrere Gespräche mit einem Vertreter von SoSafe geführt, um die einzelnen Features detailliert kennenzulernen und zu verstehen.

Die Produkte BITS, ZibaSec Awareness Training und Pagerduty werden in der Untersuchung nicht weiter bzw. detailliert betrachtet. Alle drei Projekte stellen nur Lerninhalte in verschiedenen Formaten zur Verfügung. Es ist hier nicht möglich Schulungskampagnen zu gestalten, Nutzer anzulegen oder Berichterstattungen automatisiert abzulesen. Es wäre möglich die Lerinhalte welche diese Projekte bieten, zu nutzen, um diese in anderen

Programmen zu importieren (z.B. in Moodle oder SoSafe) und diese Lerninhalte dort zu nutzen. Jedoch reicht dies nicht für eine weitere und detaillierte Betrachtung.

Das Open Source Produkt von Moodle wird zusammen mit der Open Source Phishing-Applikation GoPhish untersucht. Da Moodle eigentständig keine Phishing-Simulationen gestalten kann und GoPhish eigenständig keine Schulungen bieten kann, ergänzen sich beide Programme ideal, um diese als ein gemeinsames Konstrukt zu betrachten und zu untersuchen. Dies stellt auch ein gewisses Gleichgewicht zwischen den frei verfügbaren Produkten und den kommerziellen Produkten her.

5.4.1 Untersuchung: MoodleLMS & GoPhish

Wie bereits erwähnt, werden hier MoodleLMS und GoPhish gemeinsam betrachtet und als eine Lösung bewertet. Da MoodleLMS sich nur auf das Thema E-Learning fokussiert, wird GoPhish als Open Source Phishing-Plattform hinzugenommen, um eine ganzheitliche Bewertung zu ermöglichen.

Für die Untersuchung von MoodleLMS und GoPhish wurden zum einem die Produkt Dokumentationen als Referenz genutzt und zum anderen wurden beide Produkte in einer kleinen Demo Umgebung betrachtet.

Um MoodleLMS zu nutzen gibt es drei verschiedene Optionen dieses Produkt zu beschaffen. Die erste Option ist, das kostenlose Open Source Programm herunterzuladen und selbst auf einem eigenen Server zu hosten. Die zweite Option ist es eine Lizenz zu kaufen für das MoodleLMS-Cloud Produkt, hier wird MoodleLMS auf einem Cloud-Server gehostet und direkt von Moodle verwaltet. Die dritte Option ist es sich mit einem Moodle Dienstleister in Verbindung zu setzen, welcher einen dann berät und bei der Konfiguration unterstützt. [37, Moodle Docs.]

Da dieses Produkt in dieser Arbeit als frei verfügbares Beispiel fungiert, wird sich hier auf die kostenlose Open Source Variante fokussiert.

Mithilfe des Produktes lassen sich Kurse erstellen, in die Nutzer hinzugefügt werden können. Hinzugefügte Nutzer erhalten eine Begrüßungsnachricht. Innerhalb eines Kurses können dann beliebige Inhalte verschiedener Formen gebündelt werden. Deshalb werden hier drei Punkte für das Kriterium Schulungs Kampagnen vergeben. [40, Moodle Docs.]

Beim Kriterium Training und Inhalt erhält MoodleLMS acht Punkte. Das Produkt enthält keine Lerninhalte und keine Quizze. Jedoch stellt es die Infrastruktur bereit, um diese selbst zu erstellen oder zu importieren. Hier gibt es verschiedene Möglichkeiten, zum Beispiel kann auch auf Projekte wie ZibaSec, BITS oder Pagerduty zurückgegriffen werden, welche Inhalte zur Verfügung stellen. Diese könnten dann in MoodleLMS importiert werden. Es können verschiedene Berichte, sogenannte Kursberichte, angesehen werden, mit unterschiedlichen Statistiken zur Nutzeraktivität. Diese Statistiken sind auch mittels einfach gehaltenen Grafiken einsehbar. Jedoch lassen sich nicht komplette Berichte exportieren, es können jediglich nur vom Lehrer eingetragene Bewerungen exportiert werden. [43, Moodle Docs.] [39, Moodle Docs.]

Wie schon erwähnt unterstützt Moodle als Open Source Learning-Management-System keine Phishing-Simulationen, jedoch könnte Moodle gemeinsam mit der Open Source Software GoPhish innerhalb des Cyber-Security-Awareness-Konzeptes genutzt werden, um die Phishing-Simulation damit abzudecken. Mittels GoPhish lassen sich Kampagnen erstellen und durchführen. Dabei können verschiedene Templates selbst erstellt werden oder importiert werden. Detaillierte Auswertungen der Phishing-Kampagnen lassen sich innerhalb des GoPhish Dashboards anschauen. Diese Auswertungen lassen sich auch exportieren, jedoch nicht automatisiert per E-Mail senden. Es ist möglich die Reports mittels der vorhanden API von GoPhish zu individualisieren und anzupassen. Somit werden sieben Punkte für das Kriterium Phishing vergeben. [16, GoPhish Docs.] [17, GoPhish Docs.]

Bei der Nutzerverwaltung erhalten MoodleLMS und GoPhish fünf Punkte. Nutzer können manuell oder automatisiert mittels eines Dateiimportes angelegt werden. Zusätzlich kann bei MoodleLMS mittels LDAP eine Synchronisation zum Active Directory hergestellt werden. Bei GoPhish gibt es Möglichkeiten dies weiter über die vorhanden API zu automatisieren. Außerdem können Nutzer gruppiert werden. [44, Moodle Docs.] [45, Moodle Docs.] [18, GoPhish Docs.]

Für das Kriterium Nutzerfreundlichkeit werden fünf Punkte vergeben, sowohl die Dokumentation von MoodleLMS als auch die von GoPhish ist leicht zu finden und verständlich formuliert. Die Nutzung der Produkt ist mit etwas Hilfestellung einfach gestaltet. [41, Moodle Docs.] [18, GoPhish Docs.]

Beide Produkte sind Open Source, somit frei verfübar und werden selbst gehostet. Durch das selbst hosting haben die Anwender selbst die Möglichkeit Maßnahmen zu ergreifen, um die Anwendung und die dort gespeicherten Personenbezogenen Daten DSGVO

konform zu behandeln. Während MoodleLMS eine entsprechende Dokumentation dafür bietet und auch die DSGVO Konformität unterstützt mit entsprechenden Anforderungen, wie zum Beispiel bei der Nutzerauthentifizierung, konnte für GoPhish nichts in diesem bereich gefunden werden. Dies impliziert, dass bei der Implementierung von GoPhish eigene Maßnahmen entwickelt werden müssen. Bei einem Produkt, das selbst gehostet wird und dessen Daten auf eigenen Servern gespeichert sind, ist dies jedoch nicht problematisch. Aus diesem Grund werden für das Kriterium Datenverarbeitung vier Punkte vergeben. [42, Moodle Docs.]

Dies führt zu einer Gesamtbewertung von 32 Punkten bei insgesamt 46 möglichen Punkten.

Hochschuleignung:

Die Gesamtbewertung ist zwar niedrig ausgefallen, jedoch muss dabei beachtet werden, dass sich die Bewertungskriterien hauptsächlich auf technische und inhaltiche Aspekte beziehen. Es werden keine finanziellen Aspekte in der Bewertung berücksichtigt. Sowohl MoodleLMS als auch GoPhish sind kostenfreie Open Source Produkte, die uneingeschränkt genutzt werden können. Bei der endgültigen Produktentscheidung sollte dieser Aspekt positiv in die Entscheidungsfindung eingebracht werden, vor allem für Hochschulen, welche nur finanziell begrenzte Mittel haben, ist dies von vorteil. Ein weiterer wichtiger Aspekt ist, dass MoodleLMS bereits an einer Vielzahl von deutschen Hochschulen verwendet wird und somit auch einerseits eine große Community hat, welche sich gegenseitig unterstützen kann und andererseits, ist damit das Produkt an vielen Hochschulen schon implementiert und es müsste nur noch die Anpassungen für die Cyber-Security-Awareness-Schulungen erfolgen. [21, Moodle an Hochschulen e.V.] Jedoch ist bei diesen Produkten ein erhöhter Implementierungsaufwand gegeben. Die Infrastruktur wie Server (für das Hosting) und die Inhalte für die Schulungen müssen selbständig erarbeitet werden, welches den Aufwand erhöht.

Die Punkteverteilung sowie die Vor- und Nachteile für den Hochschulbereich werden in folgender Tabelle (5.2) zusammenfassend aufgeführt (die vollumfängliche Bewertung wird Tabellarisch im Anhang präsentiert. Tabelle: A.1):

MoodleLMS & GoPhish	
Kriterium	**Erhaltene Punkte**
A1 Schulungskampagnen	3
A2 Training und Inhalt	8
A3 Phishing	7
A4 Nutzerverwaltung	5
A5 Nutzerfreundlichkeit	5
A6 Datenverarbeitung	4
Gesamt:	**32**
Hochschuleignung: Vor- (+) & Nachteile (-)	
- Hoher Implementierungsaufwand	
+ Kostenfrei	
+ Große Community im Hochschulbereich	
+ Bereits hohe Implementierungsrate im Hochschulbereich	

Tabelle 5.2: Bewertung von MoodleLMS & GoPhish

5.4.2 Untersuchung: KnowBe4 KMSAT

Das amerikanische Unternehmen KnowBe4 Inc. bietet das Cyber-Security-Awareness Produkt KMSAT an. Eine von KnowBe4 gehostete und verwaltete Plattform, welche den Kunden dazu dient Cyber-Security-Awareness-Schulungen zu erstellen, zu verwalten und durchzuführen. Dabei werden vier verschiedene Lizensmodelle angeboten: Silber, Gold, Platinum und Diamand [34, KowBe4, 2024]. Die unterschiedlichen Lizensierungspakete unterscheiden sich vor allem in der Anzahl der mitgelieferten Trainingsinhalte und einigen technischen Features, wie zum Beispiel einem API Zugang zu Reporting und Nutzer-Events.

Da die Lizensierungspakete abhängig von den Preisen sind, werden diese erstmal außen vor gelassen. Konkrete Preise werden innerhalb der Untersuchung nicht weiter berücksichtigt, da diese meist variabel (abhängig von Nutzeranzahl und zeitlichem Angebot) sind und auch nicht öffentlich einsehbar. Es wird sich auf die höchst mögliche Lizensierung konzentriert, da diese alle Funktionalitäten zur Verfügung stellt und somit eine optimale technische Bewertung des Produktes ermöglicht. Für eine konkrete Implementierung innerhalb des Hochschulbereiches sollten diese Aspekte jedoch berücksichtigt und mit den Herstellern besprochen werden.

Für das Kriterium Schulungskampagnen werden drei Punkte vergeben. Schulungskampagnen lassen sich mit verschiedenen Modulen erstellen und die Nutzer können mittels Einladungsmails eingeladen werden. [28, KowBe4 Docs.]

Für das Kriterium Training und Inhalt erhält KnowBe4 18 Punkte. Je nach Lizensierung erhält das Produkt eine Vielzahl an unterschiedlichen Lerninahlten in unterschiedlichen Formaten (Videos, Spielerisch, Texte, Quizze) und Sprachen. Die Berichterstattung gibt zu einem die Möglichkeit die einzelnen Trainingskampagnen anzuschauen und visuell darzustellen, als auch einen sogennanten Report für Führungskräfte zu erstellen, welcher die Daten aus mehreren Trainingskampagnen zusammenträgt und so einen historischen Überblick für die jeweilige Organisation zeigt. Beide Reportarten lassen sich anpassen und somit individualisieren. Außerdem lassen sich die Reports als PDF- oder CSV-Datei exportieren. Die Reports für die Führungskräfte lassen sich so einrichtigen, dass diese automatisch vom System versendet werden. Außerdem ist der Import und Export der Trainingshinhalte ebenfalls möglich. [33, KowBe4, 2024] [29, KnowBe4 Docs] [32, KowBe4 Docs.]

Beim Kriterium Phishing erhält das Produkt neun Punkte. Es lassen sich Phishing-Kampagnen erstellen und den jeweiligen Nutzern zuordnern. Dabei bringt KnowBe4 eigene und verschiedene Phishing-Templates mit. Sowohl die Phishing-Templates als auch die Landingpages auf die die Phishing-E-Mails verlinken, lassen sich bearbeiten und somit individualisieren. Die Berichterstattung erfolgt entweder über einen Phishing-Report oder auch über den Report für die Führungskräfte, welcher automatisch exportiert und versendet werden kann. Die Phishing-Reports sind anschaulich visualisiert und auf der Plattform interaktiv gestaltet. Ebenfalls ist es auch hier möglich die Reports anzupassen und als PDF oder CSV herunterzuladen. [27, KowBe4 Docs.] [32, KowBe4 Docs.]

Für die Nutzerverwaltung erhält die Applikation sechs Punkte. Die Nutzer lassen sich effizient und einfach über verschiedene Möglichkeiten importieren, dabei funktioniert sowohl ein Dateiimport als auch eine Synchronisation des Active-Directories. Nutzergruppen lassen sich automatisch erstellen und die jeweiligen Nutzer können einfach gruppiert werden. [31, KnowBe4 Docs.]

Im Bereich der Nutzerfreundlichkeit erhält KMSAT von KnowBe4 fünf Punkte. Die Dokumentation ist übersichtlich erstellt und ist anwenderfreundlich lesbar. Da die Plattform selbst nicht getestet werden konnte, wurden hier nur Screenshots innerhalb der Dokumentation und Referenzen auf der Webseite als Anhaltspunkt für die Nutzerfreundlichkeit der

Applikation verwendet. Deshalb konnte hier nicht die volle Punktzahl vergeben werden. [25, KnowBe4 Docs.]

Beim letzten Kriterium erhält das Produkt drei Punkte. KMSAT ist nicht frei verfügbar. Trotzdessen das KnowBe4 ein amerikanisches Unternehmen ist, werden alle Daten von ihnen gemäß DSGVO verarbeitet. [26, KnowBe4 Datenschutzerklärung]

Damit beläuft sich die Gesamtbewertung vom KnowBe4 Awareness Produkt auf 44 Punkte von 46 möglichen Punkten.

Hochschuleignung:

Das Produkt an sich ist ein gutes Produkt mit vielen Features, jedoch lässt sich nichts spezielles zur Hochschuleignung finden. Es ist ein Kommerzielles Produkt, deshalb sind vor allem die Lizenzkosten zu beachten, welche nutzerabhängig sind. Dies kann für Hochschulen zu hohen Kosten führen, aufgrund der hohen Nutzer innerhalb einer Hochschule.

Die Punkteverteilung sowie die Vor- und Nachteile für den Hochschulbereich werden in folgender Tabelle (5.3) zusammenfassend aufgeführt (die vollumfängliche Bewertung wird Tabellarisch im Anhang präsentiert. Tabelle: A.2):

KnowBe4: KMSAT	
Kriterium	**Erhaltene Punkte**
A1 Schulungskampagnen	3
A2 Training und Inhalt	18
A3 Phishing	9
A4 Nutzerverwaltung	6
A5 Nutzerfreundlichkeit	5
A6 Datenverarbeitung	3
Gesamt:	**44**
Hochschuleignung: Vor- (+) & Nachteile (-)	
- Kostenpflichtig	
Keine Hochschulspezfischen Vorteile gegeben	

Tabelle 5.3: Bewertung von KnowBe4: KMSAT

5.4.3 Untersuchung: SoSafe

Die Untersuchung von dem Cyber-Security-Awareness-Produkt von SoSafe erfolgte mittels mehrerer Gespräche mit einem Vertreter des Herstellers, um ein detaillierten Einblick

zu erhalten. Zusätzlich wurde das Produkt über einen eigenen Demo-Zugang getestet. Die verschiedenen Features des Produktes und die dazugehörigen Lizensierungsmodelle lassen sich in der SoSafe Feature Matrix einsehen [57, SoSafe, 2024]. Außerdem können weitere technische Informationen über das Produkt in der Dokumentation eingesehen werden [53, SoSafe Docs.].

Als kommerzielles Produkt bietet SoSafe fünf verschiedene Lizensierungmodelle an: Essentials, Professional, Premium, Enterprise-Option und Multi-Tenancy. Dabei sind die Lizensierungsmodelle Enterprise-Option und Multi-Tenancy als Zusatz zu buchen wobei eine der ersten drei Lizensierungspakete als Grundbasis erforderlich ist. Die ersten drei Lizensierungspakete unterschieden sich im Umfang des Inhaltes und der technischen Möglichkeiten. Die zusätzlichen Lizensierungspakete geben dann noch die Möglichkeit extra Feautres zu nutzen und auf einen intensiveren Support des Herstellers zurückzugreifen. [57, SoSafe, 2024]

Da die Lizensierungspakete abhängig von den Preisen sind, werden diese erstmal außen vor gelassen. Konkrete Preise werden innerhalb der Untersuchung nicht weiter berücksichtigt, da diese meist variabel (abhängig von Nutzeranzahl und zeitlichem Angebot) sind und auch nicht öffentlich einsehbar. Es wird sich auf die höchstmögliche Lizensierung konzentriert, da diese alle Funktionalitäten zur Verfügung stellt und somit eine optimale technische Bewertung des Produktes ermöglicht. Für eine konkrete Implementierung innerhalb des Hochschulbereiches sollten diese Aspekte jedoch berücksichtigt werden und mit den Herstellern besprochen werden.

Für das Kriterium Schulungs Kampagnen werden drei Punkte vergeben. Schulungskampagnen lassen sich effizient einrichten und die Nutzer erhalten je nach Konfiguration Einladungsmails sowie Erinnerungsmails. [57, SoSafe, 2024]

Beim Kriterium Training und Inhalt erhält die Applikation 18 Punkte. Je nach Lizenz bietet SoSafe über 50 verschiedene Lerninhalte in verschiedenen Sprachen an. Die Lerninhalte sind in unterschiedlichen Formaten vorhanden, darunter sind auch spielerische Module. Außerdem werden Quizze angeboten, welche das vermittelte Wissen abfragen. Es lassen sich Lerninhalte sowohl importieren als auch exportieren. Die Berichterstattung der Schulungskampagnen sind übersichtlich dargestellt, lassen sich exportieren und ggf. auch über die sogennante Manager-Escelation automatisiert per E-Mail verschicken. [57, SoSafe, 2024] [58, SoSafe, 2024]

Im Bereich des Phishing erhält SoSafe neun Punkte. Es lassen sich Phishing-Kamapgnen erstellen, dabei bietet SoSafe verschiedene Templates an, welche zusätzlich angepasst werden können. Auch die Berichterstattung der Phishing-Kampagnen sind detailliert und visuell ansprechend dargestellt, es werden unter anderem Statistiken wie die Klickrate, Interaktionsrate und die Melderate angezeigt. [57, 56]

Beim Kriterium Nutzerverwaltung erhält das Produkt sechs Punkte. Die Nutzer können über zwei verschiedene Wege importiert werden, über eine Synchronisation des Active Directories oder über einen Datei import (CSV). Dabei können den Nutzern Gruppen-Tags mitgegeben werden, um diese automatisch zu gruppieren. [57, SoSafe, 2024] [55, SoSafe Docs.]

Bei der Nutzerfreundlichkeit werden SoSafe fünf Punkte vergeben. Das Produkt lässt sich intuitiv nutzen und auch die Dokumentation ist verständlich. Jedoch ist das finden der Dokumentationsseite nicht ganz intuitiv. [57, SoSafe, 2024] [53, SoSafe Docs.]

Beim letzten Kriterium der Datenverarbeitung erhält SoSafe drei Punkte. Als deutscher Hersteller achtet SoSafe darauf, dass das Produkt DSGVO Konform ist, jedoch ist es nicht frei verfügbar. [52, SoSafe Datenschutzerklärung]

Die Bewertung von SoSafe mittels der erstellten Bewertungskriterien beläuft sich auf eine Gesamtpunktzahl von 44 Punkten von 46 möglichen Punkten.

Hochschuleignung:

Es sind noch zwei wichtige Aspekte zu nennen. Das Produkt bietet viele ideale Features an, mit denen sehr gut im Hochschulbereich mittels verschiedenen Formaten das Cyber-Security-Awareness-Konzept vorangebracht werden kann. Der erste Aspekt, welcher zu beachten ist, ist dass das Produkt ein Kommerzielles Produkt ist. Die Kosten des Produktes werden unter anderem anhand der Nutzeranzahl bestimmt. Vor allem im Hochschulbereich kann dies durch die hohe Anzahl der Studenten schnell zu sehr hohen Kosten führen, dies muss bei der Produktentscheidung beachtet werden. Der zweite Aspekt spricht für das Produkt und seine Hochschuleignung. Als deutscher Anbieter hat sich SoSafe auf Kunden im öffentlichem Raum spezialisiert, dazu gehören unter anderem Hochschulen. Somit hat SoSafe Erfahrung mit Kunden im Hochschulbereich und die Plattform ist schon bei einigen Hochschulen in Deutschland im Einsatz. Dies spricht sehr für das Produkt, da durch die vorhandene Erfahrung die Implementierung auf bewährte Erfahrungswerte anderer Kunden im Hochschulbereich gestützt werden kann.

Die Punkteverteilung sowie die Vor- und Nachteile für den Hochschulbereich werden in folgender Tabelle (5.4) zusammenfassend aufgeführt (die vollumfängliche Bewertung wird Tabellarisch im Anhang präsentiert. Tabelle: A.3):

SoSafe	
Kriterium	**Erhaltene Punkte**
A1 Schulungskampagnen	3
A2 Training und Inhalt	18
A3 Phishing	9
A4 Nutzerverwaltung	6
A5 Nutzerfreundlichkeit	5
A6 Datenverarbeitung	3
Gesamt:	**44**
Hochschuleignung: Vor- (+) & Nachteile (-)	
- Kostenpflichtig	
+ Hersteller ist unter anderem auf Hochschulen spezialisiert	
+ SoSafe besitzt Erfahrung bei der Implementierung im Hochschulbereich	

Tabelle 5.4: Bewertung von SoSafe

5.5 Auswertung der Produkt Untersuchung

In den vorherigen Abschnitten wurden Produkte untersucht mit denen Cyber-Security-Awareness-Trainings gestaltet werden können. Vor der Untersuchung wurden Anforderungen entwickelt und mithilfe einer Bewertungstabelle aufgestellt. Die Bewertungskriterien haben sich vor allem auf technische Anforderungen für E-Learning Applikationen fokussiert. Die Produkte haben in der Untersuchung mittels der Bewertungskriterien Punkte erhalten, um diese besser vergleichen zu können. Es konnten insgesamt 46 Punkte erreicht werden.

Am Anfang wurden mehrere Produkte und Applikationen vorgestellt. Für die detaillierte Untersuchung wurden dann vier Applikationen ausgewählt, SoSafe, KnowBe4 und MoodleLMS zusammen mit GoPhish. Wichtig zu beachten ist, dass MoodleLMS und GoPhish gemeinsam betrachtet wurden sind. Dabei haben die Kommerziellen Produkte von SoSafe und KnowBe4 beide den selben Punktestand von 44 Punkten erreicht, während die Applikation ModdleLMS zusammen mit GoPhish 32 Punkte erreicht haben. Technisch gesehen sind SoSafe und KnowBe4 ebenbürtig und bieten beide ausgezeichnete Funktionen. Aufgrund der Tatsache, dass SoSafe ein deutscher Hersteller mit solider Erfahrung

im deutschen Hochschulbereich ist und durch verschiedene Kundenreferenzen gestützt wird, ist SoSafe gegenüber KnowBe4 zu bevorzugen.

Wenn jedoch ein frei verfügbares Produkt gefragt ist, ist MoodleLMS zusammen mit GoPhish eine geeignete Lösung und Alternative zu den Kommerziellen Produkten. Es ist wichtig zu beachten, dass MoodleLMS und GoPhish zwei komplett seperate Programme sind. Sie müssen beide also einzelnd implemtiert und verwaltet werden. Können jedoch beide zusammen in einem ganzheitlichem Cyber-Security-Awareness-Konzept verwendet werden. Moodle hat eine große Community im Hochschulbereich und wird bereits an vielen Hochschulen verwendet. So kann sich auf Erfahrungswerte der anderen Hochschulen gestützt werden, welches für die Eignung im Hochschulbereich spricht. Jedoch ist zu beachten, dass der Implementierungsaufwand für frei verfügbare Produkte höher ausfällt, als bei kommerziellen Produkten.

Des Weiteren hat sich bei der Untersuchung ein grundlegender Unterschied zwischen den kommerziellen und den frei verfügbaren Produkten gezeigt. komerzielle Produkte inkludieren direkt Lerninhalte, Quizze und Phishing-Templates, wobei frei verfügbare Applikation diese Inhalte nicht mitliefern. Es gibt einige frei verfügbare Produkte, die lediglich Inhalte liefern, wie beispielsweise PagerDuty, jedoch keine geeignete Applikation bereitstellen. Andererseits existieren auch frei verfügbare Applikationen wie Moodle, die zwar eine Plattform bieten, jedoch keine passenden Inhalte enthalten. Die jeweiligen Verantwortlichen müssen also bei frei verfügbaren Produkten noch die Kurse und Inhalte erstellen oder raussuchen, bevor sie mit dem Cyber-Security-Awareness-Training starten können. Dies hat zufolge, dass der Aufwand, welche die jeweilige Hochschule für die implementierung des Programmes hat, höher bei frei verfügbaren Produkten ist, als bei kommerziellen Produkten.

Die Gesamtergebnisse werden in der nachfolgenden Tabelle zusammengefasst (Tabelle 5.5). Sie zeigen einerseits die Gesamtpunktzahl der Bewertung und andererseits werden nochmal die Vor- und Nachteile aufgezeigt, welche für oder gegen eine Hochschuleignung sprechen.

Produktname:	**Gesamtpunkt-zahl**	**Hochschuleignung**	**Kommerziell / Frei verfügbar**
SoSafe	44	+ Fokus auf Kunden im öffentlichen Bereich (Hochschulen) + Gute Erfahrungs-werte für Hochschulen - Hohe Lizenzkosten durch viele Nutzer	Kommerziell
Kmsat (Know-Be4)	44	- Hohe Lizenzkosten durch viele Nutzer	Kommerziell
MoodleLMS & GoPhish	32	+ Bereits bei vielen Hochschulen im Einsatz (Moodle) + Große Hochschul Community (Moodle) + Keine Lizenz-kosten - Hoher Implement-ierungsaufwand	Frei verfügbar

Tabelle 5.5: Produkt Auswertung

6 Fazit und Ausblick

In diesem Kapitel wird zunächst eine Zusammenfassung der bisherigen Arbeit präsentiert, wobei sich die Zusammenfassung ausschließlich auf die behandelten Themen begrenzt. Die verschiedenen Ergebnisse der Untersuchungen werden im letzten Abschnitt im Fazit vorgestellt. Außerdem wird ein Ausblick auf weiterführende Arbeiten gegeben, welche in diesem Themengebiet möglich wären und diese Bachelorarbeit thematisch fortsetzen würden.

6.1 Zusammenfassung

Das Ziel dieser Bachelorarbeit war es, eine Arbeit zu bieten, welche dazu genutzt werden kann, innerhalb des Hochschulbereiches ein Cyber-Security-Awareness-Konzept aufzubauen. Dafür wurden verschiedene Aspekte betrachtet und untersucht, welche wichtig für ein Cyber-Security-Awareness-Konzept sind. Ein Cyber-Security-Awareness-Konzept setzt sich unter anderem aus folgenden Punkten zusammen: den eingesetzten Methoden, um den Nutzern die Inhalte zu präsentieren, die psychologischen Einflussfaktoren, welche beachtet werden müssen, um die Nutzer zu verstehen und somit besser auf sie eingehen zu können, den eingesetzten Messmethoden, welche dazu dienen, das Bewusstsein der NNutzer für Informationssicherheit zu messen, um somit die eigenen Maßnahmen gegebenenfalls anzupassen und aus den eingesetzten Programmen, welche unter anderem für die Cyber-Security-Awareness-Schulungen genutzt werden.

Nachdem in Kapitel zwei (2) die Grundlagen vorgestellt wurden und geklärt wurde, wie ein Cyber-Security-Awareness-Konzept aufgebaut ist, wurden in Kapitel drei (3) zwei Aspekte untersucht, die zwar unabhängig voneinander betrachtet werden müssen, jedoch in der Erstellung eines Cyber-Security-Awareness-Konzeptes beide von gleicher Bedeutung sind und maßgeblich zum Erfolg eines Cyber-Security-Awareness-Konzeptes beitragen.

Der erste Aspekt handelte von den eingesetzten Methoden, welche die Inhalte präsentieren und mit denen die Nutzer agieren, um das Wissen im Informationssicherheitsbereich aufzunehmen. Die untersuchten Methoden sind:

- Traditionelles Lernen (Präsentationen)
- Interaktives Lernen (Workshops / Dialoge)
- Passives Lernen (E-Mail-Erinnerungen / Flyer / Plakate)
- Asynchrones Lernen (E-Learning)
- Spielerisches Lernen (Lernspiele)

Der zweite Aspekt handelte von den psychologischen Einflussfaktoren, welche das Verhalten der Nutzer im Bereich der Cyber-Security beeinflussen. Dabei wurden zwei Gruppen von Einflussfaktoren vorgestellt: einerseits die Einflussfaktoren, welche das Verständnis des Nutzers bezüglich der vom Unternehmen erwarteten Verhaltensweisen beeinflussen und andereseits die Einflussfaktoren, welche auf die persönliche Bereitschaft des Nutzers abzielen, sein Verhalten anzupassen, um sich innerhalb akzeptierter Normen zu bewegen.

Ein weiterer Aspekt eines Cyber-Security-Awareness-Konzeptes, welcher in Kapitel vier (4) untersucht wurde, behandelte die Messmethoden, welche innerhalb einer Hochschule genutzt werden können, um das Bewusstsein für Informationssicherheit der Nutzer zu messen. Zu den Messmethoden gehören Befragungen / Fragebögen, Laborexperimente (Bearbeitung von Aufgaben), Phishing-Simulationen und die Meldung von Sicherheitsvorfällen.

Der vierte und letzte Aspekt dieser Arbeit, in Kapitel fünf (5), war die Evaluation von geeigneten Cyber-Security-Awareness-Applikationen. Es wurden Anforderungen formuliert und daraus Bewertungskriterien abgeleitet, die zur Bewertung und zum Vergleich von E-Learning-Applikationen im Bereich Cyber-Security-Awareness dienten.

6.2 Ausblick

Innerhalb dieser Bachelorarbeit wurden einzelne Aspekte eines Cyber-Security-Awareness-Konzeptes betrachtet und mit Hinblick auf den Einsatz im Hochschulbereich untersucht.

Dies kann weitergeführt werden, indem sich noch spezifischer auf die Hochschulorganisationen konzentriert wird, zum Beispiel könnte eine Betrachtung der einzelnen Personengruppen innerhalb einer Hochschule dabei helfen, ein noch individuelleres Cyber-Security-Awareness-Konzept für den Hochschulbereich aufzustellen.

Die einzelnen Untersuchungen und Abschnitte dieser Arbeit stellen die jeweiligen Aspekte dar, welche in einem Konzept für die Sensibilisierung im Bereich der Informationssicherheit benötigt werden, jedoch wurde hier kein in sich geschlossenes Konzept aufgebaut, dies würde den Umfang dieser Bachelorarbeit überschreiten. Jedoch könnte ein ganzheitliches in sich geschlossenes Cyber-Security-Awareness-Konzept eine sinnvolle Erweiterung zu dieser Arbeit sein.

Diese Bachelorarbeit wurde aus der Perspektive der Informatik verfasst. Es wäre jedoch sicherlich vorteilhaft, die hier untersuchten Aspekte auch ausführlicher aus der Sicht der menschlichen Psychologie zu betrachten, um den menschlichen Faktor noch präziser analysieren zu können.

6.3 Fazit

Die Ergebnisse der Untersuchungen aus Kapitel drei (3) haben gezeigt, dass eine hohe aktive Teilnahme und Interkativität der Nutzer ausschlaggebend für den Lernerfolg ist. Für den spezifischen Einsatz im Hochschulbereich ist der Einsatz der asynchronen Lernmethode mittels des E-Learnings in Kombination mit dem spielerischen Lernen zu empfehlen. Durch die unterschiedlichen Formate, welche die verschiedenen Lerntypen unterstützen, durch geringe zeitliche Kollisionen, aufgrund des asynchronen Ansatzes und der hohen Skalierbarkeit, sind dies gute Methoden für ein Cyber-Security-Awareness-Konzept innerhalb einer Hochschule.

Darüber hinaus ist ein positives Verhalten von Kollegen (Kommilitonen, Arbeitskollegen etc.) und Führungskräften von großer Bedeutung. Aufgrund der regelmäßig beginnenden Semester an Hochschulen gibt es stets zahlreiche neue Nutzer, die sich häufig an Studierenden höherer Semester oder an Professoren orientieren. Daher ist es besonders wichtig, dass die Nutzer ein positives Verhalten im Hinblick auf das Cyber-Security-Awareness-Konzept zeigen, um den neuen Nutzern eine korrekte Orientierung zu bieten. Des Weiteren sollten die Cyber-Security-Awarness-Maßnahmen für die Nutzer verständlich sein

und ihr Wissen gestärkt werden, sodass sie in der Lage sind, sichere Entscheidungen im Hinblick auf die Informationssicherheit zu treffen.

In Kapitel vier (4) wurde festgestellt, dass Fragebögen in Form von Tests oder Quizzen sowie Phishing-Simulationen optimal zur Messung der Cyber-Security-Awareness der Nutzer eingesetzt werden können. Ein hybrider Ansatz dieser beiden Methoden ist zu empfehlen. Dies ermöglicht es, mithilfe der Fragebögen das Wissen der Nutzer abzufragen und mithilfe der Phishing-Simulationen das tatsächsliche Verhalten zu messen. Außerdem senkt die Implementierung dieser Methoden mittels einer technischen Lösung den organisatorischen- und den Arbeitsaufwand während des Betriebes enorm innerhalb einer Hochschule. Des Weiteren sollten Meldewege und Prozesse definiert werden, welche es den Nutzern ermöglichen, Sicherheitsvorfälle zu melden. Die Überwachung und Auswertung dieser Meldungen ist entscheidend, um festzustellen, ob die Nutzer die Bedeutung von Cyber-Security verstanden haben und das Gelernte anwenden. Darüber hinaus werden Einblicke in die aktuelle Bedrohungslage geboten und es wird aufgezeigt, ob die eigenen definierten Prozesse und Meldewege optimal implementiert sind.

Für die Implementierung der E-Learning-Methode und der Messmethoden (Tests und Phishing-Simulationen) im Cyber-Security-Awareness Bereich wurde in Kapitel fünf (5) neben der Bewertung und dem Vergleich von spezifischen Produkten auch aufgezeigt, dass ein grundlegender Unterschied zwischen den kommerziellen und den frei verfügbaren Produkten vorhanden ist und, dass sich die Implementierung eines Cyber-Security-Awareness-Konzeptes deutlich aufwändiger mittels eines frei verfügbaren Produktes gestaltet, jedoch entfallen hierbei die Produktkosten. Es wurde gezeigt, dass im kommerziellem Bereich das E-Learning-Produkt von SoSafe eine ideale Option für Hochschulen ist. Für Produkte, welche frei verfügbar sind, wurde gezeigt, dass MoodleLMS zusammen mit GoPhish eine gute Wahl ist, welche im Hochschulbereich eingesetzt werden kann, um Cyber-Security-Awareness-Schulungen und Phishing-Simulationen durchzuführen. Sowohl die frei verfügbare als auch die kommerzielle Option werden bereits von verschiedenen Hochschulen in Deutschland genutzt und haben somit eine große Community im Hochschulbereich, so dass sich auf Erfahrungswerte bei der Implementierung und dem Betrieb gestützt werden kann.
Sollte die Hochschule über ausreichende finanzielle Mittel verfügen, empfiehlt sich die Wahl eines kommerziellen Produkts wie SoSafe. Aus technischer Sicht, sowohl hinsichtlich des Aufwands als auch der Produktmerkmale, ist dies die vorteilhaftere Option. Sollte die Hochschule nicht über die erforderlichen finanziellen Mittel verfügen, könnte die Beantragung entsprechender Fördermittel eine mögliche Option darstellen. Wenn

beides keine Option ist, ist die Wahl eines frei verfügbaren Produktes durchaus legitim. Hier ist jedoch zu beachten, dass die Implementierung aufwendiger ist und daher mehr Zeit in Anspruch nimmt.

Die Ergebnisse der jeweiligen Untersuchungen sollen den Lesern als Grundlage dienen, um ein Cyber-Security-Awareness-Konzept mit den geeigneten Tools für den eigenen Hochschulbereich entwickeln zu können.

Literaturverzeichnis

[1] Abawajy, Jemal: User preference of cyber security awareness delivery methods. In: *Behaviour and Information Technology* 33 (2012), 3, S. 237–248. – ISSN 13623001

[2] Alahmari, Saad: *A Model for Describing and Encouraging Cyber Security Knowledge Sharing to Enhance Awareness*, University of Glasgow, Dissertation, 2021

[3] APWG: Number of unique phishing sites detected worldwide from 3rd quarter 2013 to 34th quarter 2022 / Anit-Phishing Working Group. 2023. – Forschungsbericht

[4] APWG: Phishing Activity Trends Report / Anti-Phishing Working Group. November 2023 (2nd Quarter 2023). – Forschungsbericht

[5] Bada, Maria ; Sasse, Angela ; Nurse, Jason: Cyber Security Awareness Campaigns: Why do they fail to change behaviour? (2015), 01, S. 118–131

[6] Bauer, Stefan ; Bernroider, Edward W. ; Chudzikowski, Katharina: Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. In: *Computers & Security* 68 (2017), S. 145–159. – URL https://www.sciencedirect.com/science/article/pii/S0167404817300871. – ISSN 0167-4048

[7] Budge, Jinan: The Forrester Wave™: Security Awareness And Training Solutions, Q1 2022 / Forrester Wave. 2022. – Forschungsbericht

[8] Chaudhary, Sunil ; Gkioulos, Vasileios ; Katsikas, Sokratis: Developing metrics to assess the effectiveness of cybersecurity awareness program. In: *Journal of Cybersecurity* 8 (2022), 05, S. 1–19

[9] Chaudhary, Sunil ; Kompara, Marko ; Pape, Sebastian ; Gkioulos, Vasileios: Properties for Cybersecurity Awareness Posters' Design and Quality Assessment, Association for Computing Machinery, 8 2022. – ISBN 9781450396707

[10] Chen, Charlie ; Shaw, Ruey-Shiang ; Yang, s: Mitigating Information Security Risks by Increasing User Security Awareness: A Case Study of an Information Security Awareness System. In: *IT, Learning, and Performance Journal* 24 (2006), 01

[11] Davila, J.: *ZibaSec Awareness Training.* – https://learn.zibasec.com, [Letzter Zugriff: 10.04.2024]

[12] Dr. Lutz, Gollan: *BITS-Portal.* – https://www.bits-portal.eu, [Letzter Zugriff: 09.04.2024]

[13] ENISA: *ENISA threat landscape report 2018 – 15 top cyber-threats and trends.* European Network and Information Security Agency, 2019

[14] ENISA: Threat Landscape Report 2023 / European Union Agency for Cybersecurity. Oktober 2023. – Forschungsbericht. – ISBN 978-92-9204-645-3

[15] Ganchev, Ivan ; O'Droma, Mairtin ; Andreev, Radoslav: Functionality and SCORM-compliancy Evaluation of eLearning Tools. In: *Seventh IEEE International Conference on Advanced Learning Technologies (ICALT 2007)*, 2007, S. 467–469

[16] GoPhish: *GoPhish Campaigns.* – https://docs.getgophish.com/user-guide/documentation/campaigns/ [Accessed: 25.05.2024]

[17] GoPhish: *GoPhish Generating Reports.* – https://docs.getgophish.com/user-guide/documentation/generating-reports, [Letzter Zugriff: 23.05.2024]

[18] GoPhish: *GoPhish Groups.* – https://getgophish.com/documentation/0, [Letzter Zugriff: 23.05.2024]

[19] GoPhish: *Open-Source Phishing Framework.* – https://getgophish.com/#, [Letzter Zugriff: 11.04.2024]

[20] Haan, Katherine: *Best Learning Management Systems (LMS) Of 2024.* 2024. – https://www.forbes.com/advisor/business/best-learning-management-systems/, [Letzter Zugriff: 10.04.2024]

[21] Hochschulen e.V., Moodle an: *Moodle an Hochschulen.* – https://moodle-an-hochschulen.de, [Letzter Zugriff: 09.05.2024]

[22] Informationstechnik, Bundesamt für Sicherheit in der: *Awareness*. – https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Faktor-Mensch/Awareness/awareness_node.html, [Letzter Zugriff: 13.06.2024]

[23] Jimoh, Abdulwasiu: Social Engineering Attacks. (2022), 02. – URL https://www.researchgate.net/publication/358647625_Social_Engineering_Attacks

[24] Khando, Khando ; Gao, Shang ; Islam, Sirajul M. ; Salman, Ali: Enhancing employees information security awareness in private and public organisations: A systematic literature review. In: *Computers & Security* 106 (2021), S. 102–267. – URL https://www.sciencedirect.com/science/article/pii/S0167404821000912. – ISSN 0167-4048

[25] KnowBe4: *Administratorsupport*. – https://support.knowbe4.com/hc/de/sections/4406914335763-Administratorsupport, [Letzter Zugriff: 03.05.2024]

[26] KnowBe4: *Datenschutzerklaerung fuer die KnowBe4 Produkte*. – https://www.knowbe4.de/datenschutzerklaerung, [Letzter Zugriff: 03.05.2024]

[27] KnowBe4: *Durchführen von Phishing-Kampagnen*. – https://support.knowbe4.com/hc/de/sections/4406909537299-Durchführen-von-Phishing-Kampagnen, [Letzter Zugriff: 03.05.2024]

[28] KnowBe4: *Erstellen und verwalten von Trainingskampagnen*. – https://support.knowbe4.com/hc/de/articles/204948207-Erstellen-und-Verwalten-von-Trainingskampagnen, [Letzter Zugriff: 03.05.2024]

[29] KnowBe4: *Leitfaden zu Modstore und Bibliothek*. – https://support.knowbe4.com/hc/de/articles/115001221467-Leitfaden-zu-ModStore-und-Bibliothek, [Letzter Zugriff: 03.05.2024]

[30] KnowBe4: *Security Awareness Training & Simulated Phishing Platform*. – https://www.knowbe4.de, [Letzter Zugriff: 15.04.2024]

[31] KnowBe4: *Verwalten von Nutzer:innen und Gruppen*. – https://support.knowbe4.com/hc/de/sections/360000154687-Verwalten-von-Nutzer-innen-und-Gruppen, [Letzter Zugriff: 03.05.2024]

[32] KnowBe4: *Verwenden von Reports.* – https://support.knowbe4.com/hc/de/sections/360000156668-Verwenden-von-Reports, [Letzter Zugriff: 03.05.2024]

[33] KnowBe4: *KnowBe4 KMSAT Datasheet.* 2024

[34] KnowBe4: *KnowBe4 Subscription Levels.* 2024

[35] Kondruss, Bert: *Cyber Angriffe auf Universitäten.* – https://konbriefing.com/de-topics/cyber-angriffe-universitaeten.html/ [Accessed: 20.06.2024]

[36] Leach, John: Improving user security behaviour. In: *Computers and Security* 22 (2003), S. 685–692. – ISSN 01674048

[37] Moodle: *About Moodle.* – https://docs.moodle.org/404/en/About_Moodle, [Letzter Zugriff: 22.05.2024]

[38] Moodle: *The best LMS for personalised learning.* – https://moodle.com/solutions/lms/, [Letzter Zugriff: 11.04.2024]

[39] Moodle: *Moodle Bewertungen Exportieren.* – https://docs.moodle.org/404/de/Bewertungen_exportieren, [Letzter Zugriff: 09.05.2024]

[40] Moodle: *Moodle Courses.* – https://docs.moodle.org/404/en/Courses, [Letzter Zugriff: 09.05.2024]

[41] Moodle: *Moodle Documentation.* – https://docs.moodle.org/401/de/Hauptseite, [Letzter Zugriff: 23.05.2024]

[42] Moodle: *Moodle DSGVO.* – https://docs.moodle.org/404/de/DSGVO, [Letzter Zugriff: 09.05.2024]

[43] Moodle: *Moodle Kursberichte.* – https://docs.moodle.org/401/de/Kursberichte, [Letzter Zugriff: 09.05.2024]

[44] Moodle: *Moodle LDAP Server.* – https://docs.moodle.org/404/de/LDAP-Server, [Letzter Zugriff: 09.05.2024]

[45] Moodle: *Moodle Nutzerkonten Verwalten.* – https://docs.moodle.org/404/de/Nutzerkonten_verwalten, [Letzter Zugriff: 09.05.2024]

[46] Pagerduty: *Pagerduty Security Training.* – https://sudo.pagerduty.com, [Letzter Zugriff: 10.04.2024]

[47] Saint-Germain, Rene: Information Security Management Best Practice Based on ISO/IEC 17799. In: *Information Management Journal* 39(4) (2005), 01

[48] Scholl, Margit ; Leiner, Benjamin ; Fuhrmann, Frauke: Blind spot: Do you know the effectiveness of your information security awareness-raising program?, 07 2017

[49] Schütz, Andreas E. ; Fertig, Tobias ; Weber, Kristin ; Müller, Nicholas H.: How E-Learning Can Facilitate Information Security Awareness. In: *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 11590 LNCS (2019), S. 390–401. – ISBN 9783030218133

[50] Shetty, Dinesh: Social Engineering - The Human Factor. (2017). – URL https://www.exploit-db.com/docs/english/18135-social-engineering---the-human-factor.pdf

[51] Siponen, Mikko: Five dimensions of information security awareness. In: *Computers and Society* 31 (2001), 01

[52] SoSafe: *Datenschutz.* – https://sosafe-awareness.com/de/datenschutz/, [Letzter Zugriff: 03.05.2024]

[53] SoSafe: *Dokumentation & Support.* – https://de.support.sosafe.de/?l=de, [Letzter Zugriff: 03.05.2024]

[54] SoSafe: *Drive secure behavior at scale.* – https://sosafe-awareness.com, [Letzter Zugriff: 15.04.2024]

[55] SoSafe: *Nutzerverwaltung: Allgemeine Information.* – https://de.support.sosafe.de/adok/nutzerverwaltung-allgemeine-informationen, [Letzter Zugriff: 03.05.2024]

[56] SoSafe: *Phishing Simulation.* – https://de.support.sosafe.de/adok/phishing-simulation, [Letzter Zugriff: 03.05.2024]

[57] SoSafe: *Feature Matrix version 2.3.* 2024

[58] SoSafe: *Inhalts und Sprachen übersicht.* 2024

[59] Sykosch, Arnold: *Zur Messbarkeit von IT-Sicherheitsbewusstsein*, Universität Bonn, Dissertation, 2022

A Anhang

A.1 Elektronischer Anhang

Am Ende dieser Arbeit befindet sich eine CD mit dem elektronischen Anhang.

Auf dieser CD befindet sich:

- Thesis als PDF-Dokument "Thesis.pdf"

A.2 Tool Bewertung

Die Bewertung der Produkte aus Kapitel fünf (5) wird nachfolgend in Tabellarischer Form ausführlich (erhaltene Punktzahl pro Unterkategorie) präsentiert.

A.2.1 Bewertung von MoodleLMS & GoPhish

MoodleLMS & GoPhish	
Kriterium	**Erhaltene Punkte**
A1 Schulungskampagnen	
A1.1 Kampagnen erstellen	3
A2 Training & Inhalt	
A2.1 Lerninhalte sind inkludiert	1
A2.2 Mulitlinguale Einstellungen der Lerninhalte möglich	0
A2.3 Quizze / Tests sind inkludiert	1
A2.4 Berichterstattung zum E-Learning ist inkludiert	2
A2.5 Exportierung der E-Learning Berichtersttung ist möglich	1
A2.6Lerninhalte sind Anpassbar	3
A3 Phishing	
A3.1 Phishing-Simulationen durchführbar	2
A3.1 Phishing-Berichterstattung ist inklduiert	3
A3.1 Exportierung der Phishing-Berichterstattung ist möglich	2
A4 Nutzuerverwaltung	
A4.1 Nutzerimport ist über verschiedene Methoden möglich	3
A4.2 Nutzer Gruppierung ist möglich	2
A5 Nutzerfreundlichkeit	
A5.1 Einfache Dokumentation	3
A5.2 Intuitive Nutzung	2
A6 Datenverarbeitung	
A6.1 Frei verfügbar	2
A6.2 DSGVO Konform	2
Gesamtpunktzahl:	
32	
Hochschuleignung: Vor- (+) & Nachteile (-)	
- Hoher Implementierungsaufwand	
+ Kostenfrei	
+ Große Community im Hochschulbereich	
+ Bereits hohe Implementierungsrate im Hochschulbereich	

Tabelle A.1: Bewertung von MoodleLMS & GoPhish (inkl. Unterkategorien)

A.2.2 Bewertung von KnowBe4: KMSAT

KnowBe4: KMSAT	
Kriterium	**Erhaltene Punkte**
A1 Schulungskampagnen	
A1.1 Kampagnen erstellen	3
A2 Training & Inhalt	
A2.1 Lerninhalte sind inkludiert	3
A2.2 Mulitlinguale Einstellungen der Lerninhalte möglich	3
A2.3 Quizze / Tests sind inkludiert	3
A2.4 Berichterstattung zum E-Learning ist inkludiert	3
A2.5 Exportierung der E-Learning Berichtersttung ist möglich	3
A2.6 Lerninhalte sind Anpassbar	3
A3 Phishing	
A3.1 Phishing-Simulationen durchführbar	3
A3.1 Phishing-Berichterstattung ist inklduiert	3
A3.1 Exportierung der Phishing-Berichterstattung ist möglich	3
A4 Nutzuerverwaltung	
A4.1 Nutzerimport ist über verschiedene Methoden möglich	3
A4.2 Nutzer Gruppierung ist möglich	3
A5 Nutzerfreundlichkeit	
A5.1 Einfache Dokumentation	3
A5.2 Intuitive Nutzung	2
A6 Datenverarbeitung	
A6.1 Frei verfügbar	1
A6.2 DSGVO Konform	2
Gesamtpunktzahl:	
44	
Hochschuleignung: Vor- (+) & Nachteile (-)	
- Kostenpflichtig	
Keine Hochschulspezfischen Vorteile gegeben	

Tabelle A.2: Bewertung von KnowBe4: KMSAT (inkl. Unterkategorien)

A.2.3 Bewertung von SoSafe

SoSafe	
Kriterium	**Erhaltene Punkte**
A1 Schulungskampagnen	
A1.1 Kampagnen erstellen	3
A2 Training & Inhalt	
A2.1 Lerninhalte sind inkludiert	3
A2.2 Mulitlinguale Einstellungen der Lerninhalte möglich	3
A2.3 Quizze / Tests sind inkludiert	3
A2.4 Berichterstattung zum E-Learning ist inkludiert	3
A2.5 Exportierung der E-Learning Berichtersttung ist möglich	3
A2.6 Lerninhalte sind Anpassbar	3
A3 Phishing	
A3.1 Phishing-Simulationen durchführbar	3
A3.1 Phishing-Berichterstattung ist inklduiert	3
A3.1 Exportierung der Phishing-Berichterstattung ist möglich	3
A4 Nutzuerverwaltung	
A4.1 Nutzerimport ist über verschiedene Methoden möglich	3
A4.2 Nutzer Gruppierung ist möglich	3
A5 Nutzerfreundlichkeit	
A5.1 Einfache Dokumentation	2
A5.2 Intuitive Nutzung	3
A6 Datenverarbeitung	
A6.1 Frei verfügbar	1
A6.2 DSGVO Konform	2
Gesamtpunktzahl:	
44	
Hochschuleignung: Vor- (+) & Nachteile (-)	
- Kostenpflichtig	
+ Hersteller ist unter anderem auf Hochschulen spezialisiert	
+ SoSafe besitzt Erfahrung bei der Implementierung im Hochschulbereich	

Tabelle A.3: Bewertung von SoSafe (inkl. Unterkategorien)

Erklärung zur selbständigen Bearbeitung

Hiermit versichere ich, dass ich die vorliegende Arbeit ohne fremde Hilfe selbständig verfasst und nur die angegebenen Hilfsmittel benutzt habe. Wörtlich oder dem Sinn nach aus anderen Werken entnommene Stellen sind unter Angabe der Quellen kenntlich gemacht.

Hamburg	02.04.2024	[redacted]
Ort	Datum	Unterschrift im Original