HOCHSCHULE
MITTWEIDA
University of Applied Sciences

Fakultät Angewandte Computer- und Biowissenschaften

Professur Digitale Transformation und Angewandte Medieninformatik

Bachelorarbeit

Konzeption und Implementierung eines E-Learning Kurses zum Erwerb digitaler Kompetenzen im Bereich der IT-Sicherheit

Nikolas Weber

Mittweida, den 7. Oktober 2022

Erstprüfer: Prof. Dr.-Ing. Christian Roschke
Zweitprüfer: B.Sc. Susan Labude

Weber, Nikolas
Konzeption und Implementierung eines E-Learning Kurses zum Erwerb digitaler Kompetenzen im Bereich der IT-Sicherheit
Bachelorarbeit, Fakultät Angewandte Computer- und Biowissenschaften
Hochschule Mittweida — University of Applied Sciences, Oktober 2022

Referat

In dieser Bachelorarbeit wird ein E-Learning Kurs zum Kompetenzerwerb auf dem Gebiet der IT-Sicherheit konzipiert, implementiert und evaluiert. Dazu werden zunächst für Endnutzende relevante Themen der IT-Sicherheit identifiziert und die theoretischen Fundierungen für die Umsetzung als ein Web-based Training gelegt. Die Umsetzung des Konzeptes in einen Moodle-Kurs wird beschrieben. Es wird eine Evaluation der Usability des Kurses und des Lernerfolges durchgeführt.

Name: Weber, Nikolas
Studiengang: Bachelor Medieninformatik und interaktives Entertainment
Seminargruppe: MI19w3-B
English Title: Conception and Implementation of an E-Learning module to acquire digital competencies in the field of it-security

Inhaltsverzeichnis

Abbildungsverzeichnis **V**

Tabellenverzeichnis **VII**

1 Einführung und Motivation **1**

1.1 Zielstellung 2
1.2 Aufbau der Arbeit 2

2 Grundlagen **3**

2.1 IT-Sicherheit 3
2.1.1 Notwendigkeit der IT-Sicherheit 4
2.1.2 Angriffsmethoden 7
2.1.3 Faktor Mensch in der IT-Sicherheit 13
2.1.4 Gegenmaßnahmen 15
2.2 E-Learning 18
2.2.1 Kompetenzen 19
2.2.2 Formate 21
2.2.3 Psychologische Aspekte 23
2.2.4 Multimedialität 26
2.2.5 Evaluationsmodelle für E-Learning 27

3 Analyse und Konzeption **31**

3.1 Anforderungsanalyse 32
3.1.1 Funktionale Anforderungen 32
3.1.2 Nicht-Funktionale Anforderungen 33
3.2 Struktur des Moduls 34

3.2.1 Einleitung . . . 34
3.2.2 Passwörter . . . 35
3.2.3 Phishing . . . 35
3.2.4 Verschlüsselung . . . 36
3.2.5 Malware . . . 38
3.2.6 Abschlusstest . . . 39
3.3 Konzeption der Inhalte . . . 39
3.3.1 Einleitung . . . 40
3.3.2 Passwörter . . . 44
3.3.3 Phishing . . . 45
3.3.4 Verschlüsselung . . . 46
3.3.5 Malware . . . 48
3.4 Technische Konzeption . . . 50
3.4.1 Aufruf der Lerninhalte . . . 50
3.4.2 Navigation . . . 53
3.4.3 Hyperlinks . . . 53

4 Implementierung **55**
4.1 Implementierung der Inhalte . . . 55
4.1.1 Videos . . . 55
4.1.2 Text . . . 58
4.1.3 Tests . . . 59
4.2 Technische Implementierung . . . 60
4.2.1 Aufruf der Lerninhalte . . . 60
4.2.2 Navigation . . . 61
4.2.3 Hyperlinks . . . 61
4.2.4 Tests . . . 61
4.2.5 Passwörter Experiment . . . 62

5 Evaluation **65**
5.1 Lernerfolg . . . 65
5.1.1 Konzept . . . 66
5.1.2 Vorbereitung . . . 68

5.1.3 Durchführung 68
5.1.4 Ergebnisse 69
5.2 Usability 71
5.2.1 Konzept 71
5.2.2 Vorbereitung 72
5.2.3 Durchführung 74
5.2.4 Ergebnisse 74
5.3 Teilnehmende 75
5.3.1 Rekrutierung 75
5.3.2 Demografie 76

6 Zusammenfassung und Ausblick **77**

Literaturverzeichnis **I**

A System Usability Scale Scores **A1**

B Konzepte von Zwischentests **A3**

B.1 Passwörter A3
B.2 Phishing A5
B.3 Verschlüsselung A7
B.4 Malware A8

C Vortest **A11**

D Abschlusstest **A17**

Abbildungsverzeichnis

2.1 Lösegeldforderung der WannaCry-Ransomware auf einer Anzeige der Deutschen Bahn. 6
2.2 Inhalt einer Phishing-Mail, bei welcher versucht wird Nutzende auf eine gefälschte Website zu führen. 8
2.3 Sperrbildschirm des sog. Bundespolizei Virus. 11
2.4 Schematischer Ablauf eines Drive-by-Downloads. 12
2.5 Schematische Übersicht über das PDPP Evaluation Model. 28
2.6 Die fünf Ebenen der Evaluation von Trainings nach dem Kirkpatrick/Phillips-Modell. 29

3.1 Einteilung in einzelne Abschnitte. 51
3.2 Video, welches durch das Datei-Element eingebettet wurde. 52
3.3 Video, welches durch das ”Interaktiver Inhalt”-Element eingebettet wurde. 52
3.4 Navigation durch das Modul. Durch einen Klick auf die blau markierten Links können sich Lernende zu höhren Ebenen bewegen. 53

4.1 Schematische Abbildung eines Loginvorganges mittels Passwort. . . . 57
4.2 Lenkung der Aufmerksamkeit durch Farbe und eine geschweifte Klammer. 58
4.3 Eine beantwortete Frage mit Feedback in einem Zwischentest. 59
4.4 Die Eingabemaske zum Erraten des dritten Passwortes mit einer falschen Eingabe. 63

5.1 Antworten von Proband 3 bei Frage 9 im Abschlusstest 70
5.2 Einstellung der Voraussetzungen für den Zugriff auf den Link zur Usability-Umfrage. 73

Tabellenverzeichnis

3.1 Funktionale Anforderungen 32
3.2 Nicht-Funktionale Anforderungen 33
3.3 Struktur des Kapitels ”Einleitung” 35
3.4 Struktur des Kapitels ”Passwörter” 36
3.5 Struktur des Kapitels ”Phishing” 37
3.6 Struktur des Kapitels ”Verschlüsselung” 37
3.7 Struktur des Kapitels ”Malware” 38

5.1 Erreichte Punkte der Probanden in den Tests 70
5.2 Berechnete SUS-Scores der einzelnen Probanden und im Mittel 75

A.1 Scores der einzelnen Fragen von Proband 1 . . . . . A1
A.2 Scores der einzelnen Fragen von Proband 2 . . . . . A2
A.3 Scores der einzelnen Fragen von Proband 3 . . . . . A2

1. Einführung und Motivation

Die Anzahl an Bedrohungen aus dem digitalen Raum nimmt seit Jahren zu. Ransomwares, welche Krankenhäuser und Lieferketten lahmlegen, Diebstahl von vertraulichen Daten oder auch Phishing-Angriffe, durch welche Endnutzenden monetäre Schäden entstehen. Die Liste von möglichen Angriffen ist lang, genauso jedoch auch die Liste der Gegenmaßnahmen, welche zur Vermeidung von Schäden durch solche digitalen Angriffe getroffen werden. Diese Gegenmaßnahmen haben viele Dinge gemein: Sie sind komplex, technisch aufwendig und vernachlässigen oft die eigentlichen Anwendenden der zu schützenden Systeme.

Dadurch werden jedoch Bestrebungen zum Schutz von IT-Systemen unterminiert. Endanwendende empfinden Sicherheitsmaßnahmen als lästig und unkomfortabel. So wird versucht diese zu umgehen, da das Wissen über den Sinn und Zweck dieser Maßnahmen fehlt. Zusätzlich fehlt den Endanwendenden das Wissen, um selbstständig Bedrohungen zu erkennen und geeignete Gegenmaßnahmen zu ergreifen. So werden Angriffe meist erst erkannt, wenn es bereits zu spät ist.

Um die Sicherheitslücke "Mensch" zu schließen, sollten Endanwendende entsprechend in der IT-Sicherheit geschult werden. So soll einerseits Akzeptanz der Sicherheitsmaßnahmen durch Verständnis dieser erreicht werden, andererseits sollen Anwendende in die Lage versetzt werden, selbstständig Sicherheitsverstöße und Angriffe erkennen zu können, sodass rechtzeitig Gegenmaßnahmen ergriffen werden können.

Durch die Corona-Pandemie hat E-Learning in Bildung und betrieblicher Weiterbildung einen hohen Stellenwert erreicht. Auch in der Weiterbildung im Bereich der IT-Sicherheit ist E-Learning vorteilhaft. So können Arbeitnehmende entsprechende Weiterbildungen im HomeOffice durchführen und haben, im Gegensatz zu klassischen Präsenzschulungen, die Möglichkeit bei Auftreten von Sicherheitsvorfällen die Lektionen erneut zu sichten, um die richtigen Maßnahmen zu ergreifen.

1.1. Zielstellung

Noch wirkungsvoller als zu wissen, wo im Problemfall die Lösung nachgelesen werden kann, ist Kompetenz im Bereich der IT-Sicherheit zu besitzen. Da Endanwendende so selbstständig Prävention gegen IT-Angriffe betreiben und schnell sowie korrekt auf solche Angriffe reagieren können. Da der Erwerb solcher Kompetenzen immer noch keinen festen Platz in der schulischen Bildung hat, müssen sich Endnutzende selbstständig diesen Kompetenzerwerb betreiben.

In dieser Bachelorarbeit soll deshalb ein E-Learning-Kurs konzipiert und erstellt werden, welcher Endnutzenden die notwendigen Kompetenzen vermittelt. Dieser soll sich an Endanwendende richten, welche wenige bis keine Kompetenzen im Umgang mit digitalen Systemen haben. Es sollen digitale Kompetenzen im Bereich der IT-Sicherheit sowohl für die private Verwendung, als auch für den Unternehmenskontext aufgebaut werden.

1.2. Aufbau der Arbeit

Um dieses Ziel zu erreichen, werden zunächst in Kapitel 2 die notwendigen Grundlagen aufbereitet. Dazu werden Grundlagen der IT-Sicherheit, also die Inhalte des Moduls, und des E-Learnings, also der Umsetzung des Moduls, beschrieben. Danach folgt Kapitel 3. In diesem wird eine Anforderungsanalyse durchgeführt und auf der Basis der Anforderungen und der Grundlagen ein Konzept für den Kurs erstellt. Das folgende Kapitel 4 beschreibt die Umsetzung der Konzepte. Dabei wird auf die Umsetzung der Inhalte, also die entsprechende Medienproduktion, und die technische Implementierung, also das Einbinden der Inhalte und die Umsetzung von benötigten Funktionen, eingegangen. Darauf folgt die Evaluation in Kapitel 5. Dort wird die Usability und der Lernerfolg des Moduls bewertet. Daneben wird die Demografie der Teilnehmenden aufgezeigt. Die Ergebnisse werden diskutiert und eingeordnet. Kapitel 6 gibt eine kurze Zusammenfassung und stellt mögliche Weiterführungen dar.

2. Grundlagen

Im Folgenden sollen die Grundlagen, welche für die Entwicklung eines E-Learning Moduls zum Thema IT-Sicherheit erforderlich sind, vorgestellt werden. Zunächst werden die Grundlagen der IT-Sicherheit vorgestellt, diese sind für den Inhalt des Moduls relevant. Anschließend folgt die Vorstellung der Grundlagen des E-Learnings. Es werden jeweils Begriffsdefinitionen durchgeführt und folgend weitere Aspekte erklärt.

2.1. IT-Sicherheit

Unter der IT-Sicherheit versteht man "[...] Gewährleistung von Sicherheit aller eingesetzten Informationstechniken bzw. -technologien (IT), d.h. aller Hardware- und Softwaresysteme bzw. aller Rechner- und Netzsysteme."[Gab20]. Die Aufgabe der IT-Sicherheit besteht also allgemein darin, digitale Systeme vor Schaden und Manipulation durch unbefugte Dritte zu schützen, sowie den Zugriff auf digitale Informationen durch Unbefugte zu unterbinden. Der IT-Sicherheit übergeordnet ist die **Informationssicherheit**. Sie befasst sich allgemein mit dem Schutz von Informationen, egal ob diese analog oder digital vorliegen. Oft wird auch der Begriff **Cybersecurity** verwendet. Dieser hat meist einen Bezug zu Sicherheitsmechanismen im Zusammenhang mit dem Internet. Hierbei ist zu beachten, dass keiner dieser Begriffe genormt ist [Hel18, S. 2] und die Begriffe auch anders definiert werden können. Die Sicherheit ist gewährleistet, wenn die fünf Schutzziele erreicht sind. Diese sind Authentizität, Integrität, Vertraulichkeit, Verfügbarkeit und Verbindlichkeit.

Unter **Authentizität** wird die Echtheit von Objekten oder Subjekten, also Nutzenden, verstanden, welche überprüfbar ist. Das Schutzziel **Integrität** ist erfüllt, wenn Daten nicht unautorisiert und unbemerkt manipuliert werden können. Bei der **Vertraulichkeit** geht es um das Verhindern von unautorisierter Informationsgewinnung, also dem Auslesen von Daten durch Unbefugte. Die **Verfügbarkeit** sagt aus, dass

die von den Systemen angebotene Dienste von berechtigen Nutzenden in Anspruch genommen werden können und diese dabei nicht durch Unbefugte beeinträchtigt werden. **Verbindlichkeit** bedeutet die Fähigkeit eines Systems Aktionen zu Nutzenden zuordnen zu können, wobei diese die durchgeführten Aktionen hinterher nicht abstreiten können [Eck18, S. 8-12].

Im Folgenden soll anhand von Beispielen für die Verletzung dieser Schutzziele die Notwendigkeit der IT-Sicherheit erläutert werden. Aus diesen werden einige Angriffstechniken abgeleitet und näher erläutert. Anschließend wird auf die Wirkung des Faktors Mensch auf die Sicherheit in IT-Systemen eingegangen. Danach werden mögliche Gegenmaßnahmen vorgestellt.

2.1.1. Notwendigkeit der IT-Sicherheit

Nun soll die Notwendigkeit der IT-Sicherheit erläutert werden. Nach einer Befragung des Branchenverbandes der deutschen Informations- und Telekommunikationsbranche, der Bitkom, haben 86 % der deutschen Unternehmen im Jahr 2021 Schäden durch Cyberangriffe erlitten. Dies entspricht einer Steigerung von 16 % im Vergleich zum Vorjahr [BS21, S. 6]. Der so entstandene Schaden wurde für 2021 auf 223,5 mrd. € bemessen [BS21, S. 10]. Der größte Teil der Schäden wurde demnach durch den Ausfall oder die Störung von Systemen verursacht, also durch Verletzung der Verfügbarkeit, wodurch Produktions- und Betriebsabläufe beeinträchtigt wurden. Dieser Schaden wurde auf 61,9 mrd. € beziffert [ebd.]. Nach dem Lagebericht des Bundesamtes für Sicherheit in der Informationstechnik (BSI) wurde die IT-Sicherheitslage in Deutschland im letzten Berichtszeitraum als ”angespannt bis kritisch” bewertet [BSI21, S. 9]. Neben dem Anstieg der Anzahl bekannter Malware-Varianten wurde in diesem Zeitraum auch ein Anstieg an Erpressung bzw. Angriffen mit folgender Erpressung beobachtet [ebd.]. Neben Unternehmen sind auch Endverbrauchende Ziele von IT-Angriffen. So gaben laut des Lageberichts 24 % aller Befragten an im Jahr 2021 Opfer von Internetkriminalität geworden sein [BSI21, S. 47]. Dabei gab es bei 31 % unberechtigte Zugriffe auf Accounts verschiedener Dienste und 29 % gaben an, dass ihr System mit Malware infiziert wurde [ebd.]. Im Folgenden sollen nun exemplarisch einige vergangene IT-Angriffe aufgezeigt werden.

Angriff auf Europäische Arzneimittelagentur

Am 09.12.2020 kam es zu einem Angriff auf die Europäische Arzneimittelagentur (EMA), welche unter anderem für die Zulassung von Medikamenten in Europa zuständig ist. Dabei kam es zu einer Verletzung der Subjekt-Authentizität und der Vertraulichkeit. Eine Person konnte sich Zugang zu einem Rechner mit Zugang zu Daten der EMA verschaffen und die dort implementierte Zwei-Faktor-Authentisierung umgehen, da beide Faktoren auf dem Rechner gespeichert waren. So war ein unberechtigter Zugriff auf ein Nutzerkonto möglich. Es wurden dann Daten zu einem Zulassungsantrag für einen COVID-19-Impfstoff der Firma BioNTech und Pfizer gestohlen. Die gestohlenen Daten wurden später in veränderter Form veröffentlicht, womöglich um Zweifel an dem Impfstoff zu erzeugen [BSI21, S. 41].

WannaCry Ransomware

Am 12.05.2017 wurden über 300.000 Systeme in über 150 Ländern mit der WannaCry Ransomware infiziert. Diese Malware nutzte eine Sicherheitslücke in verschiedenen Windows-Betriebssystemen zur Infektion und Verbreitung. Nach dem Ausführen wurden neue ausführbare Dateien erstellt, welche der Ransomware eine Persistenz ermöglichen. Dabei werden auch Back-ups gelöscht. Anschließend wird eine Konfiguration durchgeführt, bei welcher die Schadware die Bitcoin-Adresse, zu welcher Opfer das Lösegeld überweisen sollen, erstellt. Danach wird die Verschlüsselung der Daten durchgeführt. Nach diesen Prozeduren wird dem Opfer ein Fenster angezeigt, in welchem es über die Verschlüsselung der Daten informiert wird und eine Überweisung des Lösegelds in Bitcoin gefordert wird [AVL19, S. 2 ff]. Durch diesen Angriff wurde stark auf die Verfügbarkeit eingewirkt, da die verschlüsselten Dateien nicht mehr nutzbar waren. Die WannaCry Ransomware erhielt durch das starke Einwirken auf viele Dienste, wie beispielsweise die Deutsche Bahn, mediale Aufmerksamkeit. Ein Anzeigebildschirm der Deutschen Bahn, auf welchem das entsprechende Fenster mit der Lösegeldforderung zu sehen ist, kann in Abb. 2.1 eingesehen werden.

Petya

Bei Petya, bzw. der Variante NotPetya handelt es sich, wie bei WannaCry, um eine Ransomware, welche im Jahr 2017 das erste Mal entdeckt wurde. Im Gegensatz zu WannaCry werden jedoch nicht nur Daten-Dateien und ausführbare Dateien

Abbildung 2.1.: Lösegeldforderung der WannaCry-Ransomware auf einer Anzeige der Deutschen Bahn. [Bri17]

verschlüsselt, sondern der Master Boot Record manipuliert und in einem anschließendem, kontrolliert herbeigeführten Systemabsturz mit folgendem Reboot das Betriebssystem verschlüsselt, wodurch das System komplett unbrauchbar wird [Fay18, S. 1]. Nach der Verschlüsselung wird eine Lösegeldforderung, welche in Bitcoin zu begleichen ist, angezeigt. Größtenteils wurden mit Petya Systeme in der Ukraine infiziert, jedoch verbreitete sich die Ransomware in insgesamt 64 Länder [Fay18, S. 1 f.]. Durch diesen Angriff wurde die Verfügbarkeit massiv verletzt. So war beispielsweise das Logistikunternehmen Maersk von diesem Angriff betroffen, was zu Unterbrechungen in Lieferketten führte. Daneben wurde durch die Manipulation des Master Boot Records die Integrität und durch den Diebstahl von Login-Informationen von Nutzenden die Authentizität verletzt.

The Fappening

Fappening ist ein Neologismus, welcher sich aus dem Verb ”fap“, englisch für ”masturbieren”, und dem Nomen “Happening“, englisch für ”Ereignis”, zusammensetzt. Unter diesem Begriff wird ein Sicherheitsverstoß aus dem Jahr 2014 verstanden, bei welchem Fotos von weiblichen Prominenten, auf welchen diese nackt oder knapp

bekleidet zu sehen waren, veröffentlicht wurden. Zugang zu den Fotos ist unter anderem durch Social Engineering und Phishing erlangt worden [Mar17, S. 1]. Dabei wurden Zugangsdaten zu E-Mail-Accounts und Zugriff auf Mobiltelefone erlangt. Bei diesem Angriff wurde die Vertraulichkeit der veröffentlichten Daten, sowie die Subjekt-Authentizität der E-Mail-Accounts verletzt.

2.1.2. Angriffsmethoden

Im Folgenden sollen die aktuell häufigsten Angriffsmethoden beschrieben werden. Die häufigste Angriffsmethode ist das Phishing. Rund 41 % der Angriffe im Jahr 2021 sind Phishing-Angriffe, im Jahr 2020 waren es 33 % [IBM22, S. 16]. Dieser Anstieg könne durch Auswirkungen der COVID-19-Pandemie erklärt werden. Durch mehr Kunden von Online-Versandhändlern und Corona-Hilfsmaßnahmen hätten Angreifende viele Vektoren zur Durchführung der Angriffe gehabt [BSI21, S. 24]. Die zweithäufigste Angriffsmethode ist Malware. Im Vergleich zu 2020 ist die Anzahl bekannte Malwarevarianten um 22 % gestiegen. Dies entspricht 144 mio. neuen Varianten [BSI21, S. 42]. Nach der IBM Security X-Force Threat Intelligence liegt der Anteil an Malware-Angriffen bei mindestens 26 %, höher bei Einberechnung der Malware-Angriffstypen, welche dort unter "Other" gelistet sind [IBM22, S. 8]. Nachfolgend werden diese Angriffsmethoden näher erläutert.

Phishing

Das Wort **Phishing** ist ein Kunstwort, welches aus dem Begriff "Password fishing" gebildet wurde [Mü10, S. 465]. Bei dieser Angriffsmethode werden Nachrichten an Nutzende versandt, welche vorgeben von Unternehmen oder Behörden zu sein. In diesen Nachrichten befinden sich meist Links, welche zu gefälschten Websites führen auf welchen Opfer solcher Angriffe diverse Daten eingeben sollen. Ziel dieser Angriffe ist es verschiedene, oft vertrauliche Daten zu stehlen. Dazu zählen Passwörter, Kontonummern, PINs oder Kreditkartennummern. Die Nachrichten geben vor von einem seriösen Absender zu stammen und versuchen oft das Design von offiziellen Mails nachzuahmen. Diese Methodik wird durch die Struktur von E-Mails noch unterstützt, da das Design des Mail-Systems möglichst einfach gehalten werden sollte. So ist es unter anderem möglich, den Absender zu fälschen. Dadurch können Phishing-Mails als echte Nachrichten ausgegeben werden [Hel18, S. 129]. Die Fälschung ist aus

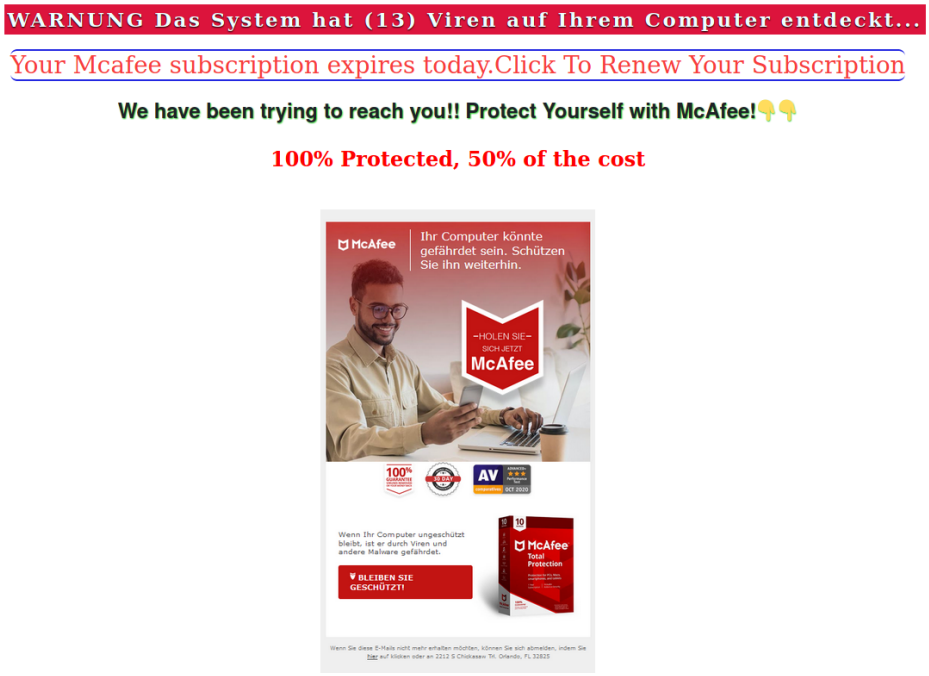


Abbildung 2.2.: Inhalt einer Phishing-Mail, bei welcher versucht wird Nutzende auf eine gefälschte Website zu führen.

der Mail oftmals nicht zu erkennen. In Abb. 2.2 kann der Inhalt einer solchen Mail eingesehen werden. Es wird behauptet, der Computer sei mit Malware infiziert, um Nutzende durch Klick auf die Abbildung auf eine gefälschte Webseite zu leiten.

Malware

Der Begriff Malware ist ein Kofferwort aus dem Begriff "Malicious Software", englisch für schädliche Software. **Malware** ist ein Oberbegriff für Software, welche vorsätzlich Schaden anrichtet, also die Schutzziele verletzen soll. Im deutschen Sprachgebrauch werden auch die Begriffe "Schadprogramme" oder "Schadsoftware" verwendet. Malware kann nach den Infektionswegen und ihrem Zweck klassifiziert werden [Hel18, S. 116]. Bei der Klassifikation nach Infektionswegen wird zwischen Viren, Würmern und Trojanischen Pferden unterschieden.

Viren sind in der Lage, wie ihre biologischen Pendants, Teile oder ihren gesamten Code in andere Dateien zu integrieren. Bei einer Virusinfektion sucht der Schädling nach vorhandenen Dateien, um diese zu infizieren. Es gibt Viren, welche nur ausführbare

Dateien befallen und deren Schadroutinen dann beim Ausführen des Wirtes gestartet werden. Daneben existieren sog. ”Makro-Viren”, welche gezielt Daten-Dateien mit der Fähigkeit zur Nutzung von Makros infizieren [Hel18, S. 116]. Hierbei wird die Schadroutine beim Öffnen der Datei in einem entsprechenden Programm, welches die Makros ausführt, beispielsweise ein Textverarbeitungsprogramm, gestartet. Viren sind in der Regel nicht in der Lage, selbstständig andere Computer zu infizieren. Dazu sind sie auf die Übertragung einer infizierten Datei angewiesen.

Als **Würmer** wird Malware bezeichnet, welche sich selbstständig replizieren kann und durch die Nutzung von Sicherheitslücken in der Lage ist, sich auf andere Computer zu übertragen [Hel18, S. 177]. Im Gegensatz zu Viren infizieren sie keine anderen Dateien.

Trojanische Pferde zeigen ein gänzlich anderes Verhalten als Viren und Würmer. Unter diesem Malware-Typus wird eine nützliche Software verstanden, welche von Nutzenden heruntergeladen und installiert wurde. Vordergründig wird hier meist die versprochene Funktionalität ausgeführt, während im Hintergrund Schadroutinen ausgeführt werden [Hel18, S. 119 f.]. Neben der Bezeichnung Trojanisches Pferd wird meist der Begriff ”Trojaner” verwendet, was in Hinblick auf die Namensherkunft aus der griechischen Sage des Trojanischen Krieges allerdings inkorrekt ist [ebd.].

Neben der Klassifikation nach den Infektionswegen kann Malware auch nach deren Zweck klassifiziert werden. Dabei wird zwischen Rootkits, Backdoors, Ransomware, Spyware, Adware und Scareware unterschieden.

Rootkits sind Malwaretypen, welche die Integrität und Verbindlichkeit verletzen können. Es handelt sich dabei meist um eine Ansammlung an Tools, mit welchen Angreifende das System manipulieren können, um unter anderem Dateien und Verzeichnisse zu verstecken oder um Logeinträge ändern zu können. Meist werden sie in Kombination mit anderen Malwaretypen oder Angriffsmethoden verwendet [Hel18, S. 120].

Backdoors ermöglichen Angreifenden Zugriff auf das infizierte System. Dadurch können Daten ausgelesen und manipuliert werden, sowie Adminrechte erlangt werden, wodurch das System auf vielfältige Weise verwendet werden kann [ebd.]. Dadurch können, je nach Nutzung durch Angreifende, die Integrität, Vertraulichkeit und Verfügbarkeit verletzt werden.

Als **Ransomware** wird Malware bezeichnet, welche den Zugriff auf Dateien oder das ganze System sperrt und zur Freigabe ein Lösegeld, englisch Ransom, verlangt. Dabei werden zwei Sub-Typen unterschieden. Der erste Typ verhindert den Zugriff auf das System durch die Anzeige eines Sperrbildschirmes, welcher nicht zu umgehen ist, während der zweite Typ im Regelfall weiterhin Zugriff auf das System gewährt, allerdings Daten verschlüsselt [AVL19, S. 1]. Dabei wird auch eine Lösegeldforderung angezeigt. Es gibt allerdings keine Garantie, dass nach der Zahlung das System wirklich freigegeben wird bzw. die Daten wieder entschlüsselt werden [Hel18, S. 120]. Ransomware gilt als größte Bedrohung für Internetnutzende und die Haupteinnahmequelle für Cyberkriminelle [AVL19, S. 1]. Durch Ransomware-Angriffe wird die Verfügbarkeit verletzt, wie in den Fällen von WannaCry und Petya beschrieben wurde, kann dies massive Auswirkungen haben. Daneben wird durch die Verschlüsselung von Daten die Integrität verletzt. Neben diesen ist bekannt, dass einige Ransomwares die Daten vor der Verschlüsselung stehlen und mit Veröffentlichung dieser gedroht wird, sollte das Lösegeld nicht gezahlt werden [BSI21, S. 12]. Dies ist zusätzlich ein Angriff auf die Vertraulichkeit.

Spyware hat den Zweck, infizierte Rechner auszuspionieren. Dazu verfügt dieser Typus über unterschiedliche Fähigkeiten zum Erlangen verschiedenster Daten. Die so erhaltenden Daten werden dann an Angreifende übermittelt. Diese Malware verletzt die Vertraulichkeit.

Adware ist eine Software, welche unerwünschte Werbung auf dem Gerät anzeigt. Diese Klassifikation ist allerdings nicht unumstritten, da einerseits das Anzeigen von Werbung an sich keine Schutzziele verletzt, andererseits kann Adware jedoch auch mit Funktionen ausgestattet sein, welche Daten stehlen oder Nutzende ausspionieren können [GKBK19, S. 1].

Unter **Scareware** wird eine Art von Malware bezeichnet, welche versucht Nutzende zu verängstigen. Dazu wird meist auf Sicherheitslücken hingewiesen oder eine Infektion des Systems behauptet. Durch Zahlung von Geld oder dem Download von spezieller Software sollen diese Probleme dann gelöst werden. Neben dieser Vorgehensweise wurde auch Scareware entdeckt, welche behauptet, Nutzende hätten Straftaten begangen und eine Zahlung würde eine weitere Strafverfolgung verhindern [Hel18, S. 121].

Auch wenn diese Klassifikationen existieren, ist gefundene Malware meist eine Mischform. Ein Beispiel dafür ist der sog. "Bundespolizei Virus". Bei diesem handelt es sich um eine Ransomware, welche den Zugriff auf den Rechner mit einem Sperrbildschirm sperrt. Dieser kann in Abb. 2.3 eingesehen werden. Neben dieser Klassifikation ist auch die Klassifikation als Scareware zutreffend, da auf dem Sperrbildschirm behauptet wird, die Sperrung sei von der Bundespolizei vorgenommen worden aufgrund von Straftaten, welche vom infizierten System aus verübt worden seien.

Abbildung 2.3.: Sperrbildschirm des sog. Bundespolizei Virus. [bV22]

Die Infektion mit Malware kann über verschiedene Wege erfolgen. Der primäre Angriffsvektor für Malware ist ein infizierter Mail-Anhang. Besonders konnten zielgerichtete Angriffe beobachtet werden, bei welchen die Malware unter anderem als Bewerbung, Rechnung oder als Lieferschein getarnt war. Neben infizierten Mail-Anhängen gilt auch das sog. Malwaretising als ein häufig genutzter Angriffsvektor. Hierbei wird Werbung, welche auf Websites angezeigt wird, kompromittiert, wodurch Computer mit Malware infiziert werden können [RN17, S. 8]. Daneben können In-

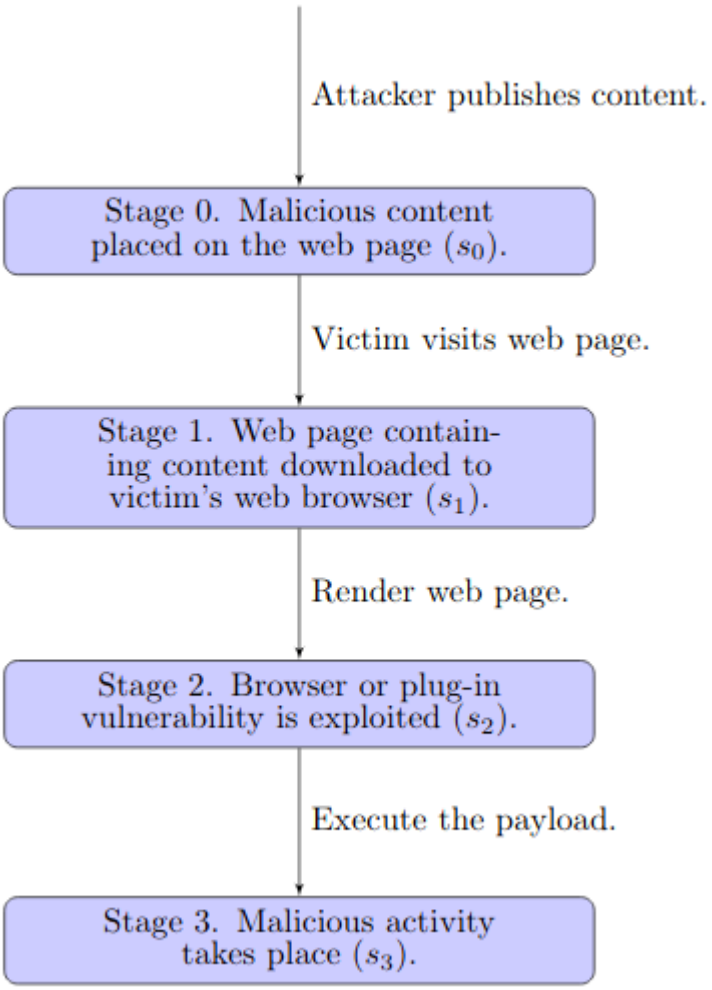


Abbildung 2.4.: Schematischer Ablauf eines Drive-by-Downloads. [LWGK13, S. 2]

fektionen durch sog. Drive-by-Downloads erfolgen. Dabei werden seriöse Webseiten kompromittiert, was dazu führt, dass Besuchende der Webseite durch das reine Aufrufen mit Malware infiziert werden können [LWGK13, S. 1]. Der schematische Ablauf eines solchen Angriffes kann in Abb. 2.4 eingesehen werden.

2.1.3. Faktor Mensch in der IT-Sicherheit

Neben den Bedrohungen der Schutzziele durch Angriffe von außen, werden diese auch durch die Nutzenden selbst bedroht. So wird das Schutzziel der Authentizität und der Vertraulichkeit durch das Verwenden von schwachen Passwörtern und der Wiederverwendung dieser konterkariert. So geben 75 % der Arbeitenden, welche ihre Arbeit im Homeoffice erledigen, an identische Passwörter für unterschiedliche Dienste zu nutzen [Viv22, S. 1]. 27 % dieser Personen geben an Passwörter auf ihrem Computer zu speichern [ebd.]. Daneben ist auch ein Defizit im Umgang mit Verschlüsselung nachweisbar. So werden von Mitarbeitenden im Homeoffice Daten der Unternehmen unverschlüsselt übertragen und diese Übertragungen über unsichere WLAN-Verbindungen durchgeführt [Viv22, S. 1 f.]. Dies zeigt sich auch in einer Untersuchung aus dem Jahr 2015, nach welcher Nutzende oft nicht in der Lage sind, verschlüsselte und signierte E-Mails zu verschicken [Reu21, S. 95 f.]. Zusätzlich wird die Bedeutung von verschlüsselten HTTP-Verbindungen von Nutzenden oft fehlinterpretiert [Reu21, S. 96 f.]. Diese Defizite führen zu Schwächen in der Vertraulichkeit. Folgend werden diese Sicherheitslücken näher erläutert.

Passwörter

Passwörter dienen der Gewährleistung der Subjekt-Authentizität. Dabei wird ein Passwort als ein Geheimnis verstanden, welches im Optimalfall nur ein bestimmtes Individuum kennt. Durch die korrekte Eingabe des Passwortes wird somit die Identität des Subjektes nachgewiesen. In diesem Nachweisverfahren wird von dem Passwort ein Hash-Wert erzeugt, welcher im entsprechenden System, beispielsweise dem Betriebssystem, hinterlegt wird. Nach der Eingabe des Passwortes durch Nutzende wird aus der Eingabe ebenfalls ein Hash-Wert mit der exakt gleichen Funktion erzeugt. Wenn die beiden Hashes übereinstimmen, wird Zugang gewährt [Eck18, S. 446]. Die Sicherheit eines Passwortes wird durch die Geheimhaltung und die Passwortwahl beeinflusst. Die Geheimhaltung von Passwörtern wird oft durch das Niederschreiben oder das Abspeichern verletzt [Eck18, 447 f.]. Daneben werden oft schwache Passwörter gewählt [Eck18, S. 448 f.]. Passwörter gelten als schwach, wenn sie durch das Ausprobieren erraten oder durch Informationen über Nutzende leicht erschlossen werden können. Nach einer Untersuchung aus dem Jahr 2018 sind 89 % der Sicherheitsverletzungen auf schwache oder gestohlene Passwörter zurückzuführen [Nob18, S. 3]. Für sichere Passwörter wird eine Mindestlänge von zwölf

Zeichen empfohlen, ferner sollten möglichst viele unterschiedliche Zeichen enthalten sein. Außerdem wird von der Verwendung privater Informationen, wie beispielsweise Namen, abgeraten [Eck18, S. 449].

Verschlüsselung

Bei der Verschlüsselung wird ein vorliegender Klartext, beispielsweise eine E-Mail oder ein HTML-Dokument, durch ein Verschlüsselungs-Verfahren in einen Kryptotext umgewandelt. Dies dient der Vertraulichkeit, da die im Klartext codierten Informationen nicht ohne weiteres aus dem Kryptotext erhalten werden können. Nach der Übertragung der entsprechenden Informationen sollen diese wieder entschlüsselt, also von einem Kryptotext in einen Klartext umgewandelt werden [Eck18, S. 285]. Dabei dürfen die Informationen im Klartext nicht verändert werden. Bei der Ver- und Entschlüsselung werden sog. Schlüssel verwendet. Dies sind Informationen, mit welchen durch die entsprechenden Funktionen, eine Umwandlung von Klartext und Kryptotext und umgekehrt stattfinden kann [Hel18, S. 6 ff.]. Man unterscheidet zwischen symmetrischen und asymmetrischen Verfahren. Bei symmetrischen Verfahren sind die Schlüssel zum Ver- und Entschlüsseln gleich, im Gegensatz dazu wird bei asymmetrischen Verfahren ein öffentlicher Schlüssel zum Verschlüsseln verwendet und ein privater Schlüssel zum Entschlüsseln [Hel18, S. 9]. Im Folgenden wird davon ausgegangen, dass die verwendeten Verschlüsselungen sicher sind, da die Diskussion um die Sicherheit kryptographischer Protokolle im Kontext dieser Arbeit nicht sinnvoll ist.

Die durch die Verschlüsselung erzeugte Vertraulichkeit wird durch Nutzende unterminiert. Dies wird im Umgang mit E-Mails erkennbar. So sind viele Nutzende nicht in der Lage, versendete Mails zu verschlüsseln [Reu21, S. 95 f.]. Dies kann auf nicht kommunizierte und verstandene Abläufe, welche zur Durchführung der Verschlüsselung erforderlich sind, zurückzuführen [ebd.]. Daneben fehlt auch das Wissen um die Existenz dieser Sicherheitsmaßnahme [Reu21, S. 93]. Daraus folgen unverschlüsselt versendete E-Mails, welche durch Lauschangriffe ausgelesen werden können, wodurch die Vertraulichkeit verletzt wird. Ähnlich verhält es sich mit dem unverschlüsselten Datentransfer, welcher bei Arbeiten im Homeoffice beobachtet werden konnte [Viv22, S. 1 f.]. In Kombination mit unsicheren WLAN-Verbindungen, welchen der Abhörschutz der Kabelgebundenheit fehlt, ist die Vertraulichkeit von eventuell sensiblen Daten bedroht.

Daneben liegen auch eine Fehlinterpretation von HTTPS-Verbindungen durch Nutzende vor. HTTPS dient unter anderem der verschlüsselten Übertragung von HTML-Dokumenten. Viele Nutzende gingen davon aus, dass eine solche Verbindung neben der Vertraulichkeit auch die Authentizität von aufgerufenen Websites gewährleiste [Reu21, S. 97]. Dadurch würden gefälschte Websites, welche beispielsweise über erhaltene Phishing-Mails aufgerufen werden als seriös eingestuft. Dies kann Nutzende verleiten, sensible Daten auf solchen Websites einzugeben. So würde die fehlerhafte Einschätzung der Authentizität zu einer Verletzung der Vertraulichkeit führen.

2.1.4. Gegenmaßnahmen

Um Schäden durch die Verletzung der Schutzziele, durch Angriffe von außen oder die Ausnutzung von durch Nutzenden herbeigeführte Sicherheitslücken, zu vermeiden sollten Gegenmaßnahmen ergriffen werden. Diese können technischer oder organisatorischer Natur sein. Nachfolgend werden zu den vorher vorgestellten Angriffsmethoden und durch Nutzende herbeigeführte Sicherheitslücken mögliche Gegenmaßnahmen dargestellt.

Phishing

Es sollen nun mögliche Maßnahmen gegen Phishing-Angriffe dargestellt werden. Eine einfache Maßnahme ist der Aufruf von Websites über direkte Links, bzw. über im Webbrowser gesetzte Lesezeichen. Anstatt durch den Link auf Phishing-Mails zu klicken kann so auf die echte Website des angeblichen Absenders zugegriffen werden. Dies setzt allerdings voraus, dass Nutzende zu einem früheren Zeitpunkt auf die Betreffende Website zugriffen.

Als ein starker Schutz gegen Phishing wird eine Zwei-Faktor-Authentifikation angesehen [Eck18, S. 573]. Dabei wird das Login bei einem Dienst, etwa beim Online-Banking, um einen weiteren Faktor erweitert. Meist werden dabei sog. Dongles verwendet, dabei handelt es sich um nicht programmier- und änderbare Geräte, welche für die Speicherung von Schlüsseln und dem Signieren von Daten verwendet werden [Eck18, S. 555]. Bei einem Login in den entsprechenden Dienst wird der Dongle benötigt, um eine sog. Attestierungssignatur zu erstellen [Eck18, S. 557 ff.]. Diese

Signatur wird an den entsprechenden Webserver übermittelt und verifiziert. Hierdurch wird sichergestellt, dass das Login tatsächlich vom authentifizierten Subjekt durchgeführt wurde. Dadurch sind erfolgreiche Phishing-Angriffe ohne Erlangung des entsprechenden Dongles nicht sinnvoll, da die erhaltenen Daten keinen Zugang zu den entsprechenden Accounts bieten.

Daneben sind Schulungs- und Sensibilisierungsmaßnahmen zu empfehlen [Reu21, S. 99]. Da es unter anderem möglich ist, die Ziele von in Phishing-Mails enthaltenen Links zu prüfen, ob diese wirklich zu der angegebenen Website führen, indem mit der Maus darüber gehovert wird. Hierfür ist allerdings die Fähigkeit URLs lesen zu können erforderlich [ebd.]. So können Nutzende selbstständig Phishing-Angriffe erkennen und sie würden keine sensiblen Daten preisgeben.

Malware

Nun sollen Maßnahmen gegen Malware erläutert werden. In der Vergangenheit wurde die Verwendung von Anti-Malware-Software als primäres Mittel empfohlen. Die Verwendung solcher Software ist allerdings umstritten, da sie mitunter selbst Sicherheitslücken erzeugen [Hel18, S. 125 f.]. Daneben wird neue Malware meist von den Scannern nicht erkannt, sondern erst nachdem diese bei den entsprechenden Herstellern bekannt geworden sind [ebd.].

Präventiv wird das regelmäßige Anlegen von Back-ups empfohlen. Hierdurch kann ein infiziertes System wieder auf einen sicheren Stand zurückgesetzt werden. Da besonders moderne Ransomware versucht Back-ups unbrauchbar zu machen, sollten diese auf einem isolierten System gespeichert werden [RN17, S. 8]. Vor dem Back-up sollte jedoch darauf geachtet werden, dass keine Malware aktiv ist, da bereits Ransomware beobachtet wurde, welche die Sperrung des Systems bzw. Verschlüsselung der Daten verzögert, um Back-ups infizieren zu können [ebd.].

Weiterhin sollte durch die Rechteverwaltung des verwendeten Betriebssystems die Installation von Software für Endnutzende verweigert werden und entsprechende Rechte nur für Accounts von Administrierenden zugelassen werden [Hel18, S. 126]. Hierdurch kann die Ausführung von Schadcode, welcher beispielsweise Persistenz ermöglicht oder die Einrichtung von Sperrmaßnahmen durchführt, verhindert werden.

Auch in Bezug auf die Infektionswege können Gegenmaßnahmen getroffen werden. Um Infektionen durch maliziöse Mail-Anhänge zu verhindern, sollten Mitarbeitende entsprechend geschult und sensibilisiert werden, um entsprechende Angriffsversuche erkennen zu können [RN17, S. 8]. Zum Schutz vor Drive-by-Downloads kann JavaScript in Webbrowsern deaktiviert werden, da dies allerdings meist mit erheblichen Funktionseinschränkungen von Webseiten einhergeht, sollten hier Scriptblocker verwendet werden, um Scripte unbekannter Herkunft blockieren zu können, ohne die Funktionalitäten der Webseite zu beeinträchtigen. Zum Schutz vor Malwaretising wird die Nutzung von AdBlockern empfohlen [ebd.].

Passwörter

Um Sicherheitslücken durch schwache Passwörter zu vermeiden, sollten Nutzende geschult werden, selbstständig sichere Passwörter auswählen zu können. Die Einführung von Passwortrichtlinien führt in der Praxis meist nicht zu mehr Sicherheit, da die Richtlinien als lästig empfunden werden [Reu21, S. 100]. Auch das vorgeschriebene Ändern von Passwörtern bringe nur wenig zusätzliche Sicherheit, da Nutzende dann meist vorhersehbare Passwörter wählen oder ein altes erneut verwenden würden [ebd.]. Durch zu strenge Passwortrichtlinien werde das Abspeichern oder Notieren dieser begünstigt [ebd.].

Neben der Passwortwahl sollte auch der Umgang mit Passwörtern geschult werden. Dadurch sollen Nutzende für die Folgen von Passwortdiebstählen und die entstehenden Sicherheitslücken durch abgespeicherte Passwörter sensibilisiert werden.

Verschlüsselung

Zur Stärkung der Vertraulichkeit sollte Verschlüsselung verwendet werden. Da die Verschlüsselung von E-Mails für Endnutzende problematisch ist, sollten diese in die Weiterentwicklung von E-Mail-Programmen einbezogen werden. Dies soll zu einer besseren Bedienbarkeit führen, wodurch Nutzende erkennen können, ob bereits eine Verschlüsselung vorliegt und, falls nicht, wie diese durchgeführt werden kann [Reu21, S. 95 f.]. Daneben sollten auch praktische Softwareschulungen durchgeführt werden, um die Endnutzenden in die konkrete Durchführung einzuführen.

Neben der Anwendung der Verschlüsselung im E-Mail-Verkehr sollte auch generell in die Praxis der Verschlüsselung im Web durch Schulungen eingeführt werden, um so beispielsweise Fehleinschätzungen zu vermeiden oder auch um aufzuzeigen wie sichere Verbindungen aufgebaut werden können. Dies soll der Vermeidung von unverschlüsselt transferierten Daten und damit der Stärkung der Vertraulichkeit dienen.

2.2. E-Learning

Als E-Learning wird allgemein das Lernen mit elektronischen Medien bezeichnet [SLW13, S. 180]. Dadurch wird dieser als Oberbegriff für verschiedene Formen der Wissensvermittlung durch elektronische Medien verwendet. Zu diesen zählen unter anderem [DSRL18, S. 5]:

- Computer-basiertes Training
- Web-based Instruction
- Mobile Learning

Im Folgenden wird der Begriff E-Learning allerdings in einer engeren Definition verwendet, nach welcher E-Learning als Wissensvermittlung durch digitale Medien verstanden wird [SLW13, S. 180]. Nach diesem Verständnis können E-Learning-Angebote nach ihren Funktionen unterteilt werden.

E-Learning kann als reine Informationsdistribution genutzt werden. Dabei werden Lernenden entsprechend aufbereitete Informationsmaterialien zur Verfügung gestellt und eine selbstständige Beschäftigung mit diesen erwartet. Dies habe jedoch hohe Anforderungen an Lernende, da Selbststeuerung, Medienkompetenz und entsprechendes Vorwissen vorausgesetzt werde [SLW13, S. 183]. Hierbei sind allerdings keine Lehrenden erforderlich.

Eine weitere Funktion von E-Learning ist das selbstständige Erschließen eines Themas. Dabei findet eine Interaktion zwischen Lernenden und den digitalen Systemen, welche die entsprechenden Inhalte bereitstellen, statt. Zusätzlich zur angeleiteten Informationsverarbeitung werden hier Übungen zum Lernstoff angeboten. Hierbei

seien die Anforderungen an Lernende geringer im Verhältnis zur reinen Informationsdistribution, da nur Motivation und Selbstorganisation vorausgesetzt werde [ebd.]. Allerdings ist hier der Entwicklungsaufwand höher, da neben der Aufbereitung der Materialien auch Instruktionen, passende Übungen und Möglichkeiten zur Rückmeldung von sinnvollem Feedback erstellt werden müssen [ebd.]. Hier sind nicht zwingend Lehrende erforderlich, diese können aber in Form von Beratenden und Tutoren auftreten.

Die dritte Funktion ist das selbstständige Konstruieren von Wissen in Zusammenarbeit mit anderen Lernenden. Diese Funktion stelle die höchsten Anforderungen an Lernende, da neben Selbststeuerung und Erfahrung im Umgang mit Medien auch Sozialkompetenz vorausgesetzt werde [ebd.]. Hierbei sind Lehrende als Initiierende und Coachende erforderlich.

Da es in dieser Arbeit um einen Kompetenzerwerb geht, soll nachfolgend der Kompetenzbegriff definiert werden und eine Erläuterung von digitalen Kompetenzen stattfinden. Anschließend sollen konkrete E-Learning-Formate vorgestellt werden. Darauf folgt eine Beschreibung von für diese Arbeit relevanten psychologischen Aspekten. Danach werden Effekte der Multimedialität im Kontext des E-Learnings beschrieben. Abschließend wird auf die Evaluation von E-Learnings eingegangen.

2.2.1. Kompetenzen

Unter **Kompetenz** wird die Fähigkeit und Bereitschaft von Personen erlerntes Wissen und Fähigkeiten in komplexen, dynamischen Situationen, unter Beachtung von Normen und Werten einzusetzen, verstanden [KSK22, S. 4 f.]. Hierbei wird also Erlerntes zielgerichtet zur Lösung eines Problems in einem bestimmten Kontext angewandt [ebd.]. Kompetenzen können als Dispositionen, welche durch Bildungs- und Erziehungsprozesse erworben wurden und die Bewältigung von Problemstellungen ermöglichen, verstanden werden [KH07, S. 21].

Als **Fähigkeit** wird die erlernte Durchführung einer bestimmten Tätigkeit verstanden. Meist findet das Lernen hier durch das Wiederholen der entsprechenden Tätigkeit statt [KSK22, S. 4].

Wissen beschreibt die Gesamtheit an Fähigkeiten und Kenntnissen. Wissen kann nicht direkt erfasst werden. Das Vorhandensein von Wissen wird durch seine Anwendung bewiesen [ebd.].

Von diesen Begriffen ist die **Qualifikation** abzugrenzen. Als Qualifikationen wird die Beglaubigung von Wissen und Fähigkeiten bezeichnet. Meist muss dafür das Wissen oder die Fähigkeit nachgewiesen werden [ebd.].

Digitale Kompetenzen sind Kompetenzen, welche im Kontext des Umgangs mit Informationstechnologie und digitalen Medien stehen [Fer12, S. 30]. Sie umfassen unterschiedliche Bereiche des Digitalen. Nach dem "Digital Competence Framework for Citizens" der Europäischen Union werden digitale Kompetenzen in 5 Felder unterteilt [VPCGVdB16, S. 8 f.].

Das erste Feld ist die **Informations- und Datenkompetenz**. In diesem Kompetenzfeld geht es um den Umgang mit Daten und Informationen. Darunter fallen das Auffinden, Bewerten und Verwalten von Informationen, ist allerdings nicht darauf beschränkt.

Das zweite Kompetenzfeld ist **Kommunikation und Zusammenarbeit**. Hierbei geht es um die Kommunikation und das Teilen von Informationen mit anderen Personen über digitale Kanäle. Zusätzlich werden hierzu die Netiquette und der Umgang mit digitalen Identitäten gezählt.

Im dritten Kompetenzfeld, der **Erstellung digitaler Inhalte**, werden Kompetenzen zur Erstellung eigener digitaler Inhalte zusammengefasst. Diese umfassen künstlerische und technische Werke. Daneben wird hierbei auch die entsprechende rechtliche Kompetenz, wie im Umgang mit dem Urheberrecht, aufgeführt.

Als viertes Feld wird die **Sicherheit** genannt. Dies umfasst einerseits die IT-Sicherheit, besonders der Schutz von eigenen Geräten und persönlichen Daten. Andererseits wird zu diesem Feld auch das Verständis der Auswirkungen von digitalen Geräten und Inhalten auf die eigene Gesundheit, sowie auf die Umwelt verstanden.

Das fünfte und letzte Kompetenzfeld ist die **Problemlösungskompetez**. Dieses umfasst Kompetenzen zur Lösung technischer Probleme, der Identifizierung benötigter Tools und Technologien, sowie die Selbstreflexion zur Auffindung fehlender Kompetenzen.

Neben diesem Framework existieren allerdings noch weitere Frameworks, welche unterschiedliche Schwerpunkte setzen. Ein Beispiel dafür ist die sog. "International Computer Driving Licence". Dabei handelt es sich um verschiedene Programme, welche von einer Non-Profit-Organisation durchgeführt werden und dabei Kompetenzen in 13 unterschiedlichen Bereichen schulen. Nach Abschluss einer Schulung wird Teilnehmenden eine entsprechende Qualifikation ausgestellt [Fer12, S. 60 ff.].

Von der "International Computer Driving Licence" werden folgende Kompetenzfelder abgedeckt [Fer12, S. 62]: Konzepte der Informations- und Computertechnologie, Nutzung von Computern und Verwaltung von Dateien, Textverarbeitung, Tabellenkalkulation, Nutzung von Datenbanken, Präsentation, Web und Kommunikation, 2D Computer Aided Design, Bildbearbeitung, Webbearbeitung, Nutzung von Gesundheitsinformationssystemen, IT-Sicherheit, Projektplanung.

2.2.2. Formate

Nun sollen einige ausgewählte Formate des E-Learnings vorgestellt werden. Hierbei ist zu beachten, dass E-Learning dabei als Wissensvermittlung durch digitale Medien verstanden wird (vgl. Kap. 2.2).

Podcasts

Der Begriff Podcast setzt sich aus den Wörtern "Ipod" und "Broadcast" zusammen. Er bezeichnet den Prozess der Erstellung von Audio- und Videodateien, deren Veröffentlichung und des Zugänglichmachens dieser [SLW13, S. 185 f.]. Neben der Anwendung in der Unterhaltung können Podcasts auch in der Lehre verwendet werden. So können Podcasts zur Anreicherung von Präsenzlehre verwendet werden, indem fachlich relevante Podcasts in den Unterricht integriert werden. Neben dem Einsatz als Informationsdokument können Podcasts auch interaktiv verwendet werden, indem Lernenden aufgetragen wird, eine entsprechende Audio- oder Videoaufnahme zu einem bestimmten Thema zu produzieren. Neben der Informationsdistribution ist auch die Anwendung beim Erlernen von Fremdsprachen denkbar, indem die erworbenen Sprachkenntnisse praktisch in der Produktion eines Podcasts angewandt werden [SLW13, S. 186].

Videospiele

Auch Videospiele können im E-Learning Kontext genutzt werden. Hierbei ist zu erwähnen, dass nicht jedes Videospiel der Wissensvermittlung dient und damit auch nicht zum E-Learning gezählt wird. Die Motivation beim Einsatz von Videospielen in Lernkontexten ist das Erreichen von bildungsfernen Zielgruppen, welche durch das spielerische Lernen angesprochen werden sollen [SLW13, S. 183 f.]. Daneben können Videospiele zum selbstgesteuerten und selbstentdeckenden Lernen genutzt werden [ebd.]. Wenn in einem solchen Videospiel auf gesellschaftlich relevante Problemstellungen eingegangen wird, spricht man von einem **Serious Game**.

Web-based Training

Unter einem Web-based Training (WBT) wird ein digitales Lernmedium verstanden, welches von Lernenden über einen Webbrowser aufgerufen werden kann [NW20, S. 590 f.]. Die entscheidenden Merkmale sind die Multimedialität und die Möglichkeit der Interaktivität, dies ist jedoch von der konkreten Gestaltung des WBTs abhängig. Meist liegen WBTs als Webanwendungen vor, welche von Lehrenden auf entsprechende Webserver hochgeladen und anschließend den Lernenden zugänglich gemacht werden. Vorteile von WBTs sind die Unabhängigkeit der Betriebsysteme der Lernenden und die Möglichkeit Testitems zu verwenden. Als Testitems werden Funktionen in WBTs bezeichnet, welche Lernenden die Möglichkeit bieten ihren Lernfortschritt zu bewerten. Aus den Ergebnissen dieser Testitems kann der Lernerfolg bestimmt, das WBT an den Lernenden adaptiert werden oder auch als eine Prüfung das Bestehen bzw. Nicht-Bestehen einer Lerneinheit angeben. WBTs haben eine deutliche Praxisrelevanz. Stand 2014 werden in rund 70 % aller deutschen Unternehmen mit mehr als 500 Mitarbeitenden WBTs genutzt [NW20, S. 590].

Massive Open Online Courses

Die Bezeichnung Massive Open Online Course (MOOC) wird für das angeleitete Lernen in durch das Internet zugänglichen Kursen bezeichnet [NW20, S. 26]. Hierbei steht der Austausch zwischen Lernenden und Lehrenden, aber auch zwischen den Lernenden untereinander im Vordergrund [NW20, S. 306]. Dabei werden Seminare

und Vorlesungen online abgehalten. Hierbei können die Vorlesungen live gehalten werden oder auch als eine Aufnahme zur Verfügung gestellt werden.

2.2.3. Psychologische Aspekte

Hier sollen nun einige psychologische Aspekte mit Relevanz für das Lernen mit digitalen Medien erläutert werden. Es wird auf deren Einfluss auf den Lernerfolg, sowie die mögliche Nutzung eingegangen.

Motivation

Motivation wird allgemein als Antriebskraft, welche Menschen dazu bringt Dinge zu tun, verstanden [HY16, S. 3]. Diese Antriebskraft ist zielgerichtet, dies bedeutet, dass Verhalten gezeigt wird, welches zum Erreichen des gesetzten Zieles führt. Die Ziele werden durch die Motive einer Person definiert [MR17, S. 225]. Man unterscheidet zwischen **intrinsischer Motivation** und **extrinsischer Motivation** [BSPL18, S. 113]. Bei der intrinsischen Motivation kommt der Antrieb von der Person selbst. Beispiele hierfür sind Neugier, Interesse an einem Thema oder auch eigene Werte [ebd.]. Die extrinsische Motivation wird durch äußere Faktoren ausgelöst. Im konkreten Fall des E-Learnings können dies beispielsweise der Erwerb einer Qualifikation, welche für eine gewünschte Tätigkeit notwendig ist, oder auch eine durch Vorgesetzte angeordnete Weiterbildungsmaßnahme sein.

Im Kontext des E-Learnings kann die Motivation der Lernenden zu einem höherem Lernerfolg führen. Allerdings kann eine entsprechende motivationsfördernde Gestaltung in Abhängigkeit von anderen Moderatorvariablen auch das Lernen negativ beeinträchtigen [PS22, S. 590]. Eine Steigerung der Motivation könne durch ansprechende Grafiken und Gestaltung des Lernmaterials erreicht werden [ebd.]. So kann Anthropomorphisierung, also die Vermenschlichung von Objekten, genutzt werden, hierdurch wird nicht nur die Motivation während des Lernens gefördert, sie bleibt nach Abschluss erhalten [ebd.].

Zur Steigerung der intrinsischen Motivation sollten die drei psychologischen Grundbedürfnisse, Autonomie, Kompetenz und soziale Eingebundenheit, erfüllt werden [PS22, S. 590 f.]. **Autonomie** bezeichnet die Selbständigkeit einer Person. Dieses Grundbedürfnis kann erfüllt werden, indem Lernenden Freiheiten geboten werden.

Kompetenz wird in diesem Kontext als das Erlernen und erfolgreiche Anwenden von Fähigkeiten und Wissen verstanden. Dieses Grundbedürfnis kann durch das Erfüllen von Aufgaben mit einem angemessenen Schwierigkeitsgrad erfüllt werden. Die **soziale Eingebundenheit** beschreibt das Bedürfnis von Menschen nach sozialer Interaktion. Dieses Bedürfnis kann durch direkten Kontakt mit anderen Menschen erfüllt werden. Da allerdings nicht jedes Format des E-Learnings Möglichkeiten zur Kommunikation mit anderen Lernenden oder den Lehrenden ermöglicht, können **Hinweisreize** genutzt werden. Als solche werden Eigenschaften von Lernmaterialien verstanden, welche ihnen menschliche Eigenschaften zuschreiben [PS22, S. 591]. Um Hinweisreize auszulösen, kann auch hier die Anthropomorphisierung genutzt werden. Auch die Verwendung von Höflichkeit, Umgangssprache, Dialekten und Soziolekten führt zu einer besseren Lernleistung durch die Aktivierung von sozialen Prozessen [PS22, S. 591 f.]. Feedback kann auch als eine Form von Hinweisreizen angesehen werden, so trägt Feedback zur Erfüllung des Grundbedürfnisses der sozialen Eingebundenheit bei.

Emotion

Der Begriff **Emotion** besitzt keine absolute Definition, stattdessen wird empfohlen diesen in einem konkreten Kontext zu definieren [MR17, S. 188]. Dennoch werden Emotionen drei Komponenten zugeordnet. Die erste Komponente ist die **Affektivität**. Darunter wird der Gefühlscharakter einer Emotion verstanden [ebd.]. Als zweite Komponente wird der **Bezug zu einem Objekt** genannt. So werden Emotionen durch ein Objekt ausgelöst und haben stets einen Bezug dazu. Hierbei muss es sich nicht um ein real existierendes Objekt handeln. Der Bezug kann auch zu Erwartungen oder Gedankenkonstrukten gelten [ebd.]. Die dritte Komponente ist die **zeitliche Dynamik**. Zum einen wird damit ausgedrückt, dass Emotionen eine zeitlich begrenzte Dauer haben. Zum anderen wird damit das Auftreten und Verschwinden durch die Kopplung an das Bezugsobjekt beschrieben. So kann eine Emotion verschwinden, wenn das Bezugsobjekt verschwindet, aber die Emotion erneut auftreten, wenn das Bezugsobjekt erneut erscheint [ebd.]. Damit können Emotionen als Empfindungen, welche im Kontext eines Objektes, hier das E-Learning-Modul, stehen und vor, während und nach der Nutzung auftreten können.

Emotionen können sowohl einen positiven als auch einen negativen Einfluss auf das Lernen haben. Durch die Bindung kognitiver Ressourcen für die Verarbeitung

der Emotion stehen diese nicht für das Verarbeiten der Lerninhalte zur Verfügung, was zu einem geringeren Lernerfolg führt [PS22, S. 589]. Daneben können positive Emotionen jedoch auch förderlich auf Lernprozesse einwirken. Wie auch bei der Motivation hängt dieser Einfluss auch von verschiedenen Moderatorvariablen ab. Positive Emotionen können durch die Gestaltung der Lernmaterialien erzeugt werden. Dabei können Farben, Formen und emotional geladene Bilder verwendet werden. Die Relevanz des Lernmaterials für die Lernenden oder für Ziele der Lernenden steht ebenfalls in Zusammenhang mit den Emotionen der Lernenden. So werden positive Emotionen erzeugt, wenn die Relevanz gegeben ist, bei Abwesenheit können negative Emotionen erzeugt werden [BSPL18, S. 281]. Weiterhin wird die Gewährung von Selbstbestimmung in Lernsituationen, also die Erfüllung des psychologischen Grundbedürfnisses der Autonomie, als förderlich für das Erzeugen positiver Emotionen angesehen [ebd.].

Aufmerksamkeit

Aufmerksamkeit ist ein kognitiver Mechanismus, welcher der Selektion von wahrgenommenen Informationen dient. Dadurch sollen irrelevante Informationen von der Verarbeitung ausgeschlossen werden und motorische Reaktionen effizient koordiniert werden [MR17, S. 104]. Diese Selektion ist notwendig, da Menschen jederzeit einer Vielzahl von Reizen ausgesetzt sind und die Verarbeitung aller Reize die Verarbeitungskapazität übersteigen würde. Nach der **Cognitive Load Theory** werden Informationen in einem Arbeitsgedächtnis verarbeitet. Dieses hat allerdings nur eine begrenzte Kapazität. Wird dieses Limit überschritten, so wird auch das Lernen beeinträchtigt [Kal11, S. 1 f.]. Daraus folgt, dass nicht zu viele Informationen zur gleichen Zeit gegeben werden sollten. Besonders lernirrelevante Informationen, beispielsweise durch dekorative Objekte, sollten auf ein Minimum reduziert werden. Im Folgenden wird auf die selektive auditive und visuelle Aufmerksamkeit eingegangen, da diese für das E-Learning von Bedeutung sind.

Bei der visuellen Aufmerksamkeit ist besonders die Steuerung der Aufmerksamkeit relevant, um Lernende nicht von den relevanten Inhalten abzulenken und ihre Aufmerksamkeit stattdessen zu diesen zu lenken. Die Aufmerksamkeit kann durch Farbe gelenkt werden. Dabei wird Aufmerksamkeit an Orte mit einer auffälligen Farbe oder einer Farbe mit Signalwirkung, wie Rot, gelenkt [Hei12, S. 165 f.]. Hier ist allerdings zu beachten, dass eine Farbfehlsichtigkeit, wie Rot-Grün-Schwäche,

die Lenkungswirkung nullifiziert oder verzerrt. Deshalb sollte Farbe nicht als alleiniges Mittel der Aufmerksamkeitssteuerung verwendet werden. So sollten zusätzliche Reize zur Orientierung gegeben werden [MR17, S. 110 f.]. Dies können Pfeile oder andere Hervorhebungen sein. Dabei ist das Einbringen von Reizen effektiver als das Ausblenden [ebd.]. Besonders dynamische Effekte wie das Blinken oder Drehen von Objekten werden als starke Aufmerksamkeitsfänger angesehen [Hei12, S. 167]. Bei Blinkeffekten sollte eine Blinkfrequenz von unter 3 Hz verwendet werden, um schädliche Auswirkungen auf Lernende mit Epilepsie zu vermeiden [ebd.].

Bei der auditiven Aufmerksamkeit soll die Aufmerksamkeit auf gegebene auditive Reize, wie gesprochene Erklärungen, fokussiert werden. Um den vollen Informationsgehalt von auditiven Informationen aufnehmen zu können, sollten auditive Reize nicht gleichzeitig gegeben werden, da nur der Inhalt einer Nachricht gleichzeitig erfasst werden kann [MR17, S. 105 f.]. Da die nicht beachteten eingehenden Reize jedoch trotzdem abgeschwächt verarbeitet und weitergeleitet werden [MR17, S. 108] und damit Verarbeitungskapazität in Anspruch nehmen, sollte nur der gewünschte Lerninhalt durch die auditiven Reize übermittelt werden, also keine weiteren Stimuli in den Audiospuren des E-Learnings zu finden sein. Dies umfasst unter anderem Hintergrundmusik und Störgeräusche.

2.2.4. Multimedialität

Multimedia bezeichnet die Darstellung von Informationen durch unterschiedliche Kodierungsmöglichkeiten in einem Medium. Beispielsweise die Verwendung von Texten, Grafiken und Audio in einem Medium. Der Lernerfolg bei der Verwendung von mutimedialen Lernmaterialien ist generell höher als die Nutzung von monomedialen Inhalten [WM09, S. 114]. Dies ist damit zu begründen, dass bei der Verarbeitung von Informationen unterschiedlicher Kodierung über unterschiedliche Kanäle verarbeitet wird. Die so erhaltenen mentalen Repräsentationen der Information tragen dann gemeinsam zur Konstruktion eines mentalen Modells des Lerninhaltes bei [WM09, S. 115]. Hierbei müssen allerdings auch alle angebotenen Kodierungen von den Lernenden genutzt werden. Um positive Effekte erzielen zu können, müssen allerdings bei der Gestaltung der Medien einige Dinge berücksichtigt werden, neben Grundsätzen wie Lesbarkeit von Schriften. So sollten Texte nicht in Kombination mit Videos oder Animationen auftreten, da durch den sog. Split-Attention-Effect, welcher durch die begrenzte Verarbeitungskapazität des kognitiven Systems der Lernenden

bedingt ist, Teile der Medien nicht verarbeitet werden können [WM09, S.117]. Bei der Verwendung von Animationen wird empfohlen die einzelnen Teilschritte durch eine Narrative zu verbinden [RPY18, S. 10], um Lernende bei dem Verstehen von den Zusammenhängen zwischen den Teilschritten zu unterstützen. Ein weiterer Effekt, welcher bei der Gestaltung multimedialer Inhalte genutzt werden kann, ist der sog. Modalitätseffekt. Dieser besagt, dass die maximale kognitive piktoriale und textuelle Verarbeitungskapazität genutzt werden kann, wenn gesprochene Texte zusammen mit passenden Abbildungen gegeben werden [WM09, S. 118]. Bei all diesen Effekten sollte allerdings nicht die maximale Kapazität des Arbeitsgedächtnisses außer Acht gelassen werden.

2.2.5. Evaluationsmodelle für E-Learning

Evaluation hat im Allgemeinen die Aufgabe, Wissen zur Bewertung eines Sachverhalts zu sammeln, um dadurch Entscheidungen über diesen Sachverhalt vorzubereiten [NW20, S. 548]. Im Kontext von E-Learnings sollen die Usability der verwendeten Medien, die genutzten Lernformen, -strategien und -erfolge, sowie die Effektivität der Mediendidaktik evaluiert werden [NW20, S. 551]. Dadurch soll die Qualität und Wirksamkeit von digitalen Lernangeboten gemessen werden und Möglichkeiten der Verbesserung oder auch Daten für die zukünftige Entwicklung von neuen Lernmedien gesammelt werden. Für die Evaluation existieren verschiedene Modelle, wie den Goal-Free Evaluation Approach nach Scriven und das PDPP Evaluation Model nach Zhang und Chang. Der Goal-Free Evaluation Approach evaluiert nach dem Erreichen der Ziele eines Projektes im Vergleich zu den vorgesehenen Zielen [Tud14, S. 13 f.]. Das PDPP Evaluation Model ist nach den vier durchzuführenden Aktivitäten während der Evaluation benannt: Planning Evaluation, Development Evaluation, Process Evaluation und Product Evaluation [ZC12, S. 4]. Während jedem dieser Schritte werden dann unterschiedliche Faktoren evaluiert. Ein Schema dieses Vorgehens kann in Abb. 2.5 eingesehen werden.

Neben diesen wird auch das **Kirkpatrick/Phillips-Modell** verwendet. Nach diesem Model sollen Daten auf fünf unterschiedlichen Ebenen erfasst werden, um die Wirksamkeit von Schulungen nachzuweisen [JSC21, S. 43 f.]. Die erste Ebene ist die **Reaction**. Sie befasst sich mit der direkten Reaktion von Lernenden auf das Training. Die zweite Ebene, das **Learning**, beschreibt den Zuwachs von Wissen und Fähigkeiten durch das Training. Auf der dritten Ebene, dem **Behavior**, wird der Transfer des

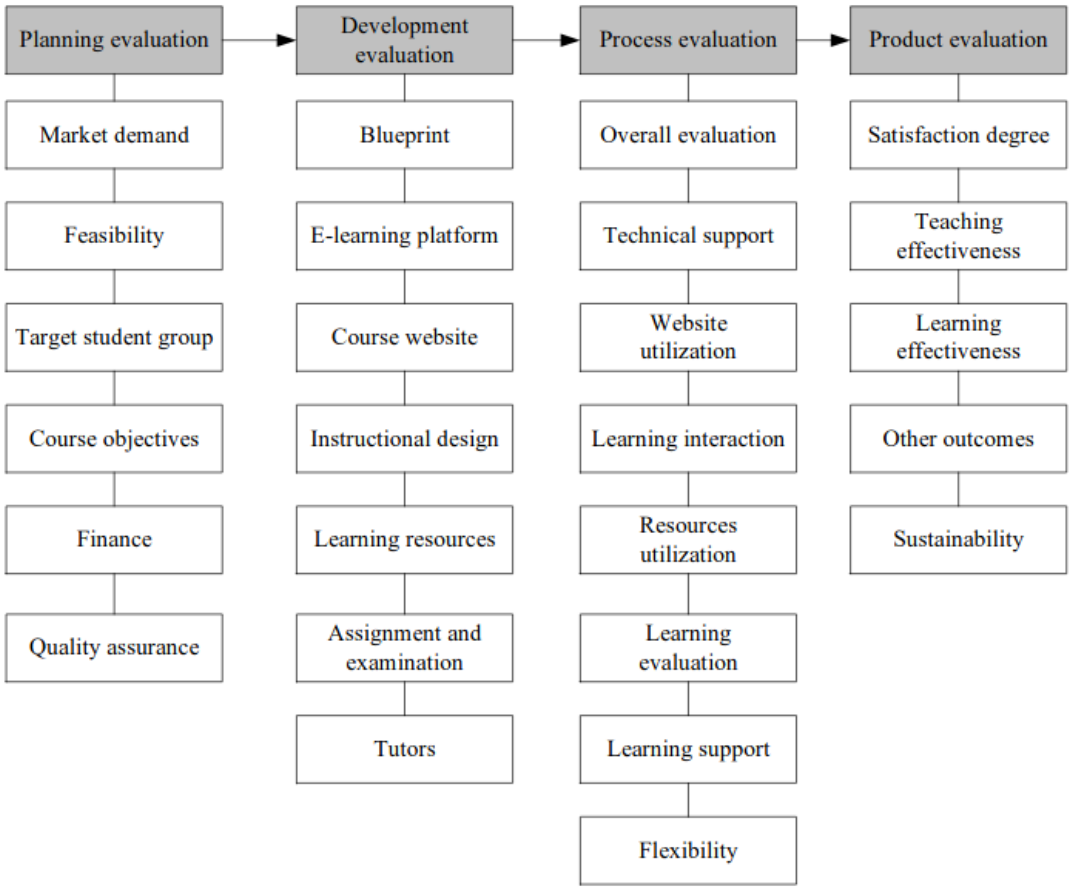


Abbildung 2.5.: Schematische Übersicht über das PDPP Evaluation Model. Quelle: [ZC12, S. 4]

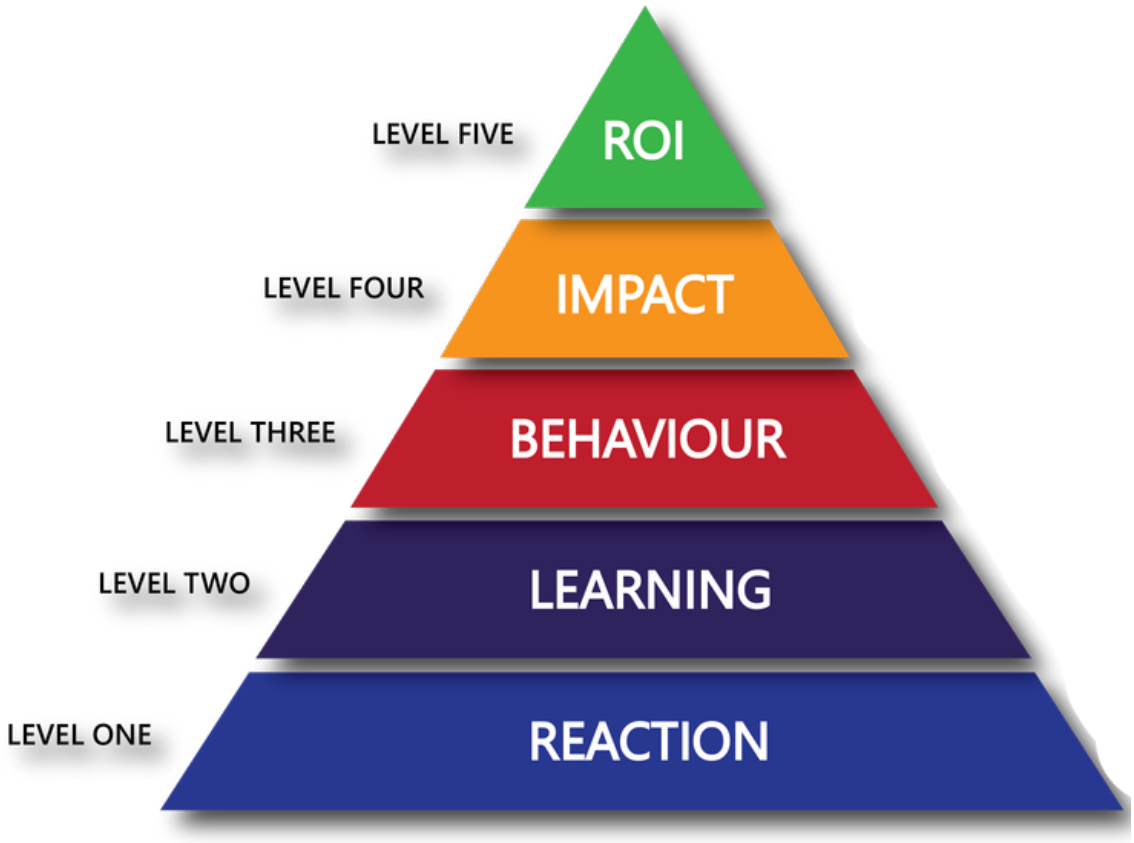


Abbildung 2.6.: Die fünf Ebenen der Evaluation von Trainings nach dem Kirkpatrick/Phillips-Modell. Bearbeitet nach [Ltd18]

Gelernten gemessen, dabei wird die Anwendung im Alltag der Lernenden betrachtet. Die folgende Ebene, die **Results**, manchmal auch als Impact bezeichnet, evaluiert den Einfluss auf die Organisation, welche das Training durchführt, bzw. deren Mitglieder, welche an dem Training teilnehmen. Die letzte Ebene **Return on investment**, bezieht sich vorallem auf wirtschaftliche Organisationen und evaluiert monetäre Vorteile, welche durch die Durchführung des Trainings entstehen und setzt diese mit den Kosten für das Training in Verhältnis [JSC21, S. 43 f.]. Eine grafische Darstellung dieser Ebenen kann in Abb. 2.6 eingesehen werden.

3. Analyse und Konzeption

Nun soll das Konzept des E-Learning-Moduls erstellt werden. Allgemein soll das Modul als ein Web-based Training (WBT) umgesetzt werden. Dieses Format wurde gewählt, da es auf technischer Seite eine Unabhängigkeit von den Betriebssystemen der Lernenden ermöglicht und multimediale Inhalte verwendet werden können. Aus Sicht des Lernens haben WBTs den Vorteil, dass Testitems verwendet werden können, welche Feeback zum Lernfortschritt geben, das psychologische Grundbedürfnis nach sozialer Eingebundenheit erfüllen und in Form eines Abschlusstests zur Evaluation des Lernerfolges verwendet werden können. Neben diesen Faktoren sind WBTs für Lernende praktisch, da sie sich keine Software installieren müssen und von jedem internetfähigen Gerät aus das Modul bearbeiten können. Zusätzlich sind WBTs in deutschen Unternehmen verbreitet, sodass Lernende entweder bereits Erfahrung mit solchen Angeboten haben oder hier in ersten Kontakt mit WBTs treten können und Erfahrung für das spätere Berufsleben sammeln können.

Die Inhalte des Moduls wurden auf Basis der in Kapitel 2.1 erarbeiteten Grundlagen gewählt. Es soll allgemein in die IT-Sicherheit mit ihrer Motivation, Zielstellung und Methoden eingeführt werden. Daneben sollen Nutzende für die Sicherheit, welche von Passwörtern und Verschlüsselung erzeugt wird, sensibilisiert und entsprechende Kompetenzen zur Wahl von starken Passwörtern, sowie dem sicheren Umgang mit ihnen vermittelt werden. Im Bereich der Verschlüsselung soll Grundlagenwissen, Handlungskompetenz zur Verschlüsselung von E-Mails und Wissen zur Einordnung der Nutzung kryptographischer Verfahren erlangt werden. Daneben sollen im Modul aktuell relevante Bedrohungen besprochen werden. Nutzende sollen Kompetenzen erlangen Phishing-Angriffe selbstständig zu erkennen. Daneben soll auch auf die Bedrohung durch Malware aufmerksam gemacht werden. Hier soll Grundlagenwissen vermittelt und Handlungskompetenz zur Prävention und Beseitigung von Infektionen vermittelt werden.

Zur Erstellung des Konzepts folgt zunächst eine Anforderungsanalyse, um die funktionalen und nicht-funktionalen Anforderungen beschreiben zu können. Darauf folgt

Code	Anforderung
FA1	Das Modul muss Lernenden den Aufruf der Lerninhalte ermöglichen
FA2	Das Modul muss Lernenden ermöglichen zwischen den Lernelementen zu navigieren
FA3	Das Modul muss multimediale Inhalte wiedergeben können
FA4	Das Modul muss Lernenden ermöglichen Tests durchzuführen
FA5	Das Modul muss die Verwendung von Hyperlinks ermöglichen

Tabelle 3.1.: Funktionale Anforderungen

die Struktur des Moduls, die Konzeption der Inhalte und abschließend das Konzept zur technischen Umsetzung.

3.1. Anforderungsanalyse

Im Folgenden wird die Anforderungsanalyse durchgeführt. Es werden dabei zunächst die funktionalen Anforderungen beschrieben. Unter funktionalen Anforderungen werden die erforderlichen Funktionalitäten einer Software verstanden [Bal11, S. 109]. Anschließend folgt eine Beschreibung der nicht-funktionalen Anforderungen. Diese legen fest, auf welche Weise die Funktionalität erfüllt werden soll (ebd.).

3.1.1. Funktionale Anforderungen

Nun folgen die funktionalen Anforderungen. Sie können in Tab. 3.1 eingesehen werden. **FA1** beschreibt eine grundlegende Anforderung an das Modul, da ohne die Möglichkeit auf die zur Verfügung gestellten Lernmaterialien zugreifen zu können kein Kompetenzerwerb stattfinden kann. Deshalb muss das Modul den Lernenden ermöglichen auf die gewünschten Inhalte zuzugreifen. In **FA2** wird die Anforderung an eine Möglichkeit zwischen den einzelnen Inhalten zu wechseln beschrieben, dazu soll es eine Navigationsfunktion geben. Die Anforderung **FA3** ist notwendig, da zur Nutzung positiver Einflüsse auf das Lernen durch Multimedialität, welche in Kap. 2.2.4 näher beschrieben sind, die Verwendung verschiedener Medientypen im Modul möglich sein muss. Es soll möglich sein Texte, Grafiken und Videos mit Audiospuren

Code	Anforderung
NA1	Das Modul muss auch für Personen mit wenig Erfahrung im Umgang mit digitalen Systemen gut benutzbar sein
NA2	Das Modul muss die Kompetenz im Bereich der IT-Sicherheit der Nutzenden verbessern

Tabelle 3.2.: Nicht-Funktionale Anforderungen

abzuspielen. Damit Lernende ihren Fortschritt bei der Kompetenzentwicklung bewerten können, Feedback erhalten und eine Evaluierung des gesamten Lernerfolges durch einen Abschlusstest möglich wird, müssen Tests verwendet werden können, dies wird in **FA4** beschrieben. Die letzte funktionale Anforderun, **FA5**, sieht die Verwendung von Hyperlinks vor, da zur Erfüllung des psychologischen Grundbedürfnisses der Autonomie Lernende auf externe Materialien zugreifen können sollen. Dabei sollen hier nur weiterführende Inhalte, welche Lernende bei besonderem Interesse bei einem Thema sichten können, verlinkt werden. Die verlinkten Inhalte werden nicht in Test abgefragt.

3.1.2. Nicht-Funktionale Anforderungen

Hier sollen die nicht-funktionalen Anforderungen beschrieben werden. Sie können in Tab. 3.2 eingesehen werden. Die Anforderung **NA1** soll sicherstellen, dass eine gute Usability vorhanden ist. Dies ist besonders relevant, da die Zielgruppe dieses WBTs Endanwendende mit geringen digitalen Fähigkeiten sind. Deshalb muss auch die Bedienbarkeit des Moduls für ebendiese Gruppe gewährleistet sein. Anforderung **NA2** ist das eigentliche Ziel dieser Arbeit. Nach dem Abschluss des Moduls sollen Lernende über ein Mindestmaß an digitalen Kompetenzen im Bereich der IT-Sicherheit verfügen. Der Zuwachs an Kompetenz soll durch den Abschlusstest nachgewiesen werden.

3.2. Struktur des Moduls

Das Modul ist in 5 Kapitel unterteilt. Jedes dieser Kapitel behandelt einen Themenblock der IT-Sicherheit. Zusätzlich ist den Themenblöcken ein Kapitel vorgelagert, welches die Motivation des Moduls darlegt und Lernenden die Relevanz des Themas IT-Sicherheit näherbringen soll. Zu Beginn des Moduls ist ein Instruktionsvideo zu finden, welches die allgemeine Benutzung des Moduls erklärt, daneben soll die Verwendung der Ergebnisse des Abschlusstests im Rahmen der Evaluation mit entsprechender Anonymisierung erläutert werden. Die Themenblöcke sind linear aufeinander folgend, allerdings können Lernende jederzeit auf jeden Block zugreifen. Hierdurch soll das psychologische Grundbedürfnis der Autonomie erfüllt werden, dadurch sollen positive Emotionen erzeugt und eine motiviationssteigernde Wirkung erzielt werden, für Details siehe Kap. 2.2.3. Am Ende jedes Themenblocks soll sich ein Selbsttest finden, welcher abprüft, ob die Lernziele erreicht wurden. Diese können Wissensfragen oder auch kleine Übungsaufgaben enthalten. Dadurch kann einerseits das psychologische Grundbedürfnis der Kompetenz erfüllt werden, andererseits kann hier ein Feedback gegeben werden. So werden Lernende für das erfolgreiche Lösen gelobt und erhalten zusätzliche Erklärungen, wenn eine Aufgabe nicht gelöst werden konnte. Zusätzlich sollen weiterführende Materialien verlinkt werden, welche sich Lernende bei Interesse optional ansehen können. Im Folgenden werden die einzelnen Themenblöcke vorgestellt.

3.2.1. Einleitung

In diesem Kapitel wird zunächst grundlegend in die IT-Sicherheit eingeführt. Zunächst findet dabei eine Definition statt. Zur Steigerung der intrinsischen Motivation der Lernenden wird danach aufgezeigt, dass die IT-Sicherheit eine praktische Relevanz hat, dazu werden Erkenntnisse und Beispiele aus Kap 2.1.1 aufgeführt. Ebenfalls zur motivationssteigerung soll danach anhand einer Analogie gezeigt werden, dass die IT-Sicherheit eine geteilte Verantwortung ist und die Lernenden selbst einen Teil zur Sicherheit beitragen. Eine schematische Darstellung der Struktur kann in Tab. 3.3 eingesehen werden.

Titel	Medientyp	Inhalt
Was ist IT-Sicherheit?	Video	Definition des Begriffs "IT-Sicherheit", Beschreibung der Schutzziele und der Aufgaben
Praktische Relevanz	Video	Darstellung aktueller Bedrohungslage basierend auf Kap. 2.1.1, Vorstellung vergangener Sicherheitsvorfälle
Verantwortung	Video	Erklärung der geteilten Verantwortung durch eine Analogie
Zwischentest	Test	Fragen zur Wiederholung des Gelernten

Tabelle 3.3.: Struktur des Kapitels "Einleitung"

3.2.2. Passwörter

Das zweite Kapitel beschäftigt sich mit dem Thema Passwörter. Zur Steigerung der Motivation soll die Relevanz der Passwörter für die IT-Sicherheit hervorgehoben werden. Als Wissen für die Einordnung von Passwörtern soll der Prozess der Authentifizierung durch Passwörter erklärt werden. Anschließend wird konkret vermittelt, welche Faktoren ein starkes Passwort ausmachen und die Kompetenz zur Wahl eines solchen Passworts vermittelt. Um das Verständnis der Faktoren eines starken Passwortes zu verbessern sollen Lernende anschließend mit Passwörtern experimentieren können. Zum Abschluss sollen Lernende für den sicheren Umgang mit Passwörtern sensibilisiert werden. Die Struktur dieses Kapitels kann in Tab. 3.4 eingesehen werden.

3.2.3. Phishing

Im dritten Kapitel wird das Thema Phishing behandelt. Zu Beginn wird zunächst das Ziel und der allgemeine Ablauf von Phishing-Angriffen aufgezeigt. Dabei wird Bezug zum "Fappening"-Vorfall genommen, um die praktische Relevanz dieses Kapitels zu verdeutlichen. Anschließend wird zur Vertiefung dieser Theorie ein Phishing-Angriff anhand einer konkret erhaltenen Phishing-Mail demonstriert. Darauf folgt ein Abschnitt, welcher konkrete Handlungskompetenz zum Erkennen solcher Angriffe vermitteln soll. Anschließend soll die Zwei-Faktor-Authentifikation als eine mögliche

Titel	Medientyp	Inhalt
Funktion von Passwörtern	Video	Erklärung der Funktion von Passwörtern und des Prozesses der Authentifizierung
Ein starkes Passwort	Video	Faktoren von starken Passwörtern, Wahl eines starken Passwortes
Passwörter Experiment	Interaktives Element	Lernende können mit verschiedenen Passwörtern experimentieren, um den Einfluss von unterschiedlichen Faktoren auf die Sicherheit eines Passwortes zu erfahren.
Umgang mit Passwörtern	Video	Sicherer Umgang mit Passwörtern
Zwischentest	Test	Fragen zur Wiederholung des Gelernten

Tabelle 3.4.: Struktur des Kapitels "Passwörter"

Gegenmaßnahme vorgestellt werden, um Lernenden zusätzliches Wissen zur Abwehr von Phishing-Angriffen zu vermitteln. Eine Darstellung der Struktur dieses Kapitels kann in Tab. 3.5 eingesehen werden.

3.2.4. Verschlüsselung

Verschlüsselung ist das Thema des vierten Kapitels. Dabei werden zunächst die Grundlagen vermittelt, das allgemeine Verfahren, die Zielstellung, Schlüssel und die Unterscheidung zwischen symmetrischer und asymmetrischer Verschlüsselung. Anschließend werden die abstrakten Konzepte von Verschlüsselung und Schlüssel anhand einer Demonstration veranschaulicht, um ein besseres Verständnis zu erreichen. Es folgt ein Video, welches mögliche Anwendungen der Verschlüsselung zeigt. Danach folgt ein Videotutorial, welches konkret zeigt, wie eine E-Mail verschlüsselt werden kann. Anschließend wird noch HTTPS erläutert und mit Bezug auf das vorherige Kapitel erklärt, dass HTTPS kein Schutz vor Phishing ist.

Titel	**Medientyp**	**Inhalt**
Was ist Phishing?	Video	Erklärung des Ablaufes und der Zielstellung von Phishing
Demonstration	Video	Ein Phishing-Angriff wird demonstriert
Erkennung von Phishing	Video	Grundlegender Aufbau von URLs, Erkennung von Phishing Mails, Erkennung gefälschter Webseiten
Zwei-Faktor-Authentifikation	Video	Zwei-Faktor-Authentifikation wird als eine Gegenmaßnahme vorgestellt.
Zwischentest	Test	Fragen zur Wiederholung des Gelernten

Tabelle 3.5.: Struktur des Kapitels "Phishing"

Titel	**Medientyp**	**Inhalt**
Einführung	Video	Grundlegendes Verfahren, Erklärung von Schlüsseln
Demonstration	Video	Der Ablauf von Ver- und Entschlüsselungsprozessen, sowie die Funktion von Schlüsseln wird durch eine einfache Funktion demonstriert.
Anwendung	Video	Verschiedene Anwendungen von Verschlüsselung werden aufgezeigt
Tutorial: E-Mail Verschlüsselung	Video	Der konkrete Ablauf der Verschlüsselung einer E-Mail wird gezeigt.
HTTPS	Video	HTTPS und seine Bedeutung wird erklärt
Zwischentest	Test	Fragen zur Wiederholung des Gelernten

Tabelle 3.6.: Struktur des Kapitels "Verschlüsselung"

Titel	Medientyp	Inhalt
Was ist Malware?	Video	Definition und Klassifizierung, Vorstellung einiger Vertreter
Angriffsvektoren	Video	Darstellung möglicher Angriffvektoren
Datentypen	Text	Es werden verschiedene Datentypen und deren Relevanz der IT-Sicherheit aufgezeigt
Prävention	Video	Es werden präventive Maßnahmen gegen Malware gezeigt
Infektion: Was tun?	Video	Maßnahmen bei einer Malware-Infektion
Diskussion: AntiVirus-Programme	Video	Möglichkeiten und Problematiken von Anti-Malware-Software werden vorgestellt
Zwischentest	Test	Fragen zur Wiederholung des Gelernten

Tabelle 3.7.: Struktur des Kapitels "Malware"

3.2.5. Malware

Schlussendlich wird im fünften Kapitel das Thema Malware behandelt. Zu Beginn wird der Begriff definiert und die möglichen Klassifikationen aufgezeigt. Anschließend werden mögliche Angriffsvektoren behandelt. Danach folgt ein Cheetsheat, welches verschiedene häufig verwendete Datentypen erklärt und deren Bedrohungspotential einschätzt. Dies ist nicht nur für das folgende Kapitel, sondern auch für die Entwicklung von Datenkompetenz relevant. Im nachfolgenden Kapitel werden mögliche Präventivmaßnahmen gezeigt. Dabei werden die vorher erwähnten Angriffvektoren betrachtet und Maßnahmen durch Infektion durch verschiedene Datentypen, welche u.a. per Mail verschickt werden, besprochen. Anschließend werden Möglichkeiten im Falle einer Infektion aufgezeigt. Dabei sollen Lernende verstehen, dass das vollständige Entfernen einer Infektion mit großem Aufwand verbunden ist, um die Bedeutung der Prävention hervozuheben. Zum Abschluss des Kapitels wird konkret über Anti-Malware-Software gesprochen und die Möglichkeiten, Limitationen und mögliche Gefahren solcher Software erörtert.

3.2.6. Abschlusstest

Das Ende des Moduls bildet der Abschlusstest. Hierbei sollen Lernende Fragen aus allen vorherigen Bereichen beantworten.

3.3. Konzeption der Inhalte

Nun werden die Inhalte konzipiert. Visuelle Inhalte sollen allgemein aufgeräumt und frei von Ablenkungen präsentiert werden. Dabei sollen möglichst wenige, aber aussagekräftige Inhalte auf einmal gezeigt werden. Dies dient der Vermeidung der Überlastung des Arbeitsgedächtnisses. Bei auditiven Inhalten soll auf eine angenehme Lautstärke und die Vermeidung von Störgeräuschen geachtet werden. Durch das Verwenden von eingesprochenen Texten, soll das psychologische Grundbedürfnis der sozialen Eingebundenheit zur Steigerung der Motivation erfüllt werden. Um positive Emotionen hervorzurufen soll im Modul allgemein Humor verwendet werden, dabei soll allerdings keine Übertreibung stattfinden, um zu verhindern, dass die Emotion zuviele kognitive Ressourcen einnimmt.

Die Inhalte werden in vier unterschiedlichen Medientypen dargestellt werden. Bei **Videos** werden verschiedene Situationen aufgenommen und mit einer erklärenden Audiospur hinterlegt. Dabei können Präsentationen aufgenommen werden. Dies dient der Vermittlung von erforderlichen Grundlagen. Um den Modalitätseffekt (siehe Kap. 2.2.4) zu nutzen, sollen die Präsentationen möglichst wenig Text enthalten. Stattdessen sollen hier überwiegend Abbildungen verwendet werden. Andere Möglichkeiten sind die Aufnahme von Software, für entsprechende Tutorials, oder Demonstrationen. Da bei der Aufnahme von Software nicht gewährleistet werden kann, dass Übersichtlichkeit und Aufgeräumtheit vorhanden sind, sollen hier relevante Stellen durch den Mauszeiger und das Markieren relevanter Texte, sofern möglich, hervorgehoben werden.

Texte dienen hier zur Vermittlung von Informationen, welche nicht für die Videoform geeignet sind. Daneben werden sie als sog. Cheat-Sheets ausgegeben. Bei Texten soll stets ein weißer Hintergrund und eine schwarze Schrift verwendet werden, um Lesbarkeit sicherzustellen. Die Schriftgröße wird entsprechend groß gewählt.

Bei einem **interaktiven Element** handelt es sich um einen Abschnitt des Moduls, in welchem Lernende durch interaktive Übungen das Gelernte vertiefen können. Die konkrete Ausgestaltung hängt hier von dem konkreten Element ab.

Tests dienen der Kontrolle des Lernfortschritts und dem Erhalten von Feedback. Hierbei können unterschiedliche Arten von Wissenskontrollen durchgeführt werden. Unter diese fallen u.a. Multiple- und Single-Choice-Fragen. Die Tests können als Zwischentests, welche am Ende eines Kapitels angesiedelt sind und sich nur auf das entsprechende Kapitel beziehen, und als Vor- bzw. Abschlusstest, welche für die Evaluation des Lernerfolges genutzt werden, durchgeführt werden.

Zusätzlich sollen weiterführende Informationen zu bestimmten Themen verlinkt werden. Dabei soll es sich um ein freiwilliges Zusatzangebot handeln, welches Lernende bei besonderem Interesse nutzen können. Die verlinkten Inhalte werden nicht in den Tests abgefragt, können aber zu einem besseren Verständnis des Gelernten beitragen. Diese Verlinkungen dienen der Erfüllung des psychologischen Grundebürfnisses der Autonomie und zu einem kleinen Teil der Kompetenz.

Nun werden in Inhalte im Einzelnen nach der in Kap. 3.2 aufgezeigten Reihenfolge konzipiert.

3.3.1. Einleitung

Was ist IT-Sicherheit? Hier soll ein Video erstellt werden. Es wird die Titelfrage gestellt und im Folgenden beantwortet. Dabei wird die Aufgabe der IT-Sicherheit, sowie die Schutzziele vorgestellt. Das Video dient der Vermittlung von Grundlagenwissen, auf welches sich in den späteren Kapiteln bezogen wird. Die Lernziele sind die Vermittlung des Wissens zur Definition des Begriffs IT-Sicherheit und der Bennenung und Beschreibung der fünf Schutzziele.

Praktische Relevanz Es soll ein Video in gleicher Manier wie in dem vorhergehenden Kapitel erstellt werden. Hier werden zunächst einige Auszüge von Statistiken aus der Bitkom-Studie (siehe [BS21]), dem Lagebericht des BSI (siehe [BSI21]) und der IBM Security X-Force Threat Intelligence (siehe [IBM22]) vorgestellt und erläutert. Da diese Folien viel Inhalt haben werden, soll einerseits Relevantes hervorgehoben

werden und andererseits den Lernenden ausreichend Zeit gegeben werden, diese Auszüge zu sichten. Abschließend sollen kurz zwei Sicherheitsvorfälle erwähnt werden. Dabei soll es um die WannaCry Ransomware und The Fappening gehen, um darzustellen, dass IT-Sicherheit sowohl für Unternehmen, als auch für Privatpersonen von Relvanz ist. Dies dient der Steigerung der Motivation, da für Lernende so die Relevanz der IT-Sicherheit für ihren Alltag sichtbar wird. Falls weiteres Interesse seitens der Lernenden besteht, sollen zusätzlich Hyperlinks zu weiteren Informationen zu diesen Vorfällen gegeben werden. Nach der Sichtung des Videos sollen Lernende einen Überblick über die Bedrohungslage haben, verstehen, dass die IT-Sicherheit sowohl für Unternehmen als auch für Privatpersonen relevant ist und die Begriffe "WannaCry" und "The Fappening" einordnen können.

Verantwortung In diesem Video soll Lernenden erklärt werden, dass IT-Sicherheit eine geteilte Verantwortung verschiedener Parteien ist. Dazu wird eine Analogie der Sicherheit im Straßenverkehr aufgegriffen, um dieses Prinzip in einem bekannten Kontext vorzustellen. Da Sicherheit im Straßenverkehr durch die gemeinsame Verantwortung von Verkehrsteilnemenden, der Wartung von Straßen und Fahrzeugen, Verkehrssteuerung und Gesetzen ensteht. Dieses Prinzip wird dann auf die IT-Sicherheit übertragen, da dort die Sicherheit durch das Zusammenspiel von Softwareentwicklung, Administration, Hardwareproduzierenden und Endnutzenden zustande kommt. So soll die Motivation der Lernenden gesteigert werden, da diese erfahren, dass sie einen Teil der Verantwortung tragen und zumindest das Verstehen der Grundlagen der IT-Sicherheit ein hilfreiches Mittel zur Erfüllung dieser Verantwortung ist. Hier sollen Lernende verstehen, dass IT-Sicherheit eine geteilte Verantwortung ist und diesen Begriff erklären können. Zudem sollen Lernende die Verantwortlichen für die IT-Sicherheit benennen können.

Zwischentest Der Zwischentest soll hier ein Feedback zum Lernerfolg des ersten Kapitels geben. Dazu wird zu jedem vorhergehendem Abschnitt Fragen gestellt. Hier werden vier Fragen gestellt. Hier wird exemplarisch der Zwischentest für das erste Kapitel gezeigt werden. Die Konzepte für die Zwischentests der anderen Kapitel sind in der gleichen Art konzipiert und können aus Gründen der Übersichtlichkeit in Anhang B eingesehen werden.

Zunächst soll Grundlagenwissen über IT-Sicherheit abgeprüft werden. Dazu werden zwei Fragen gestellt:

Zuerst sollen Lernende in einer Single-Choice-Frage die passende Definition auswählen.

Welche Definition von IT-Sicherheit ist korrekt?

- *Schutz sämtlicher Geheimnisse eines Unternehmens vor Verlust oder Diebstahl*
- *Schutz von Computern, Smartphones und anderen Geräten vor Vandalismus, Verlust oder Beschädigung*
- *Schutz von Computersystemen und darauf befindlichen Daten vor Verlust, Zerstörung, Manipulation und Zugriff durch dritte, welche digitale Angriffsvektoren nutzen*
- *Schutz von Netzwerken und ihren Daten vor unterschiedlichen Angriffen aus dem Internet.*

Danach werden Erklärungen der fünf Schutzziele gegeben und Lernende sollen aus einer Liste möglicher Antworten, welche auch irrelevante Begriffe enthält, die korrekten zuordnen.

Welche Begriffe sind jeweils gemeint?

- *Echtheit von Objekten und Subjekten*
- *Daten sind sicher vor Manipulation*
- *Nur ausgewählte Personen können einen Text lesen*
- *Der Dienst kann ohne Einschränkungen verwendet werden*
- *Die Aktionen von Nutzenden können ihnen zugeordnet werden*

Die Liste der Antwortmöglichkeiten enthält folgende Begriffe, die irrelevanten sind kursiv geschrieben:

1. Authentizität
2. Integrität
3. *Integration*
4. Vertraulichkeit
5. *Autorität*

6. Verfügbarkeit
7. Verbindlichkeit
8. *Nachprüfbarkeit*

Es folgt eine Frage zur praktischen Relevanz. Hier soll in einer Single-Choice-Frage die richtige Antwort gewählt werden.

Für wen ist IT-Sicherheit relevant?

- *Große Unternehmen mit vielen vertraulichen Daten*
- *Sicherheitsexperten*
- *Jede Person, welche ein digitales Gerät nutzt*
- *Polizei, Gerichte und Regierung*

Die letzte Frage bezieht sich auf die Verantwortung für IT-Sicherheit. Hier soll im Multiple-Choice-Verfahren aus einer Liste die Verantwortlichen Stellen ausgewählt werden. Diese sind die folgenden, auch hier sind die falschen Antworten kursiv:

Wer trägt Verantwortung für die IT-Sicherheit?

- Administration
- Endanwendende
- *Autofahrende*
- Gesetzgebung
- Softwareentwicklung
- *Chuck Norris*
- *Bauamt*
- *Der öffentlich-rechtliche Rundfunk*

3.3.2. Passwörter

Funktion von Passwörtern Hier soll ein Video erstellt werden, welches eine Einführung in das Thema Passwörter gibt. Dabei wird Lernenden erklärt, dass Passwörter der der Authentizität dienen und dass ein starkes Passwort bereits zu erhöhter Sicherheit führen kann. Dabei soll ein Bezug zur geteilten Verantwortung der IT-Sicherheit gemacht werden, um darzustellen, dass Passwörter Teil der Verantwortung sind. Dies soll dazu dienen den motivationalen Effekt der geteilten Verantwortung für dieses Kapitel zu nutzen. Zusätzlich soll schematisch der Prozess der Authentifizierung gezeigt werden, um technisches Hintergrundwissen zu vermitteln. Die Lernenden sollen nach Bearbeitung dieses Abschnittes den Einfluss von Passwörtern auf die IT-Sicherheit verstehen und den Prozess der Authentifizierung beschreiben können.

Ein starkes Passwort In diesem Video soll konkrete Handlungskompetenz zur Wahl starker Passwörter vermittelt werden. Dazu wird zunächst der Einfluss der Länge und der Anzahl verwendeter unterschiedlicher Zeichen auf die Sicherheit des Passworts erklärt. Anschließend soll exemplarisch eine Passwortliste gezeigt werden, um Lernenden einige Negativbeispiele aufzuzeigen. Es soll eine Erklärung folgen, dass diese schwachen Passwörter oft gewählt werden, da sie leicht zu merken sind. Dabei soll auf das Spannungsfeld zwischen der Sicherheit eines Passwortes und der Merkbarkeit hervorgehoben werden. Auf Basis dieser Überlegungen soll Lernenden eine Methodik zur Wahl sicherer und merkbarer Passwörter durch die Bildung von Sätzen gezeigt werden. Die Lernziele sind das Verstehen der Einflüsse von Länge und unterschiedlicher verwendeter Zeichen auf die Sicherheit eines Passwortes, die Fähigkeit, die Sicherheit eines Passwortes bewerten zu können und eine Methodik zur Wahl sicherer Passwörter erklären zu können.

Passwörter Experiment Dieses interaktive Element soll Lernenden die Möglichkeit geben, den Einfluss von Länge und Größe des Zeichensatzes auf die Sicherheit eines Passwortes nachvollziehen zu können. Dabei werden Lernenden drei Passwörter vorgegeben. Dabei handelt es sich um eine vierstellige Zahlenfolge, eine sechstellige Zahlenfolge und eine vierstellige Kombination aus Zahlen und Buchstaben. Lernende sollen dabei versuchen die drei Passwörter zu erraten. Dadurch soll verdeutlicht wer-

den, dass die Länge eines Passwortes maßgeblich für dessen Sicherheit ist. Lernziel davon ist die Vertiefung von Faktoren eines sicheren Passwortes.

Umgang mit Passwörtern In diesem Abschnitt des Moduls sollen Lernende in den sicheren Umgang mit Passwörtern eingeführt werden. Dazu sollen in einer humorvoll gestalteten Collage Negativbeispiele aufgezeigt werden. Lernende sollen sensibilisiert werden, dass die Speicherung von Passwörtern auf einem Computer oder die Notiz von eben diesen den Sinn von Passwörtern untergräbt. Zum Abschluss soll kurz auf Passwortmanagement-Software eingegangen werden und diese diskutiert werden, um einen möglichen Ansatz zur Verwaltung vieler unterschiedlicher Passwörter aufzuzeigen und Lernenden das Wissen zu geben, welches notwendig ist, um dessen Wirksamkeit, sowie Einfluss auf die Sicherheit bewerten zu können. Die Lernziele sind die Beherrschung des sicheren Umgangs mit Passwörtern, das Kennen des negativen Einflusses der Speicherung von Passwörtern und das Kennen und die Einordnung von Passwortmanagement-Software.

3.3.3. Phishing

Was ist Phishing? Dieses Video soll eine Einleitung zum Thema Phishing werden. Zur Herstellung eines Praxisbezuges soll als Einführung der Fappening-Vorfall aufgegriffen werden. Auf dieser Basis sollen die Ziele eines Phishing-Angriffes vermittelt werden. Anschließend wird schematisch der Ablauf eines solchen Angriffes gezeigt. Nach Sichtung dieses Videos sollen Lernende wissen, was ein Phising-Angriff ist, den Ablauf eines solchen Angriffes skizzieren können und die Folgen benennen können.

Demonstration Um die Theorie des vorhergehenden Videos zu veranschaulichen, soll hier eine entsprechende Phishing-Mail geöffnet, auf die entsprechenden Links geklickt und die entsprechende Webseite aufgerufen werden. Dadurch soll bei Lernenden ein tieferes Verständnis für den Ablauf von Phishing-Angriffen erlangt werden.

Erkennung von Phishing In diesem Video sollen Lernende Handlungskompetenz zur Erkennung von Phishing erwerben. Dabei wird zunächst das dazu erforderliche Hintergrundwissen vermittelt. Zunächst wird der Aufbau und die Funktion von URLs erklärt. Fall Lernende weiteres Interesse an dieser Thematik haben, sollen

weiterführende Materialien verlinkt werden. Anschließend wird grob in den technischen Part von E-Mails eingeführt und einige Problematiken hervorgehoben werden, welche Phishing begünstigen. Danach wird praktisch an der Phishing-Mail und der Webseite aus dem vorherigen Video gezeigt, woran hier Phishing erkannt werden kann. Die Lernziele sind das Kennen des grundlegenden Aufbaus von URLs, die Fähigkeit Phishing-Mails anhand verschiedener Merkmale erkennen zu können und gefälschte Webseiten identifizieren zu können.

Zwei-Faktor-Authentifikation Um Lernenden eine mögliche Gegenmaßnahme gegen Phishing aufzuzeigen, soll hier die Zwei-Faktor-Authentifikation vorgestellt werden. Dabei wird zunächst der Ablauf eines Authentifikationverfahrens gezeigt. Anschließend der Ablauf eines solchen Verfahrens mit einem zweiten Fakor. Dabei werden unterschiedliche Möglichkeiten der Realisierung, die Verwendung von Dongles oder auch durch Codes, welche per Mail oder SMS versendet werden, gezeigt. Abschließend werden die Vorteile, aber auch die Limitationen dieses Verfahrens erörtert, dadurch sollen Lernende selbst abschätzen können, ob die Zwei-Faktor-Authentifikation in ihrem Anwendungsfall sinnvoll ist. Durch dieses Video sollen Lernende den Begriff "Zwei-Faktor-Authentifikation" erklären können, den allgemeinen Ablauf kennen und die Einsatzmöglichkeiten in verschiedenen Anwendungsfällen beurteilen können.

3.3.4. Verschlüsselung

Einführung Das einführende Video erklärt Lernenden die Grundlagen, welche für den Kompetenzerwerb in den folgenden Abschnitten notwendig sind. Zunächst wird der Begriff Verschlüsselung allgemein erklärt und der Ablauf erläutert. Anschließend wird der Unterschied zwischen einer symmetrischen und asymmetrischen Verschlüsselung erklärt. Danach folgt eine Erklärung zu Schlüsseln. Die Lernziele dieses Videos sind die Fähigkeit den Begriff "Verschlüsselung" und den Unterschied zwischen symmetrischer und asymmetrischer Verschlüsselung erklären zu können.

Demonstration Da die Konzepte von Verschlüsselung und Schlüsseln sehr abstrakt sind und technisch weniger versierte Lernende mit der rein theoretischen Erklärung vermutlich kein ausreichendes Verständnis von der Verschlüsselung erlangen, soll hier eine Demonstration erfolgen. Dazu soll ein Text durch eine Caesaren-Chiffre

verschlüsselt und anschließend wieder entschlüsselt werden. Dadurch soll einerseits der Ablauf einer Verschlüsselung visualisiert werden und andererseits das Prinzip der Schlüssel aufgezeigt werden. Zur Demonstration wird ein Tool auf der Webseite boxentriq.com verwendet. Dieses wird im Kurs verlinkt, um Lernenden die Möglichkeit zu geben, die Chiffre selbst auszuprobieren. Vor der Demonstration soll die Funktionsweise der Caesaren-Chiffre erläutert werden. Nach Bearbeitung dieses Videos sollen Lernende das Prinzip einer symmetrischen Verschlüsselung verstehen und erklären können, was unter einem Schlüssel verstanden wird.

Anwendung Dieses Video soll Lernenden einige konkrete Anwendungen von Verschlüsselung vorstellen. Dies soll die praktische Relevanz und die Alltäglichkeit der Verschlüsselung aufgezeigen. Außerdem können Lernende hieraus weitere Maßnahmen zur Verbesserung der Vertraulichkeit eigener Daten ableiten. Dabei soll die Verschlüsselung von E-Mails, von Webseiten, das Verschlüsseln von Dateien und das Signieren vorgestellt werden. Die Lernenden sollen nach Sichtung des Videos verschiedene Anwendungen der Verschlüsselung aufzählen können.

Tutorial: E-Mail Verschlüsselung Der im vorherigen Video gezeigte Anwendungsfall der Verschlüsselung einer E-Mail soll nun hier praktisch gezeigt werden. Dabei sollen Lernende die Fähigkeit erwerben, eine solche Verschlüsselung selbst durchführen zu können. Um gewährleisten zu können, dass Lernende die gezeigten Schritte zum Erreichen dieses Ziels auch direkt selbst ausprobieren können, wird im Video die freie Open-Source-Software Thunderbird verwendet. Im Anschluss werden einige Faktoren benannt, welche dabei beachtet werden müssen, wie das sichere Austauschen von Schlüsseln bei einer symmetrischen Verschlüsselung oder die korrekte Verwendung von Schlüsseln bei einer asymmetrischen Verschlüsselung. Die Lernenden sollen wissen, dass eine Verschlüsselung von E-Mails möglich ist und die einzelnen Schritte, welche dazu notwendig sind, aufzählen können.

HTTPS Dieses Video soll Fehleinschätzungen von HTTPS, welche bei Endanwendenden in großer Zahl vorkommen, siehe dazu Kap. 2.1.3, korrigieren. Dazu soll zunächst die allgemeine Funktion von HTTP erläutert und darauf aufbauend die Notwendigkeit einer Verschlüsselung für dieses Protokoll erläutert werden. Anschließend soll der Sicherheitsgewinn durch die durch HTTPS bedingte Steigerung der Vertraulichkeit vermittelt werden. Hier soll explizit darauf eingegangen werden, dass

HTTPS nur die Vertraulichkeit schützt, allerdings keine Authentizität gewährleistet. Die Lernziele dieses Videos sind das Wissen den Unterschied zwischen HTTP und HTTPS erklären zu können, die Fähigkeit nachprüfen zu können, ob eine Webseite durch HTTPS verschlüsselt wurde und das Wissen, dass HTTPS keine Authentizität gewährleistet.

3.3.5. Malware

Was ist Malware? Das erste Video dieses Kapitels soll den Begriff Malware definieren. Danach wird die Klassifizierung von Malware nach Infektionswegen und Zweck vorgestellt. Dadurch sollen Lernende einen Überblick über die Vielzahl unterschiedlicher Malware erhalten und verstehen, dass die Bedrohung durch Malware sehr vielfältig ist. Nach Sichtung dieses Videos sollen Lernende den Begriff "Malware" definieren können und die Klassifikation von Malware kennen.

Angriffsvektoren Um Lernende für mögliche Infektionswege zu sensibilisieren und die Grundlagen für Präventionsmaßnahmen zu legen, sollen in diesem Video die möglichen Infektionswege vorgestellt werden. Zuerst soll der Infektionsweg über E-Mail-Anhänge erläutert werden. Anschließend wird auf Infektionen über Webbrowser, also Drive-by-Download und Malvertising eingegangen. Lernende sollen nach Bearbeitung des Videos verschiedene Infektionswege für Malware kennen.

Datentypen Hier wird ein Textdokument hinterlegt, in welchem häufig vorkommende Dateitypen mit ihren Dateiendungen aufgelistet sind. Dabei wird jeder dieser Dateitypen kurz beschrieben und dessen Bedrohungspotential eingeschätzt. Das hier erhaltene Wissen wird in dem nächsten Video vorausgesetzt. Nach Sichtung dieses Textdokumentes sollen Lernende unterschiedliche Dateitypen kennen und deren Gefährlichkeit einschätzen können.

Prävention Das Video in diesem Abschnitt soll Lernenden Möglichkeiten zur Prävention von Malwareinfektionen aufzeigen, welche von Personen ohne umfangreiche Computerkenntnisse umgesetzt werden können. Zunächst wird gezeigt, worauf bei Anhängen von Mails geachtet werden muss, dabei wird auch auf das vorhergehende Textdokument verwiesen. Als ein hilfreiches Tool zur Bewertung von Mail-Anhängen

wird VirusTotal vorgestellt. Da die meisten browserbasierten Infektionen über JavaScript stattfinden, wird gezeigt, wie JavaScript deaktiviert werden kann. Allerdings hat dies den Nachteil, dass viele Webseiten dann nicht mehr korrekt funktionieren. Deshalb werden ScriptBlocker wie uMatrix vorgestellt. Als Maßnahme gegen Malvertising werden Adblocker vorgestellt. Daneben werden weitere Präventionsmaßnahmen, wie regelmäßige Back-ups und eine restriktive Rechteverwaltung vorgestellt. Die Lernziele dieses Videos sind das Wissen zur Prävention von Infektionen durch Mail-Anhänge und browserbasierten Angriffsmethoden, sowie die Fähigkeit weitere Präventionsmaßnahmen aufzählen zu können.

Infektion: Was tun? In diesem Video werden Lernenden die Möglichkeiten bei einer Malware-Infektion erklärt. Begonnen wird hier mit einer als sehr sicher geltenden Methode: Das Neuaufsetzen des Systems. Da dies allerdings sehr aufwändig ist, wird im Weiteren die Möglichkeit der Systemwiederherstellung aufgezeigt. Auch das Beseitigen von Malware mittels Anti-Malware-Software wird beschrieben, dessen Wirksamkeit wird im folgenden Video ausführlicher diskutiert. Auch die Möglichkeit Malware selbst zu entfernen wird erwähnt, allerdings nicht weiter ausgeführt, da dies einerseits zu spezifisch für einzelne Malware-Varianten wird und andererseits den Umfang eines Grundlagenkurses überschreitet. Nach Sichtung des Videos sollen Lernende verschiedene Möglichkeiten zum Entfernen von Malware kennen und verstehen, dass die Beseitigung einer Infektion in der Regel mehr Aufwand als die Prävention bedeutet.

Diskussion: AntiVirus-Programme Das letzte Video dieses Kapitels soll sich mit Anti-Malware-Software befassen. Lernende sollen erfahren, dass die Verwendung solcher Software in Fachkreisen umstritten ist. Dazu sollen einige Problematiken wie der tiefe Eingriff in Systeme durch Anti-Malware-Suits und das Erkennen neuer Malware-Varianten besprochen werden. Dadurch sollen Lernende in die Lage versetzt werden, die Verwendung von Anti-Malware-Software kritisch zu beurteilen. Die Lernenden sollen durch dieses Video in die Lage versetzt werden, Vor- und Nachteile von Anti-Malware-Software nennen zu können und den Nutzen solcher Software einschätzen zu können.

3.4. Technische Konzeption

Nun wird das Konzept zur technischen Umsetzung erstellt. Das Modul soll auf der Lernplattform Moodle erstellt werden, da Moodle die funktionalen Anforderungen an das Modul erfüllt. Es können Lerninhalte als Videos, Texte und interaktive Elemente eingebettet werden (**FA1** und **FA3**). Dazu können durch Links in einzelne Abschnitte und auch wieder zurück zur Gesamtansicht navigiert werden (**FA2**). Außerdem bietet Moodle bereits die Möglichkeit Tests zu erstellen, dabei gibt es bereits vorgefertigte Funktionen, welche u.a. zur Erstellung von Single-Choice, Multiple-Choice oder auch Drag-and-Drop-Aufgaben genutzt werden können (**FA4**). Zusätzlich können in Moodle Hyperlinks zu externen Materialien direkt im Kurs angelegt werden (**FA5**). Im Folgenden werden die Konzepte der technischen Umsetzung für die im vorherigen Kapitel konzipierten Inhalte beschrieben.

3.4.1. Aufruf der Lerninhalte

Die Lerninhalte werden nach den in der Struktur ausgearbeiteten Kapiteln in verschiedene Abschnitte unterteilt. Die Abschnitte verfügen eine Überschrift, welche der Kapitelbezeichnung entspricht. Die Unterteilung kann in Abb. 3.1 eingesehen werden. Die Lerninhalte sollen dann innerhalb dieser Abschnitte platziert werden, damit sie zu einem Thema zugeordnet werden können. Die Reihenfolge innerhalb der Abschnitte wird wie die Reihenfolge der Abschnitte gehandhabt. Die ersten Inhalte stehen oben und anschließend geht es in absteigender Reihenfolge bis zum Zwischentest. Folgend wird berschrieben, wie die Inhalte eingebunden werden sollen.

Videos sollen über das Element ”Interaktiver Inhalt” eingebunden werden. Dabei können verschiedene H5P-Elemente angelegt werden. Es soll ”Interactive Video” gewählt werden. Dieses Element soll statt des Datei-Elements verwendet werden, da die Videos hier in voller Größe dargestellt werden. In Abb. 3.2 kann ein Video, welches zu Testzwecken hochgeladen wurde in einem Datei-Element eingesehen werden. In Abb. 3.3 kann das gleiche Video in einem ”Interaktiver Inhalt”-Element eingesehen werden. Bei einem Vergleich wird ersichtlich, dass das Video in dem Datei-Element kleiner dargestellt wird, als in dem ”Interaktiver Inhalt”-Element. Zwar kann das Video in beiden Elementen im Vollbildmodus angesehen werden, allerdings sollen Videos auch ohne Wissen über das Vorhandensein eines Vollbildmodus in einer angenehmen Größe angesehen werden können, um Usability für Personen mit wenig bis keiner

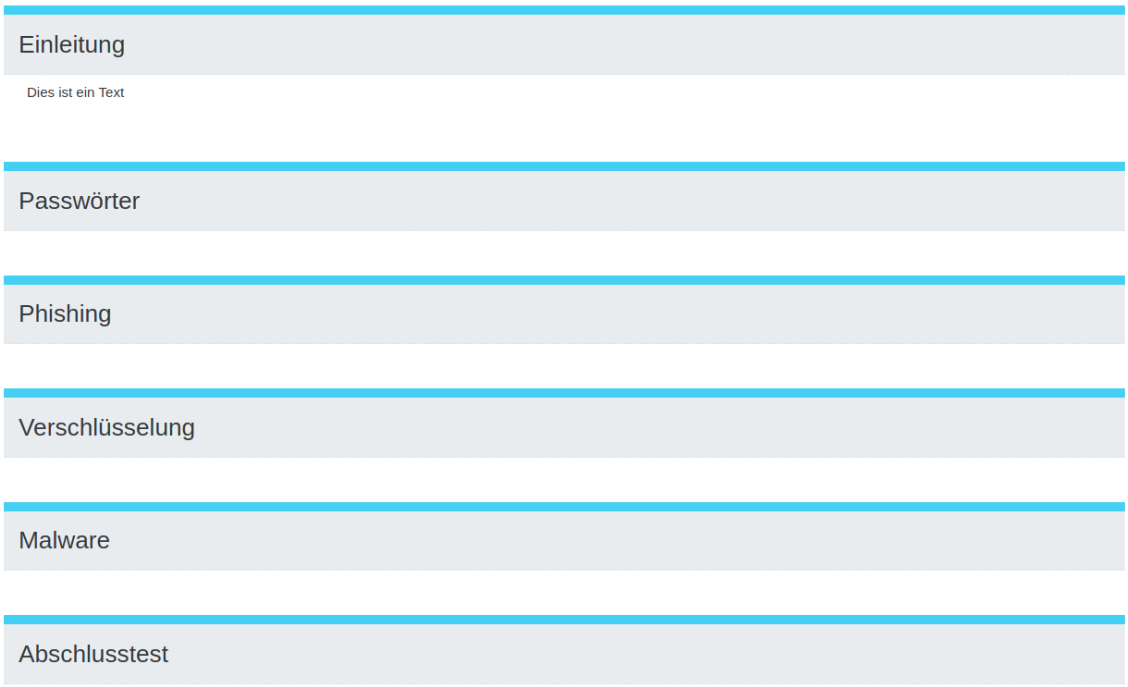


Abbildung 3.1.: Einteilung in einzelne Abschnitte.

Erfahrung im Umgang mit digitalen Systemen zu gewährleisten. Zusätzlich bestünde die Möglichkeit bei dem ”Interaktiver Inhalt”-Element klickbare Einblendungen einzufügen, dies wurde allerdings nicht benötigt.

Texte sollen durch das Datei-Element eingebunden werden. Dadurch wird das hinterlegte Textdokument bei einem Klick sofort heruntergeladen. Die Textdokumente sollen im pdf-Format vorliegen, da sie so auf verschiedenen Betriebssystemen ohne zusätzliche Software geöffnet werden können. Daneben können gängige Webbrowser diese direkt darstellen.

Das **interaktive Element** des ”Passwörter Experimentes” soll das ”Interaktiver Inhalt”-Element verwenden. Dabei soll ”Quiz” gewählt werden. Dadurch können Fragen mit Freitextantworten beantwortet werden, welchen feste Längen vorgeschrieben werden können. Die Antworten sollen dann gegen ein Schlagwort geprüft werden. Dadurch wird ein Element generiert, welches Lernenden ermöglicht, das Passwort zu raten und anschließend direkt prüfen können, ob das eingegebene Passwort das gesuchte ist.

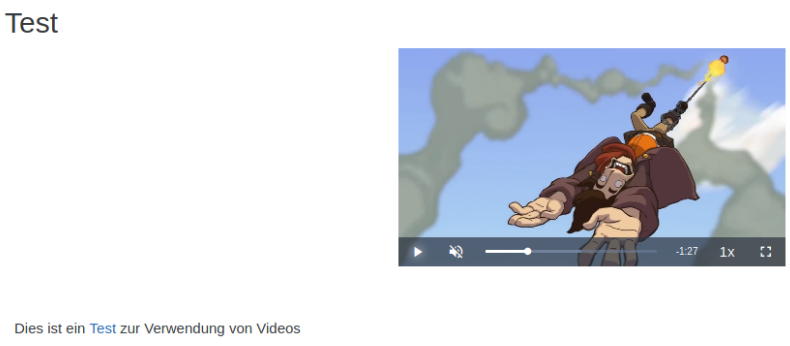


Abbildung 3.2.: Video, welches durch das Datei-Element eingebettet wurde.

Abbildung 3.3.: Video, welches durch das ”Interaktiver Inhalt”-Element eingebettet wurde.

Abbildung 3.4.: Navigation durch das Modul. Durch einen Klick auf die blau markierten Links können sich Lernende zu höhren Ebenen bewegen.

Tests sollen in Moodle durch das gleichnamige Element angelegt werden. Dadurch können verschiedene, vorgefertigte Aufgabentypen verwendet werden. Dabei sind sämtliche benötigte Typen bereits vorhanden, dies umfasst Single- und Mulitple-Choice, Anordnung von Elementen und Drag-and-Drop auf Bildern. Zwischentests sollen beim Abschicken lediglich ein Feedback zum Lernerfolg geben und keine Bewertung haben. Außerdem sollen sie beliebig oft wiederholt werden können. Die Tests zur Evaluation des Lernerfolges sollen nicht wiederholt werden können und eine bepunktete Bewertung haben. Die Tests sollen so eingestellt werden, dass zu jeder Frage ein Feedback gegeben wird.

3.4.2. Navigation

Moodle erstellt automatisch eine Navigationsmöglichkeit. Diese kann in Abb. 3.4 eingesehen werden. Dabei kann erkannt werden, dass der aktuelle Abschnitt, hier ”Test”, sowie das Kapitel, zu welchem der Abschnitt zugehörig ist, hier ”Allgemeines zum Kurs”, einsehbar ist. Durch einen Klick auf die blauen Links kann zu höheren Ebenen navigiert werden. Dadurch können Lernende mit einem Klick auf ”GDIT_BA”, was das Kürzel für diesen Kurs ist, zur Startseite des Kurses zurückkehren, von welcher aus in andere Abschnitte navigiert werden kann.

3.4.3. Hyperlinks

Für die Erstellung von Hyperlinks zu weiterführenden Informationen soll das ”Link/URL”-Element verwendet werden. Dort kann eine Beschreibung und die Ziel-URL eingetragen werden. Lernende können dieses Element öffnen und dann auf den dort hinterlegten Hyperlink klicken, um zu den jeweiligen Informationen zu gelangen. Dies hat den Vorteil, dass Lernende nicht durch ein Versehen zu einer anderen Webseite geführt werden, sondern nur in einem entsprechenden Link-Element landen.

4. Implementierung

Nun soll die Implementierung der zuvor erstellten Konzepte beschrieben werden. Die Umsetzung des Moduls erfolgte auf der Lernplattform Moodle. Zuerst soll die Implementierung der Inhalte, also die Medienproduktion und die Erstellung der Lernmaterialien beschrieben werden. Anschließend wird die technische Umsetzung, also das konkrete Erstellen des Moduls in Moodle und das Einbinden der erstellten Medien erläutert.

4.1. Implementierung der Inhalte

Es soll nun die Implementierung der Inhalte beschrieben werden. Es wurden größtenteils Videos produziert, da sich diese für die Vermittlung von Kompetenzen in der IT-Sicherheit am besten eignen, da einerseits der Modalitätseffekt für die Theorie verwendet werden kann und andererseits auch praktische Anwendungen gezeigt und Angriffsszenarien demonstriert werden können. Daben wurde auch ein Text erstellt. Für das Geben von Feedback wurden Tests angelegt.

4.1.1. Videos

Videos wurden mit dem Open-Source-Tool OBS aufgenommen. Es wurde bei nahezu allen Videos der komplette Bildschirm aufgenommen. Die so erstellten Aufnahmen hatten eine Auflösung von 1920x1080 und wurden mit 60 FPS im mp4-Format aufgenommen. Das Video, bei welchem nicht der ganze Bildschirm aufgezeichnet wurde, war der Abschnitt ”Demonstration” im Kapitel ”Phishing”, da hier aus Sicherheitsgründen eine virtuelle Maschine, welche durch das Programm VirtualBox erstellt wurde, mit einem Windows 7 Betriebssystem verwendet wurde. Dabei wurde

dann nur die virtuelle Maschine aufgenommen, um Lernende nicht durch die sichtbaren Elemente des Virtualisierungsprogramms und die Anzeige von zwei Taskleisten unterschiedlicher Betriebssysteme zu verwirren.

Aufgenommen wurden entweder zu Demonstrationszwecken andere Programme, wie beispielsweise Thunderbird im Video "Tutorial: E-Mail Verschlüsselung" im Kapitel "Verschlüsselung" oder auch der Firefox im Video "Prävention" im Kapitel "Malware", oder Präsentationen im Vollbildmodus. Die Aufnahme von Präsentationen erfolgte bei Theorievideos, wie "Funktion von Passwörtern" im Kapitel "Passwörter". Diese Präsentationen wurden mit dem Programm LibreOffice Impress erstellt und abgespielt.

Die Folien der Präsentationen wurden minimalistisch und aufgeräumt gestaltet. Es sollte vermieden werden, Lernende durch zu viele Informationen zu überfordern. Um positive Emotionen hervorzurufen, wurden Cartoon-artige Abbildungen verwendet. Es wurde ebenfalls Humor verwendet. Humor wird allgemein als ein Kommunikationsvorgang verstanden, welcher das Ziel verfolgt, Emotionen wie Freude oder Belustigung, ausgedrückt durch Reaktionen wie Lachen, hervorzurufen [SG17, S. 10 ff]. Humor im Lernkontext kann Motivation der Lernenden steigern [SG17, S. 82 f.] und zu einer besseren Gedächtnisleistung führen [SG17, S. 82]. Um negative Auswirkungen des Humors auf das Lernen zu vermeiden, wie den Verlust von Konzentration auf die Lerninhalte [SG17, S. 83] oder eine zu hohe Belastung des Arbeitsgedächtnisses, wurde Humor stets im Kontext des Lerninhaltes verwendet und kein übertriebener Humor verwendet.

Zusätzlich sollte der Modalitätseffekt genutzt werden, um eine bessere Lernleistung zu erzielen. Dazu wurden zusätzlich zu den auditiven Erklärungen passende Abbildungen gezeigt. Als Beispiel kann hier in Abb. 4.1 ein Screenshot aus dem Video "Funktion von Passwörtern" aus dem Kapitel "Passwörter" eingesehen werden. Dort wurde erklärt wie ein Loginvorgang mit Authentifizierung durch ein Passwort abläuft. Die einzelnen Abbildungen wurden nacheinander, passend zur Audiospur, eingeblendet. So wurden die einzelnen Teilschritte nacheinander erläutert.

In den Audiospuren wurden die Lerninhalte im Bezug auf die visuell dargestellten Inhalte erklärt. Lernende wurden höflich gesiezt. Außerdem wurden sie in einigen Videos direkt angesprochen, dies dient der Erfüllung des psychologischen Grundbedürfnisses der sozialen Eingebundenheit zur Motivationssteigerung. Es wurde versucht möglichst wenige Störgeräusche aufzunehmen, durch das zur Verfügung stehende

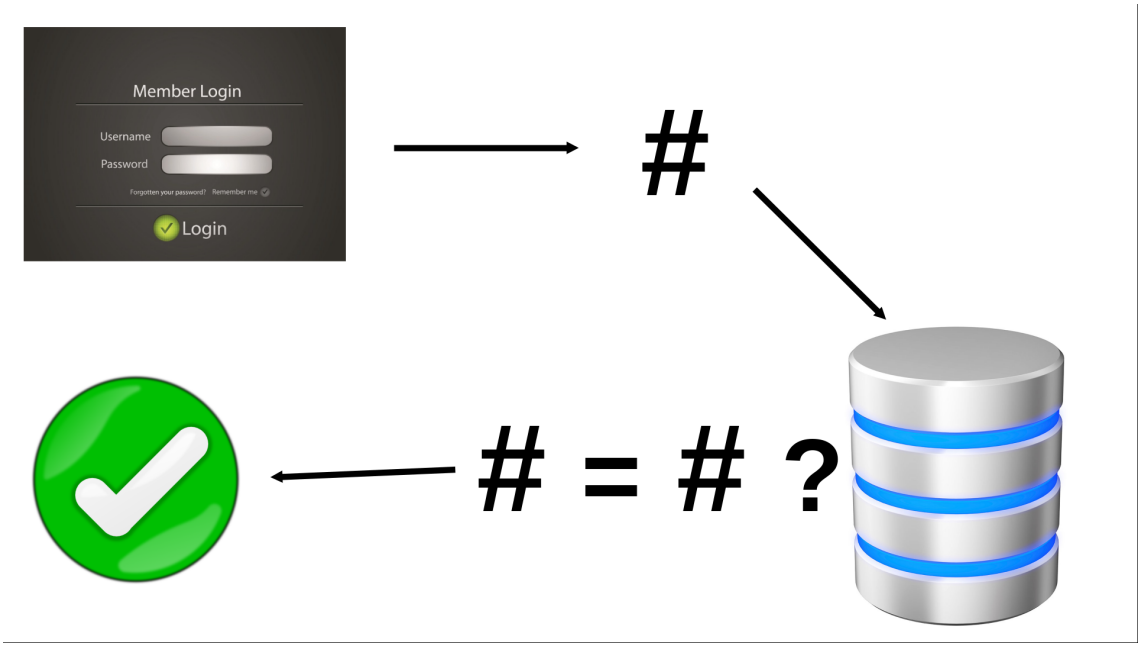


Abbildung 4.1.: Schematische Abbildung eines Loginvorganges mittels Passwort.

Mikrofon war es jedoch nicht möglich dies komplett zu erreichen. Die Entfernung sämtlicher Störgeräusche durch Nachbearbeitung war nicht möglich, da ansonsten die Qualität der Audiospuren beeinträchtigt würde. Da die Störgeräusche die Audiospuren nur gering beeinträchtigten, wurden diese beibehalten.

Die so aufgenommenen Videos wurden anschließend mit dem Open-Source-Programm Kdenlive bearbeitet. Dabei wurden Versprecher und Fehler herausgeschnitten und Atem- und Schmatzgeräusche entfernt. Bei aufgenommenen Präsentationen konnten entsprechende Stellen mit den Geräuschen herausgeschnitten werden. Bei anderen Videos, bei welchen das einfache Herausschneiden zu Sprüngen in der Videospur geführt hätte, wurden Schnitte an den entsprechenden Stellen gesetzt und durch den ”Volume”-Audioeffekt die Lautstärke auf das absolute Minimum reduziert. Zusätzlich wurden bei Aufnahmen von Software ein weißes Rechteck über die Taskleiste gelegt. Dadurch sollte eine Ablenkung durch dort befindliche, unwesentliche Informationen, wie das Aufnahmedatum oder geöffnete Programme, vermieden werden. Nach der Bearbeitung wurden die Videos in maximaler Qualität im mp4-Format exportiert.

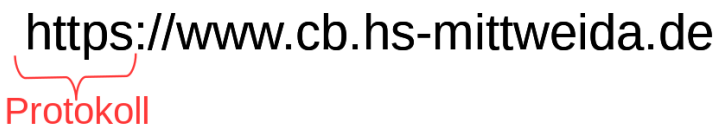


Abbildung 4.2.: Lenkung der Aufmerksamkeit durch Farbe und eine geschweifte Klammer.

Hervorhebungen in Theorievideos wurden ursprünglich in der Nachbearbeitung eingefügt, da dies allerdings zu technischen Problemen mit Kdenlive führte, wurden die Hervorhebungen direkt in die Präsentationen eingepflegt. Dies brachte den zusätzlichen Vorteil mit sich, dass der gesprochene Text besser mit den Hervorhebungen synchronisiert werden konnte. Diese wurden generell in roter Farbe angelegt, da diese eine starke Lenkungswirkung auf die Aufmerksamkeit hat. Neben der Farbe sollte die Aufmerksamkeit auch durch weitere Faktoren gelenkt werden. Um die Nullifizierung der Signalwirkung der Farbe durch eine Farbfehlsichtigkeit zu verhindern wurden zusätzlich noch Formen verwendet. Ein Beispiel dafür kann in Abb. 4.2 eingesehen werden. Dort wird ein Screenshot aus dem Video ”Erkennung von Phishing” auf dem Kapitel ”Phishing” gezeigt. In diesem wird anhand eines Beispiels der Aufbau einer URL erklärt. Der aktuell besprochene Bestandteil ist durch eine geschweifte Klammer mit einer roten Färbung hervorgehoben. In praktischen Videos, in welchen Software gezeigt wird, wurden Elemente durch Mausbewegungen und das Markieren von Elementen und einen auditiven Hinweis in der Audiospur auf das Element hervorgehoben.

4.1.2. Text

Das Textdokument ”Datentypen” im Kapitel ”Malware” wurde mit dem Online-LaTeX-Editor Overleaf erstellt. Für die einzelnen Beschreibungen der Formate wurde jeweils ein ”\paragraph{}”-Element verwendet. Dadurch wurden die vorgestellten

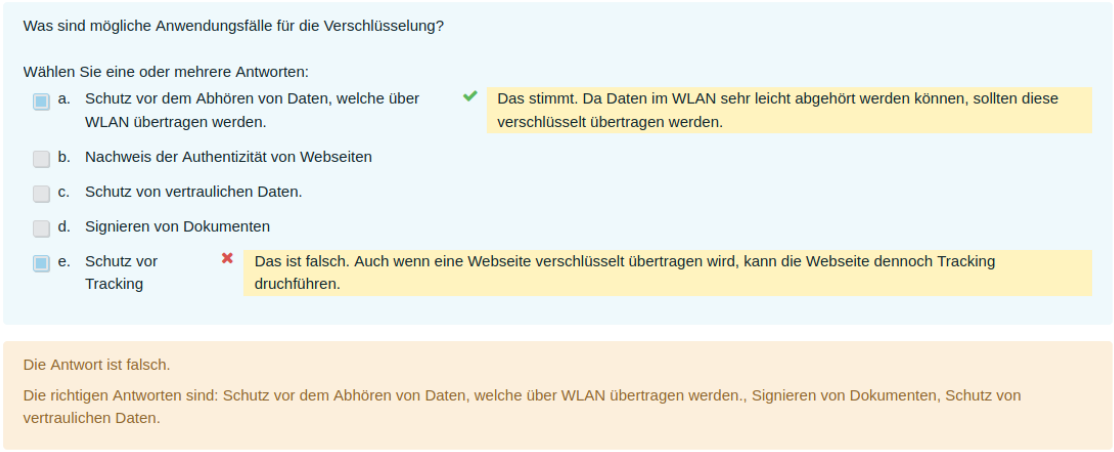


Abbildung 4.3.: Eine beantwortete Frage mit Feedback in einem Zwischentest.

Formate hervorgehoben. Danach folgt der Fließtext, welcher den Einfluss des vorgestellen Formates auf die Sicherheit beschreibt. Die Schrift ist zur Lesbarkeit schwarz auf weißem Hintergrund gehalten.

4.1.3. Tests

Die Zwischentests und die Tests zur Evaluation des Lernerfolges wurden nach den vorher erstellten Konzepten umgesetzt. Dabei wurden Fragen und Antworten im Wortlaut übernommen. Zur Erstellung von Hinweisreizen, welche eine Steigerung des Lernerfolges durch Erfüllung des psychologischen Grundbedürfnisses der sozialen Eingebundenheit bezwecken sollen, wurde zu jeder möglichen Antwort ein Feedback verfasst. Das Feedback gibt Auskunft über die Richtigkeit der gewählten Antwort und begründet dies. Ein Beispiel dafür kann in Abb. 4.3 eingesehen werden. Dabei wurde in einer Multiple-Choice-Frage eine richtige und eine falsche Antwort ausgewählt. Bei diesen Antworten wird das entsprechende Feedback angezeigt. Darunter befindet sich eine allgemeine Meldung, welche informiert, ob diese Aufgabe korrekt bearbeitet wurde und die richtigen Antworten angibt.

4.2. Technische Implementierung

Nun soll die technische Umsetzung beschrieben werden. Es wurden die erstellten Inhalte in den Moodle-Kurs eingebunden und die benötigten technischen Funktionen implementiert. Da Moodle bereits über die benötigten Funktionen verfügt, mussten keine eigenen Funktionen erstellt werden, sondern die zur Verfügung stehenden Funktionalitäten eingefügt und konfiguriert werden.

4.2.1. Aufruf der Lerninhalte

Wie aus der Konzeption ersichtlich ist, wurden fünf unterschiedliche Abschnitte erstellt, welche die einzelnen Kapitel darstellen. Zu diesen Abschnitten kommt noch ein eigener Abschnitt für den Abschlusstest und für eine kurze Einleitung, welche eine Danksagung für die Teilnehmenden, eine allgemeine Einführung in die Nutzung des Moduls, sowie Informationen zur Verwendung der Daten, welche über den Abschlusstest und die Usability-Evaluation erhoben werden, enthält. In diesem Abschnitt befindet sich auch der Vortest zur Lernerfolgsmessung. Bei sämtlichen Lerninhalten wurde jeweils eine Beschreibung erstellt, welche direkt auf der Übersichtsseite des Kurses angezeigt werden. Hierdurch ist für Lernende sofort ersichtlich, um welchen Medientyp es sich handelt und welches Thema behandelt werden soll.

Videos wurden über das Element ”Interaktiver Inhalt” eingebunden. Es wurde das H5P-Element ”Interactive Video” verwendet. Allerdings wurden keine interaktiven Elemente genutzt. Der Titel wurde in die vorgesehenen Felder eingetragen. Sämtliche Optionen in den Anzeigeeinstellungen wurden deaktiviert. Sämtliche andere Einstellungen wurden auf dem Standard belassen.

Der **Text** ”Datentypen” wurde durch das ”Datei”-Element eingebunden. Das durch Overleaf erzeugte PDF-Dokument wurde hochgeladen und als die in dem Element verlinkte Datei angegeben. In dem Dropdown-Menü ”Anzeigen” wurde ”Automatisch” eingestellt. Durch diese Option wählt Moodle automatisch die passende Anzeigeoption aus. Dies wurde gewählt, um Kompatibilität für möglichst viele Webbrowser zu erreichen. Bei einem Test mit dem Webbrowser Mozilla Firefox wurde bei Klick auf das Element im Kurs direkt die hinterlegte PDF-Datei geöffnet.

4.2.2. Navigation

Für die Navigation war es nicht notwendig eine Implementierung durchzuführen, da Moodle automatisch Navigationsmöglichkeiten im Kurs erzeugt. Es wird eine Navigation von den Seiten der einzelnen Elemente zur Hauptseite des Kurses angelegt, siehe dazu Abb. 3.4. Daneben werden unter dem Inhalt der einzelnen Elemente Links erzeugt, welche zum vorherigen und dem nachfolgenden Element führen.

4.2.3. Hyperlinks

Externe Inhalte wurden durch das ”Link/URL”-Element eingebettet. Es wurden der Titel und die externe URL eingetragen. Sämtliche Einstellungen wurden auf Standard belassen. Dadurch wird bei Klick auf das Element die entsprechende Unterseite mit der Beschreibung und der klickbaren URL angezeigt. Bei Klick auf die URL wird dann die verlinkte Ressource aufgerufen. Auf der Hauptseite des Kurses wurden die ”Link/URL”-Elemente eingerückt, um darzustellen, dass es sich hierbei um fakultative Inhalte handelt.

4.2.4. Tests

Tests wurden durch das gleichnamige Element angelegt. Hier wurden keine Beschreibungen angelegt, da der Titel bereits aussagekräftig genug ist. Hier werden nur die Zwischentests beschrieben. Für die Tests zur Evaluation siehe Kap. 5.1.2. Es wurde keine zeitliche Begrenzung für die Tests eingestellt, dies gilt sowohl für den Zeitraum, in welchem die Tests genutzt werden können, als auch die Dauer der Tests. Zusätzlich wurde eine unbegrenzte Anzahl an Versuchen eingestellt. Dadurch können die Zwischentests jederzeit zum Erhalt von Feedback zum Lernfortschritt genutzt werden. Die Anordnung der Fragen wurde so eingestellt, dass die Tests jeweils auf einer einzigen Seite angezeigt werden. Dadurch soll vermieden werden, dass Funktionen für das Wechseln zwischen Seiten übersehen werden, wodruch Lernende nicht alle Aufgaben bearbeiten können.

Für die Fragen wurden jeweils die in den zugehörigen Konzepten angegebenen Aufgabentypen verwendet. Für Single-Choice-Aufgaben wurde der Multiple-Choice-Typ gewählt und bei der Option ”Eine oder mehrere Antworten?” die Option ”Nur eine

Antwort erlauben" gewählt. Für Antworten wurde eine alphabetische Nummerierung gewählt. Es wurde die Option für eine variable Positionierung von Antworten bei Single- und Multiple-Choice-Fragen verwendet. Die hierdurch erzeugte Variation soll verhindern, bei einem erneuten Versuch die richtigen Antworten nicht durch das Merken der Position von falschen Antworten zu erschließen. Wo dies möglich war, sollten die "Standard-Anweisungen" angezeigt werden. Dadurch wurden in den Fragen Texte generiert, welche erklären wie diese beantwortet werden kann. Bei Aufgaben, welche auf dem Multiple-Choice-Typ basieren, wurde bei den jeweiligen Antworten ein Feedback hinterlegt, welches bei Wahl der Antwort zusätzliche Informationen zur Richtigkeit der Antwort gibt. Bei Aufgabentypen, welche diese Funktion nicht unterstützen, wie Anordnungsaufgaben, wurde eine Erklärung zur richtigen Antwort in dem Feld "Allgemeines Feedback" hinterlegt. Dadurch soll Lernenden Feedback gegeben werden und bei nicht verstandenen Inhalten nochmals eine kurze textuelle Erklärung erhalten werden.

4.2.5. Passwörter Experiment

Das interaktive Element "Passwörter Experiment" wurde in Moodle durch das "Interaktiver Inhalt"-Element angelegt. Es wurde das "Quiz"-H5P-Element verwendet. In diesem ist es möglich dem Quiz unterschiedliche Fragen hinzuzufügen. Dabei wurde dreimal der Typ "Essay" verwendet, da dieser Freitextantworten ermöglicht, welche gegen Schlagwörter geprüft werden können. In den Interaktionseinstellungen für diesen Fragentyp wurde die Zeichenanzahl an das jeweils zu erratene Passwort angepasst, sodass exakt vier bzw. sechs Zeichen eingegeben werden können. Das so erzeugte Element gibt Lernenden die Möglichkeit nach Eingabe der Zeichen auf "Überprüfen" zu klicken. Dadurch wird die Eingabe überprüft und eine Rückmeldung über die Richtigkeit der Eingabe gegeben. Diese Rückmeldung ist ein Hinweisreiz, welche neben der Information auch das soziale Grundbeürfnis der sozialen Eingebundenheit erfüllen soll. Die drei zu erratenen Passwörter sind 4321, 834597 und 69uz. Dabei wird jeweils gegen das exakte Schlagwort geprüft, allerdings wird beim dritten Passwort die Groß- und Kleinschreibung nicht beachtet, da so das Passwort leichter erraten werden kann. Lernende werden entsprechend darauf hingewiesen. In Abb. 4.4 kann die Eingabemaske nach Überprüfung einer inkorrekten Eingabe des dritten Passwortes eingesehen werden.

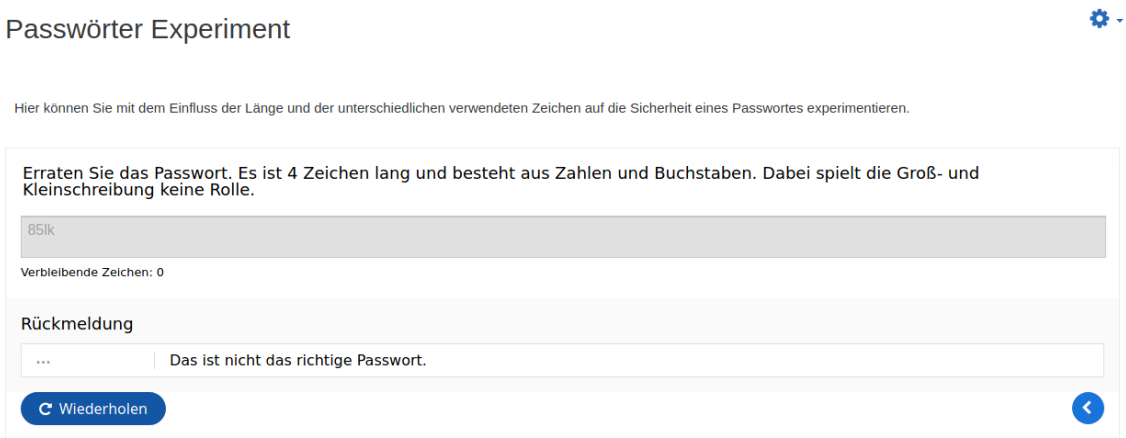


Abbildung 4.4.: Die Eingabemaske zum Erraten des dritten Passwortes mit einer falschen Eingabe.

5. Evaluation

Im Folgenden wird die Evaluation des erstellten E-Learning-Moduls beschrieben. Die Evaluation soll die ersten beiden Ebenen des Kirkpatrick/Phillips-Modell, also die Reaction und das Learning, betrachten, da diese für die Wirksamkeit des Moduls am relevantesten sind. Die weiteren Ebenen, insbesondere die dritte Ebene, könnten zukünftig in einer Weiterführung des Projektes evaluiert werden. Da die Reaction die direkte Reaktion der Lernenden auf das Training erfasst, soll diese durch eine Evaluation der Usability des Moduls erfasst werden. Da durch eine Befragung zur Usability evaluiert werden kann, ob Lerndende das Training sinnvoll nutzen konnten und ob diese mit der Nutzung zufrieden waren [Bro95, S. 3], soll so die Reaction erfasst werden. Allerdings wird hierdurch kein Lernerfolg gemessen. Die Ebene des Learnings soll durch eine eigene Messung des Lernerfolges erfasst werden. Dazu sollen zwei Tests durchgeführt werden, aus deren Vergleich die Kompetenzentwicklung durch das Modul erfasst werden soll. In den nächsten Kapiteln wird die Evaluation des Lernerfolges und der Usability beschrieben. Es wird dabei jeweils auf das Konzept, die Vorbereitung, die Durchführung und die Ergebnisse eingegangen. Abschließend folgen einige Informationen zu den Teilnehmenden des Kurses.

5.1. Lernerfolg

Es gelten drei Qualitätskriterien an eine Lernerfolgsmessung. Diese sind Objektivität, Reliabilität und Validität. Unter **Objektivität** wird die Unabhängigkeit der Ergebnisse von den erfassenden Personen verstanden. **Reliabilität** ist die Messgenauigkeit, sie gibt an, ob das Wissen bzw. die Fähigkeiten zuverlässig gemessen wird. **Validität** gibt an, ob die Messung auch die gewünschten Werte misst, also ob tatsächlich die für die Lernerfolgsmessung relevanten Fähigkeiten erfasst werden [KGH15, S. 250 ff.]. Zur Messung des Lernerfolges sollen zwei Tests durchgeführt werden. Durch den ersten Test sollen die bereits vorhandenen digitalen Kompetenzen der Lernenden erfasst werden. Zum Abschluss wird ein zweiter Test durchgeführt.

Dieser erfasst die Kompetenzen nach Abschluss des Moduls. Der Lernerfolg soll durch einen Vergleich der beiden Tests erfasst werden. Zusätzlich sollen bei beiden Tests die gegebenen Antworten der Lernenden gesichtet werden, um Auffälligkeiten, wie zu schwere Fragen zu erkennen.

5.1.1. Konzept

Zur Gewährleistung der Objektivität werden die Tests, wie auch die Zwischentests, automatisch durch ein vorher erstelltes Bewertungsschema bewertet. Zur Verbesserung der Reliabilität wurde ein angemessener Schwierigkeitsgrad gewählt, wodurch zu leichte und zu schwere Aufgaben vermieden werden sollen, dadurch sollen die Aufgaben trennscharf sein. So befindet sich beispielsweise bei der zweiten Frage des Abschlusstests eine falsche Antwortmöglichkeit, welche das Alphabet und das Hochzählen von eins bis neun enthält. Diese Antwortmöglichkeit erfüllt zwar die Anforderungen der Länge und unterschiedlichen Zeichen an Passwörter, ist allerdings zu leicht zu erraten. Diese Feinheit würde Lernenden mit einer sehr ausgeprägten Kompetenz zur Beurteilung von Passwörtern auffallen, während Lernende mit einer weniger ausgeprägten Kompetenz diese Antwort als richtig markieren würden. Weiterhin wurden Multiple-Choice-Fragen konfiguriert, sodass falsch markierte Antwortmöglichkeiten die erhaltenen Punkte bei der jeweiligen Frage verringern, wodurch verhindert wird, dass eine Aufgabe richtig gelöst wird, indem sämtliche Möglichkeiten ausgewählt werden. Die Validität dieser Evaluation soll verbessert werden, indem verschiedene Maßnahmen ergriffen werden. Es soll komplett auf Lückentexte oder Aufgaben zur Vervollständigung von Sätzen verzichtet werden, da diese durch ein Verständnis der deutschen Sprache beantwortet werden können, ohne über das abzuprüfende Wissen zu verfügen. Stattdessen soll auf Aufgabentypen gesetzt werden, welche weniger Lösungshinweise bieten, wie Multiple-Choice, Single-Choice, Sortieren von Begriffen und Zuordnung von Begriffen. Zusätzlich sollen die Aufgaben der Tests einen direkten Bezug zu den Inhalten des Moduls haben, um zu vermeiden, Irrelevantes abzufragen. Um sicherzustellen, dass durch das Ergebnis der Lernerfolgsmessung auch wirklich die Kompetenz im Bereich der IT-Sicherheit gemessen wird, werden die einzelnen Aufgaben gewichtet. Dabei werden Aufgaben, welche Fähigkeiten und Wissen prüfen, welche einen großen Einfluss auf die IT-Sicherheit haben, wie das Erkennen von Phishing-Angriffen oder das richtige Verhalten bei einer Malwareinfektion, stärker gewichtet, als Aufgaben, bei welchen die

geprüften Inhalte einen geringeren Einfluss auf die IT-Sicherheit haben, wie ein Grundverständnis von Verschlüsselung oder allgemeines Hintergrundwissen.

Zu Beginn des Kurses wird eine Nullmessung durchgeführt. Nullmessungen dienen in Kombination mit einer späteren Lernstandmessung zum Vorher-Nachher-Vergleich [KK06, S. 149]. Dadurch kann der Lernerfolg gemessen werden. Der Test zur Nullmessung entspricht aus Gründen der Vergleichbarkeit im Wesentlichen dem Abschlusstest. Dies bedeutet, dass die gleichen Themengebiete abgeprüft werden und die entsprechenden Fragen gleich gewichtet sind. Allerdings sind die Fragen abgeändert. Dadurch soll verhindert werden, dass Lernende die Antworten der Nullmessung einfach auf den Abschlusstest übertragen können. Zusätzlich gelten hier andere Überprüfungsoptionen als im Abschlusstest, wodurch die Lernenden kein Feedback zur Richtigkeit ihrer Antworten erhalten. Dadurch können richtige Antworten in der Nullmessung nicht zu korrekten Antworten im Abschlusstest führen, wodurch die Messung verfälscht werden würde. Die Nullmessung kann von den Lernenden nur jeweils einmal durchgeführt werden. Das Konzept des Vortests kann in Anhang C eingesehen werden.

Der Abschlusstest soll, wie der Vortest, von den Lernenden nur einmal abgelegt werden können. Da die Bearbeitung des Moduls selbstständig erfolgt, können Lernende den Test jederzeit starten, allerdings wird empfohlen diesen erst abzulegen, wenn die vorherigen Kapitel bearbeitet wurden. Der Abschlusstest besteht, wie der Vortest, aus zehn Aufgaben, welche sämtlichen Lerngebiete des Moduls abdecken, dabei kann eine Aufgabe mehrere Kapitel umfassen. Zur Quantifizierung des Lernerfolges sollen Punkte vergeben werden. Insgesamt sollen 100 Punkte erreicht werden können. Punkte werden durch das Geben von richtigen Antworten in den Tests erlangt. Da sich die Aufgaben nur in geringer Weise in ihrem Aufwand unterscheiden und die Aufgaben nach dem Beitrag zur IT-Sicherheit der von ihnen abgeprüften Fähigkeiten gewichtet werden sollen, werden die zu erreichenden Punkte einer Aufgabe als prozentuale Gewichtung verstanden. Um den Abschlusstest zu bestehen, müssen mindestens 60 Punkte erreicht werden. Dadurch ist es nicht möglich den Abschlusstest nur das das korrekte Beantworten der Fragen mit geringem Einfluss auf die IT-Sicherheit zu bestehen. Das Konzept des Abschlusstests kann in Anhang D eingesehen werden.

Der Lernerfolg durch das Modul wird als ausreichend betrachtet, wenn der Abschlusstest von allen Probanden bestanden wird und beim Abschlusstest mehr Punkte als beim Vortest erreicht werden.

5.1.2. Vorbereitung

Die Nullmessung wurde als ein Vortest, welcher am Beginn des Kurses angesiedelt ist, umgesetzt. Während der Abschlusstest sich am Ende befindet. Beide entsprechen den zuvor erstellten Konzepten. Im Gegensatz zu den Zwischentests wurden hier in den Bewertungseinstellungen die Anzahl der erlaubten Versuche jeweils auf eins gestellt, damit beide Tests von jeder teilnehmenden Person nur einmal ausgefüllt werden können. Zusätzlich wurde die Bestehensgrenze auf 60,00 eingestellt, um das Bestehen bei Erlangung von 60 Punkten zu implementieren. Wie auch bei den Zwischentests wurden auch hier kein Datum zu Öffnung des Tests, so ist dieser direkt zu Beginn der Evaluation verfügbar, und kein Zeitlimit für einen Versuch eingestellt. Für die Schließung der Tests wurde der 12.08.22 eingestellt, um zu diesem Stichtag mit der Evaluation des Lernerfolges beginnen zu können.

Die Fragen wurden analog zu den Zwischentests erstellt, siehe dazu Kap. 4.2.4. Der einzige Unterschied ist die Bepunktung. Während diese für die Zwischentests irrelevant ist, wurden hier die Punkte entsprechen dem Konzept eingestellt, sodass insgesamt 100 Punkte erreicht werden können.

5.1.3. Durchführung

Die Test-Elemente wurden bereits konfiguriert, um am 12.08.22 keine Versuche mehr zuzulassen. Aufgrund eines Konfigurationsfehlers, bei welchem durch das falsche Beantworten der Frage 4 im Abschlusstest eine Punktzahl von -14 erreicht werden konnte, musste eine Neubewertung nach Korrektur des Fehlers durchgeführt werden. Dabei änderte sich die erreichte Punktzahl von Proband 3 im Abschlusstest. Die Punktzahlen der Vor- und Abschlusstests wurden automatisch von Moodle anhand der eingestellten Bepunktung der einzelnen Fragen berechnet. Es wurden die Punkte der Vortests und der Abschlusstests der jeweiligen Probanden verglichen. Zusätzlich wurden die eingereichten Antworten gesichtet.

5.1.4. Ergebnisse

Die Punktzahlen, welche die Probanden in den Tests erreichten, können in Tab. 5.1 eingesehen werden. Bei Proband 1 und 2 kann eine Steigerung der Punktzahlen beobachtet werden. Während bei Proband 3 die Punktzahl des Abschlusstests niedriger ist als des Vortests, sodass vor Durchführung der Neubewertung der Abschlusstest nicht bestanden wurde, da eine Punktzahl von 48 erreicht wurde.

Bei Sichtung der Antworten des Abschlusstests von Proband 3 konnte eingesehen werden, dass der Grund für die niedrige Punktzahl das falsche Beantworten der Fragen 4 (Erkennung von Phishing) und 9 (Prävention von Malwareinfektionen), welche 14 und 12 Punkte geben, ist. Während Probanden 1 und 2 beide Fragen korrekt beantworteten, wodurch ein zu hoher Schwierigkeitsgrad ausgeschlossen werden kann. Ein entsprechender Kompetenzdefizit als Grund für die falsche Antwort bei Frage 4 erscheint unwahrscheinlich, da Proband 3 die entsprechende Frage im Vortest und Frage 3 im Zwischentest des Kapitels "Phishing", bei welcher Bereiche, an welchen eine Phishing-Mail erkannt werden kann, markiert werden sollen, korrekt beantwortete. Womit diese Kompetenz bereits erfasst werden konnte. Somit könnte es sich hier um einen Eingabefehler handeln. Sollte dies der Fall sein, würde Proband 3 76 Punkte erreichen, was eine Steigerung im Vergleich zum Vortest wäre.
In Abb. 5.1 kann die Antwort von Proband 3 bei Frage 9 im Abschlusstest eingesehen werden. Hier wären die Antworten a., c. und d. richtig gewesen. Dass Antwort d. nicht von Proband 3 als richtige Antwort erkannt wurde, könnte damit erklärt werden, dass im Abschnitt "Prävention" des Kapitels "Malware" zwar das Deaktivieren von JavaScript als mögliche Präventionsmaßnahme vorgestellt wird, allerdings auch der Nachteil der Einschränkung der Funktionalität von Webseiten, welche daraus resultiert beschrieben wird. Vermutlich wird deswegen das Deaktivieren von JavaScript von Proband 3 nicht als geeignete Präventionsmaßnahme betrachtet. Im gleichen Kapitel wurde auch das Gewähren möglichst geringer Rechte bei der Nutzung als Präventionsmaßnahme besprochen. Gründe für das Wählen von Antwort b. und e. konnten nicht gefunden werden, da beide Maßnahmen im Kapitel "Malware" nicht besprochen werden und in den jeweiligen Kapiteln keine Erwähnung von Malware stattfindet. Daher wird hier eine Antwort durch Raten vermutet.

Zwar haben alle Probanden den Abschlusstest bestanden, allerdings wurde nicht bei allen Probanden eine Verbesserung der Punktzahlen im Abschlusstest im Vergleich zum Vortest beobachtet. Deshalb wird der Lernerfolg als nicht ausreichend gegeben

Proband	Vortest	Abschlusstest
1	34,36	94,67
2	57,00	95,33
3	65,67	62,00

Tabelle 5.1.: Erreichte Punkte der Probanden in den Tests

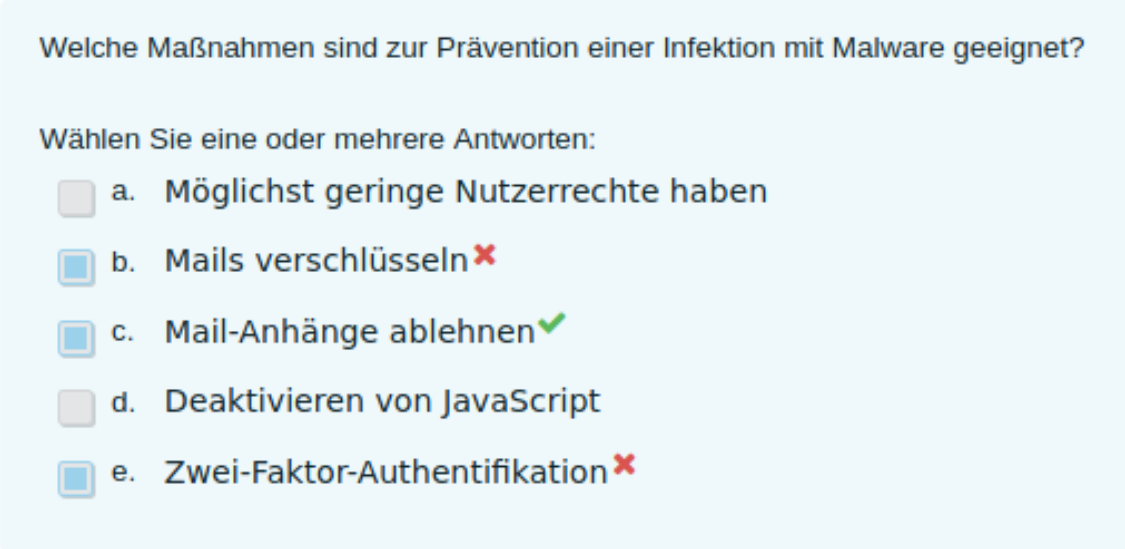


Abbildung 5.1.: Antworten von Proband 3 bei Frage 9 im Abschlusstest

angesehen. Hier ist allerdings zu erwähnen, dass die niedrigere Punktzahl im Abschlusstest von Proband 3 das Resultat eines Eingabefehlers sein könnte, sollte dies der Fall sein, so wäre auch hier die angestrebte Steigerung der Kompetenz in der IT-Sicherheit, welche durch die Punktzahl dargestellt wird, vorhanden. Zusätzlich ist zu beachten, dass die Anzahl an Probanden gering war. Dadurch hat das Ergebnis eine geringe Aussagekraft und es sollte in einer möglichen Weiterführung des Projektes nochmals mit einer größeren Anzahl an Probanden evaluiert werden.

5.2. Usability

Usability wird meist als die Angemessenheit zu einem Zweck bezeichnet, also ob ein Werkzeug im Kontext seiner vorgesehenen Nutzung dem zu erreichenden Ziel angemessen ist. Diese Angemessenheit enthält meist drei Komponenten: die Wirksamkeit, die Effizienz und die Zufriedenheit. Die **Wirksamkeit** beschreibt die Fähigkeit des Systems es Nutzenden zu ermöglichen durch die Verwendung das vorgesehene Ziel zu erreichen. Im Kontext des E-Learnings wird darunter verstanden, ob durch das Modul überhaupt gelernt werden kann. Die **Effizienz** gibt den Ressourcenverbrauch während des Erreichens des Ziels an. Im Kontext des E-Learnings ist dies die Effizienz der Entwicklung neuer Kompetenzen. Die **Zufriedenheit** gibt die subjektiven Reaktionen der Nutzenden durch die Verwendung des Werkzeuges an [Bro95, S. 2].

5.2.1. Konzept

Zur Evaluation der Usability soll ein Verfahren genutzt werden, welches einerseits verlässliche Daten liefert, um diese sinnvoll zur Evaluation verwenden zu können, und andererseits keinen großen Aufwand für die Lernenden darstellt, da diese bereits viel Zeit in das Modul investierten und ein zu aufwendiges Verfahren abschreckend sein könnte, was zu wenig erhobenen Daten führen kann. Ein solches Verfahren ist der System Usability Scale (SUS) [Klu17]. Schöpfer Brooke verfolgte mit diesem Verfahren das Ziel ein schnelles Verfahren zu entwicklen, welches schnell und kostengünstig Daten liefert, [Bro95, S. 3], spätere Untersuchungen wiesen eine hohe Qualität des Verfahrens und der erhobenen Daten nach [Klu17].

Der SUS basiert auf einer fünfstufigen Likert-Skala, wobei Lernende zu zehn Aussagen Bewertungen abgeben sollen. Dabei ist der Wert 1 auf der Likert-Skala mit ”strongly disagree” und der Wert 5 mit ”strongly agree” bezeichnet [Bro95, S. 3]. Die dazwischen befindlichen Werte sind als Abstufungen zu verstehen. Zur Evaluation soll die deutsche Übersetzung des SUS von der Bundeszentrale für gesundheitliche Aufklärung verwendet werden [TS17, S. 37]. Die Skalen sollen in einem Umfrage-Tool zur Verfügung gestellt werden. Um zu gewährleisten, dass Lernende die Umfrage nicht vor der Nutzung des Moduls ausfüllen, soll die Verlinkung erst nach der Abgabe des Abschlusstests, unabhängig des Ergebnisses, aktiviert werden.

Durch die Auswertung und Normalisierung der Antworten kann ein SUS-Score bestimmt werden. Dabei ist der durchschnittliche Score 68 [Klu17]. Deshalb wird als minimaler Wert, bei welchem die Usability als ausreichend gegeben angesehen wird, 68 verwendet.

5.2.2. Vorbereitung

Für die Erhebung von Daten zur Usability des Moduls wurde der System Usability Scale (SUS) in deutscher Sprache in dem Tool Google Docs umgesetzt. Dabei wurde die deutsche Übersetzung von der Bundeszentrale für gesundheitliche Aufklärung verwendet [TS17, S. 64]. Hier wurde das Wort "System" durch das Wort "Lernsystem" ersetzt. Dadurch soll der Kontext des Kurses während des Ausfüllens erhalten bleiben. Zusätzlich zu den Fragen des SUS wird die Hochschul-E-Mail-Adresse und demografische Daten, wie Alter und Geschlecht, abgefragt. Die Abfrage der Hochschul-E-Mail-Adresse dient zur Erkennung von Duplikaten während der Auswertung. So können mehrfache Antworten einer Person erkannt werden. Sollte dies der Fall sein, so wird nur der erste abgeschickte Bogen zur Evaluierung verwendet, da dieser die empfundene Nutzbarkeit besser wiedergibt, als eine spätere Antwort, bei welcher die Antworten aus Erinnerung und Überdenken gegeben werden. Die erhobenen demografischen Daten sollen zur Identifizierung der erreichten Personengruppe, im Verhältnis zur geplanten Zielgruppe, dienen. Sämtliche Fragen des SUS sind als Pflichtfragen eingestellt worden, um so zu jeder Frage eine Antwort zu erhalten.

Der Zugriff auf die Google Docs-Umfrage erfolgt, wie bei den anderen externen Verlinkungen, durch das "Link/URL"-Element. Allerdings wurde hier eine Voraussetzung für den Zugriff auf dieses Element eingestellt. Die Einstellungen können in Abb. 5.2 eingesehen werden. Diese Bedingungen wurden eingestellt, um zu gewährleisten, dass der Link erst nach Abgabe des Abschlusstests, unabhängig vom Bestehen, aufgerufen werden kann. Da vor der Abgabe des Tests keine Punkte vorhanden sind, treffen vor Abgabe beide Bedingungen nicht zu. Erst mit der Abgabe werden die Punkte eingetragen, sodass erst dann eine der beiden Bedingungen zutreffen kann. Größer oder gleich 60 Punkte entspricht dabei dem Bestehen, während weniger als 60 dem Nicht-Bestehen entspricht. Dieser Weg musste gewählt werden, da Moodle keine Möglichkeit bietet direkt auf die Abgabe eines Tests zu prüfen.

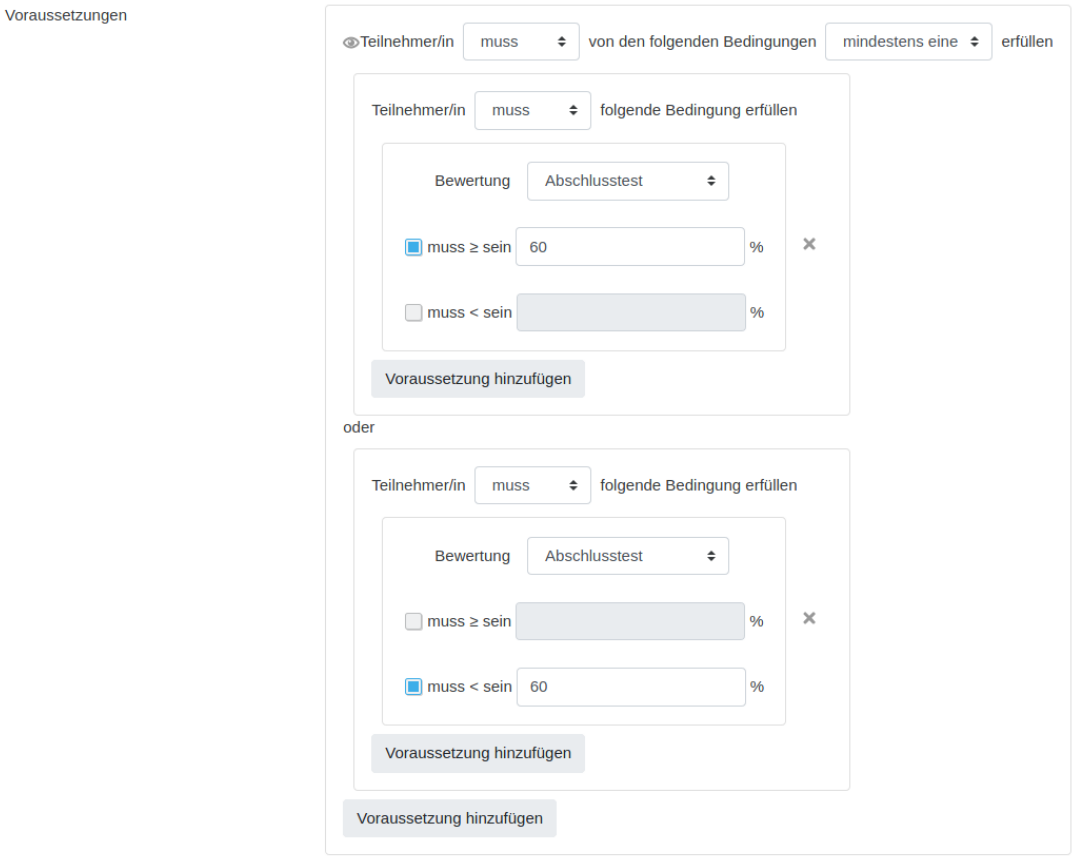


Abbildung 5.2.: Einstellung der Voraussetzungen für den Zugriff auf den Link zur Usability-Umfrage.

5.2.3. Durchführung

Die Umfrage wurde online geschaltet und die Antworten am 12.08.22 ausgewertet. Dies entspricht dem Stichtag, ab welchem auch die Tests nicht mehr durchgeführt werden konnten. Spätere eingehende Antworten konnten wegen des Fehlens der zugehörigen Lernerfolgsmessungen nicht beachtet werden. Zur Auswertung der Daten zur Usability, welche durch die Google Docs-Umfrage erhoben wurde, wurde der SUS-Score berechnet. Dazu wurde eine Antwort mit ”stimme überhaupt nicht zu” als der Wert 1 und eine Antwort mit ”stimme voll zu” als der Wert 5, sowie die dazwischen liegenden Antworten als entsprechende dazwischen liegende Werte interpretiert [TS17, S. 38]. Bei den Antworten 1, 3, 5, 7 und 9 wurde jeweils der Wert 1 abgezogen. Bei den Antworten 2, 4, 6, 8 und 10 wurden die entsprechenden Werte von 5 abgezogen. Die Werte wurden addiert und die Summe mit 2,5 multipliziert. Dadurch entstehen die SUS-Scores für einzelne Fragebögen [ebd]. Um daraus die Usability des gesamten Kurses zu ermitteln, wurde das arithmetische Mittel berechnet, indem die einzelnen SUS-Scores addiert und dann durch ihre Anzahl geteilt wurden.

5.2.4. Ergebnisse

Die SUS-Scores der einzelnen Probanden, sowie das arithmetische Mittel, können in Tab. 5.2 eingesehen werden. Bei allen Probanden, sowie im Mittel, wurde der minimale Wert von 68 überschritten. Da es möglich ist, die Scores in ein Notensystem zu übertragen [Klu17], können auch für die einzelnen Scores Noten vergeben werden. Dabei würden alle drei Scores und das Mittel einem A+ entsprechen, was im deutschen Schulsystem einer 1 entsprechen würde. Daraus folgt, dass die Usability des Kurses als gewährleistet angesehen werden kann.

Die Scores der einzelnen Fragen können in Anhang A eingesehen werden. Dabei fällt auf, dass Frage 1 insgesamt den niedrigsten Score erreicht, besonders da dies die einzige Frage ist, bei welcher bei Proband 1 und 2 nur ein Score von 2 erreicht wurde. Bei dieser Frage sollen Nutzende angeben, ob sie das Lernsystem gerne häufiger benutzen würden. Der niedrige Score könnte damit begründet werden, dass sich die Probanden nach Abschluss des Moduls selbst als kompetent in der IT-Sicherheit einstufen und deshalb eine weitere Nutzung des Moduls als wenig sinnvoll erachten.

Proband	Score
1	85
2	92,5
3	92,5
Mittel	90

Tabelle 5.2.: Berechnete SUS-Scores der einzelnen Probanden und im Mittel

Wie auch bei den Daten der Lernerfolgsmessung ist auch hier die Aussagekraft der Daten gering, da nur drei Probanden an der Evaluation teilnahmen. Deshalb sollte die Usability auch hier in einer möglichen Weiterführung des Projektes nochmals mit einer größeren Anzahl an Probanden evaluiert werden.

5.3. Teilnehmende

Im Folgenden sollen die teilnehmenden Probanden vorgestellt werden. Dabei soll zunächst erläutert werden, wie diese zur Teilnahme an dem Kurs rekrutiert wurden. Anschließend wird auf die Demografie der Teilnehmenden eingegangen. Die erhobenen demografischen Daten wurden lediglich anonymisiert verwendet. Zusätzlich wurden diese Daten nach Abschluss der Arbeit gelöscht, um einen Missbrauch dieser Daten zu verhindern.

5.3.1. Rekrutierung

Um Personen mit geringen Kompetenzen im Umgang mit digitalen Systemen als Teilnehmende zu gewinnen, wurden explizit Personen aus nicht-technischen Bereichen rekrutiert. Dazu wurde eine Rundmail an die Fakultät soziale Arbeit der Hochschule Mittweida gesandt, in welcher zur Teilnahme am Kurs und der Evaluation aufgerufen wurde. In dieser Mail wurden direkt die für die Einschreibung notwendigen Daten verschickt. Da hierdurch nur wenige Probanden gewonnen werden konnten, wurden Personen aus dem Bekanntenkreis herangezogen. Da der Kurs allerdings nur für Angehörige der Hochschule Mittweida zugänglich ist, nahmen diese Personen durch den Hochschul-Account des Autors an dem Kurs teil. Weil so durchgeführte Tests allerdings nicht in den Bewertungsstatistiken der Test erscheinen, wurde

hierfür zusätzliche, für andere Nutzende versteckte Tests verwendet. Um die Tests auswerten zu können, wurden bei diesen versteckten Tests die Bewertungseinstellungen verändert, sodass nach dem Abschluss eines Tests der Versuch mit Informationen über Richtigkeit der Antworten, sowie die erreichten Punkte angezeigt werden kann. Die Aufgaben sind identisch mit denen der entsprechenden anderen Tests. Um zu vermeiden, dass hierdurch die Lernerfolgsmessung verfälscht wird, da so die richtigen Antworten des Vortests eingesehen werden könnten, wurden diese Probanden während der Durchführung und Auswertung der Tests durch eine Bildschirmübertragung über den Instant-Messaging-Dienst Discord beobachtet. Die so erhobenen Daten wurden durch Screenshots gesichert und manuell zu den anderen Daten hinzugefügt. Anschließend wurden die versteckten Test-Elemente gelöscht, damit der Kurs exakt wie bei den Hochschul-Probanden weiter genutzt werden kann.

5.3.2. Demografie

Demografische Daten wurden über die Google Docs-Umfrage, welche auch zum Erfassen der Usability durch den SUS genutzt wurde, erhoben. Es wurden Grunddaten wie Alter und Geschlecht abgefragt. Zusätzlich wurde bei studierenden Teilnehmenden nach dem Studiengang, dem angestrebten Abschluss und dem Studienmodell gefragt. Diese Fragen enthielten ein Feld zur Eingabe einer eigenen Antwort, falls die vorgegebenen Antworten nicht zutreffend sind. Dabei konnten diese Fragen unbeantwortet gelassen werden, um zu signalisieren, dass die Person nicht studiert.

Zwei der Probanden stammten aus dem Bekanntenkreis des Autors, der dritte Proband ist Mitglied der Hochschule Mittweida und wurde durch die Rundmail rekrutiert. Beim Alter gab ein Proband 23 und die anderen beiden 24 Jahre an. Bei der Geschlechtsverteilung wurde jeweils einmal männlich, weiblich und divers angegeben. Die Probanden gaben alle an, in Vollzeit zu studieren. Dabei wurden als Studiengänge Biochemie, Soziale Arbeit und Wirtschaftsrecht genannt. Hierbei gaben zwei Probanden an, im Bachelor zu studieren und einer im Master.

Insgesamt wurde bei den Probanden eine Repräsentation unterschiedlicher Geschlechter und Fachrichtungen erreicht. Allerdings wäre es für die Evaluation sinnvoll gewesen, wenn Probanden aus anderen Altersstufen teilgenommen hätten, weil so die Verständlichkeit der Inhalte und die Usability des Moduls auch für weitere Gruppen evaluiert hätte werden können.

6. Zusammenfassung und Ausblick

In dieser Arbeit wurde das Konzept eines E-Learning Kurses zum Erwerb digitaler Kompetenzen im Bereich der IT-Sicherheit erstellt und dieses mit der Lernplattform Moodle umgesetzt. Dabei wurden allgemeine Informationen zur IT-Sicherheit vermittelt und die Themengebiete Passwörter, Phishing, Verschlüsselung und Malware behandelt. Die Vermittlung erfolgte überwiegend durch Videos, in welchen die Themengebiete in einer Kombination aus visuellen Darstellungen der Sachverhalte und auditiven Erklärungen unterrichtet wurden.

Der erstellte Kurs wurde nach den ersten beiden Ebenen des Kirkpatrick/Phillips-Modell evaluiert. Dabei wurde die Reaction durch eine Evaluation der Usability mittels System Usability Scale durchgeführt und der Lernerfolg durch eine Lernerfolgsmessung evaluiert. Bei der Usability konnten gute Ergebnisse erzielt werden, bei der Lernerfolgsmessung jedoch nicht. Allerdings haben die bei der Evaluation erhobenen Daten aufgrund der geringen Anzahl an Teilnehmenden nur eine geringe Aussagekraft.

In einer möglichen Weiterführung des Projektes sollte also eine weitere Evaluation mit einer größeren Anzahl an Teilnehmenden durchgeführt werden. Dabei sollte auch versucht werden, weitere Altersstufen als Probanden anzuwerben. Bei einer weiteren Evaluation der Usability könnten weitere Frameworks wie UMUX oder SUPR-Q verwendet werden, um die Aussagekraft der Bewertung zu steigern. Um die Wirkung des Moduls und die damit vermittelten Kompetenzen besser einschätzen zu können, sollten weitere Ebenen des Kirkpatrick/Phillips-Modells untersucht werden. Besonders eine Betrachtung der dritten Ebene, dem Behaviour, wäre sinnvoll, um Verhaltensänderungen durch die neu erworbenen Kompetenzen zu beobachten. Daneben wäre auch eine ästhetische Untersuchung in der Ebene der Reaction denkbar.

Literaturverzeichnis

[AVL19] Maxat Akbanov, Vassilios Vassilakis und Michael Logothetis: *WannaCry Ransomware: Analysis of Infection, Persistence, Recovery Prevention and Propagation Mechanisms*, *Journal of Telecommunications and Information Technology*, Bd. 01:S. 113–124, 2019.

[Bal11] Helmut Balzert: *Lehrbuch der Softwaretechnik: Entwurf, Implementierung, Installation und Betrieb*, Spektrum Akademischer Verlag Heidelberg, 2011, ISBN 978-3-8274-2246-0.

[Bri17] Volker Briegleb: *Ransomware WannaCry befällt Rechner der Deutschen Bahn*, 2017, URL: https://www.heise.de/newsticker/meldung/Ransomware-WannaCry-befaellt-Rechner-der-Deutschen-Bahn-3713426.html, besucht am 01.06.2022.

[Bro95] John Brooke: *SUS: A quick and dirty usability scale*, *Usability Evaluation in Industry*, Bd. 189:S. 4–7, 1995.

[BS21] Achim Berg und Sinan Selen: *Wirtschaftsschutz 2021*, 2021, URL: https://www.bitkom.org/sites/default/files/2021-08/bitkom-slides-wirtschaftsschutz-cybercrime-05-08-2021.pdf, besucht am 01.06.2022.

[BSI21] BSI: *Die Lage der IT-Sicherheit in Deutschland 2021*, 2021, URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2021.pdf?__blob=publicationFile&v=3, besucht am 01.06.2022.

[BSPL18] Veronika Brandstätter, Julia Schüler, Rosa Maria Puca und Ljubica Lozo: *Motivation und Emotion*, Springer Berlin, Heidelberg, 2018, ISBN 978-3-662-56685-5.

[bV22] bleib Virenfrei: *Bundespolizei Virus (BKA Trojaner) - So entfernen Sie ihn*, 2022, URL: https://www.bundespolizei-virus.de/, besucht am 01.06.2022.

[DSRL18] Gayle Davidson-Shivers, Karen Rasmussen und Patrick Lowenthal: *Web-Based Learning*, Springer Nature, 2018, ISBN 978-3-319-67840-5.

[Eck18] Claudia Eckert: *IT-Sicherheit*, De Gruyter Oldenbourg, 2018, ISBN 978-3-11-056390-0.

[Fay18] Sharifah Yaqoub Fayi: *What Petya/NotPetya Ransomware Is and What Its Remidiations Are*, *Advances in Intelligent Systems and Computing*, Bd. 738:S. 93–100, 2018.

[Fer12] Anusca Ferrari: *Digital Competence in Practice: An Analysis of Frameworks*, Publications Office of the European Union, 2012, ISBN 978-92-79-25093-4.

[Gab20] Roland Gabriel: *Revision von IT-Sicherheit*, 2020, URL: https://www.gabler-banklexikon.de/definition/it-sicherheit-70719/version-374912, besucht am 01.06.2022.

[GKBK19] Jun Gao, Pingfan Kong, Tegawendé Bissyandé und Jaques Klein: *Should You Consider Adware as Malware in Your Study?*, *IEEE International Conference on Software Analysis, Evolution and Reengineering*, Bd. 26:S. 604–608, 2019.

[Hei12] Andreas Heinecke: *Mensch-Computer-Interaktion*, Springer Berlin, Heidelberg, 2012, ISBN 978-3-642-13507-1.

[Hel18] Roland Hellman: *IT-Sicherheit*, De Gruyter Oldenbourg, 2018, ISBN 978-3-11-049485-3.

[HY16] Jiying Han und Hongbiao Yin: *Teacher motivation: Definition, research development and implications for teachers*, *Cogent Education*, Bd. 3, 2016.

[IBM22] IBM: *X-Force Threat Intelligence Index 2022*, 2022, URL: https://www.ibm.com/downloads/cas/ADLMYLAZ, besucht am 01.06.2022.

[JSC21] Cathy James-Springer und Katherine Cennamo: *A Tool for Determining e-Learning Readiness*, Springer Cham, 2021, ISBN 978-3-030-76994-9.

[Kal11] Salva Kalyuga: *Cognitive Load Theory: How Many Types of Load Does It Really Need?*, *Educational Psychology Review*, Bd. 23:S. 1–19, 2011.

[KGH15] Ernst Kircher, Raimund Girwidz und Peter Häußler: *Physikdidaktik*, Springer Spektrum Berlin, Heidelberg, 2015, ISBN 978-3-642-41745-0.

[KH07] Eckart Klieme und Johannes Hartig: *Kompetenzkonzepte in den Sozialwissenschaften und im erziehungswissenschaftlichen Diskurs*, *Kompetenzdiagnostik Zeitschrift für Erziehungswissenschaft*, Bd. 8:S. 11–29, 2007.

[KK06] Donald Kirkpatrick und James Kirkpatrick: *Evaluating Training Programs: The Four Levels*, Berret-Koehler Publishers, Inc., 2006, ISBN 978-1-57675-796-3.

[Klu17] Brandy Klug: *An Overview of the System Usability Scale in Library Website and System Usability Testing*, 2017, URL: https://quod.lib.umich.edu/w/weave/12535642.0001.602?view=text;rgn=main, besucht am 29.07.2022.

[KSK22] Ralf Knackstedt, Jürgen Sander und Jennifer Kolomitchouk: *Kompetenzmodelle für den Digitalen Wandel*, Springer Berlin, Heidelberg, 2022, ISBN 978-3-662-63673-2.

[Ltd18] Arhine Solutions Ltd: *Business Development through People Development*, 2018, URL: https://www.arhine.com/training.html, besucht am 01.06.2022.

[LWGK13] Van Lam Le, Ian Welch, Xiaoying Gao und Peter Komisarczuk (Hg.): *Anatomy of Drive-by Download Attack*, Proceedings of the Eleventh Australasian Information Security Conference (AISC 2013), Adelaide, Australia, Australian Computer Society, 2013.

[Mar17] Alice Marwick: *Scandal or sex crime? Gendered privacy and the celebrity nude photo leaks*, *Ethics and Information Technology*, Bd. 19:S. 117–191, 2017.

[MR17] Jochen Müsseler und Martina Riegler: *Allgemeine Psychologie*, Springer Berlin, Heidelberg, 2017, ISBN 978-3-642-53898-8.

[Mü10] Klaus-Rainer Müller: *Handbuch Unternehmenssicherheit*, Viweg+Teubner Verlag Wiesbaden, 2010, ISBN 978-3-8348-9772-5.

[Nob18] Calvin Nobles: *Botching Human Factors in Cybersecurity in Business Organizations*, *HOLISTICA*, Bd. 9:S. 71–88, 2018.

[NW20] Helmut Niegemann und Armin Weinberger: *Handbuch Bildungstechnologie*, Springer Berlin, Heidelberg, 2020, ISBN 978-3-662-63673-2.

[PS22] Mario Pfannstiel und Peter Steinhoff: *E-Learning im digitalen Zeitalter*, Springer Gabler Wiesbaden, 2022, ISBN 978-3-658-36113-6.

[Reu21] Christian Reuter: *Sicherheitskritische Mensch-Maschine-Interaktion*, Springer Fachmedien Wiesbaden GmbH, 2021, ISBN 978-3-658-32795-8.

[RN17] Ronny Richardson und Max North: *Ransomware: Evolution, Mitigation and Prevention*, *International Management Review*, Bd. 13:S. 10–21, 2017.

[RPY18] Bibin Rubini, Anna Permanasari und Winda Yuningsih: *Learning Multimedia Based on Science Literacy on the Lightning Theme*, *Jurnal Penelitian dan Pembelajaran IPA*, Bd. 4:S. 89–104, 2018.

[SG17] Tabea Scheel und Christine Gockel: *Humor at Work in Teams, Leadership, Negotiations, Learning and Health*, Springer Cham, 2017, ISBN 978-3-319-65691-5.

[SLW13] Daniel Süss, Claudia Lampert und Christine Wijen: *Medienpädagogik*, Springer VS, 2013, ISBN 978-3-531-19045-7.

[TS17] Meinald Thielsch und Martin Salaschek: *Toolbox zur kontinuierlichen Website-Evaluation und Qualitätssicherung (Version 2.1)*, Bundeszentrale für gesundheitliche Aufklärung (BZgA), Köln, 2017.

[Tud14] Uranchimeg Tudevdagva: *Structure Oriented Evaluation Model for E-Learning*, Dissertation, Technische Universität Chemnitz, 2014.

[Viv22] P Vivekananth: *Cybersecurity Risks in Remote Working Environment and Strategies to Mitigate Them*, *International Journal of Engineering and Management Research*, Bd. 12:S. 108–111, 2022.

[VPCGVdB16] Riina Vourikari, Yves Punii, Stephanie Carretero Gomez und Godelieve Van den Brande: *DigComp 2.0: The Digital Competence Framework for Citizens. Update Phase 1: the Conceptual Reference Model*, Publications Office of the European Union, 2016, ISBN 978-92-79-66966-8.

[WM09] Elke Wild und Jens Möller: *Pädagogische Psychologie*, Springer Berlin, Heidelberg, 2009, ISBN 978-3-540-88573-3.

[ZC12] Weiyuan Zhang und Y L Cheng: *Quality Assurance in E-Learning: PDPP Evaluation Model andits Application*, *International Review of Research in Open and Distributed Learning*, Bd. 13:S. 66–82, 2012.

Anhang

A. System Usability Scale Scores

Frage	Score
1	2
2	3
3	3
4	4
5	4
6	3
7	3
8	4
9	4
10	4
$\sum$	34

Tabelle A.1.: Scores der einzelnen Fragen von Proband 1

Frage	Score
1	2
2	4
3	4
4	4
5	3
6	4
7	3
8	4
9	4
10	4
$\sum$	37

Tabelle A.2.: Scores der einzelnen Fragen von Proband 2

Frage	Score
1	3
2	4
3	4
4	4
5	3
6	4
7	4
8	3
9	4
10	4
$\sum$	37

Tabelle A.3.: Scores der einzelnen Fragen von Proband 3

B. Konzepte von Zwischentests

B.1. Passwörter

Frage: **Wie läuft der Authentifizierungsprozess mittels Passwort ab?**

Antwort:

1. Eingabe des Passwortes
2. Erzeugen des Hashwertes des Passwortes
3. Abgleich mit dem hinterlegten Hash
4. Bewertung des Ergebnisses
5. Rückmeldung

Geprüfte Kenntnisse: technisches Hintergrundwissen zu Passwörtern

Frage: **Was macht ein Passwort sicher?**

Antwortmöglichkeiten:

- *Es sollte möglichst gut zu merken sein*
- Es muss möglichst lang sein
- Es muss möglichst viele unterschiedliche Zeichen haben
- Es sollte nicht aus Informationen über Nutzende erschlossen werden können
- *Es sollte möglichst menschenlesbar sein*

Geprüfte Kentnisse: Wissen über Faktoren eines starken Passwortes

Frage: **Welche Aussagen sind zutreffend?**

Antwortmöglichkeiten:

- Das Notieren eines Passwortes hat einen negativen Einfluss auf die Sicherheit
- *Passwortmanager machen alle Passwörter sicherer*
- *Es ist egal, ob ich mir ein Passwort merken kann, solange ich es in der Nähe meines Computers verstecken kann*
- Je weniger das Passwort verwendet wird, desto sicherer ist es
- Ein altes Passwort sollte man nicht nochmal verwenden

Geprüfte Kentnisse: Sicherer Umgang mit Passwörtern

Frage: **Geben Sie an, welche Passwörter sicher sind**

Antwortmöglichkeiten:

- *55555555555555555555555555555555*
- 4963684669736368653430526965736 56e4669736368654469654963684772696c6c65
- *456789*
- f9c1a7c2fc329aaabccd94cae507ebf6
- *Passwort*
- *donkey*
- IchFische40RiesenFischeDieIchGrille
- BrotErbseTorteBirneApfel!!!SchokiKeksBonbon

Geprüfte Kentnisse: Bewertung und Bildung von starken Passwörtern

B.2. Phishing

Frage: **Was beschreibt der Begriff "Phishing"?**

Antwortmöglichkeiten:

- *Ein Angriff auf wassergekühlte Computer, bei dem die Wasserkühlung zum Auslaufen gebracht wird*
- Angreifende geben vor offiziell von Banken, OnlineShops, Behörden oder ähnlichem zu kommen, um Daten, wie Passwörter, zu stehlen
- *Das Fälschen von Webseiten*

Geprüfte Kentnisse: Definition des Begriffes "Phishing"

Frage: **Ordnen Sie die Begriffe zu den Bestandteilen einer URL zu**

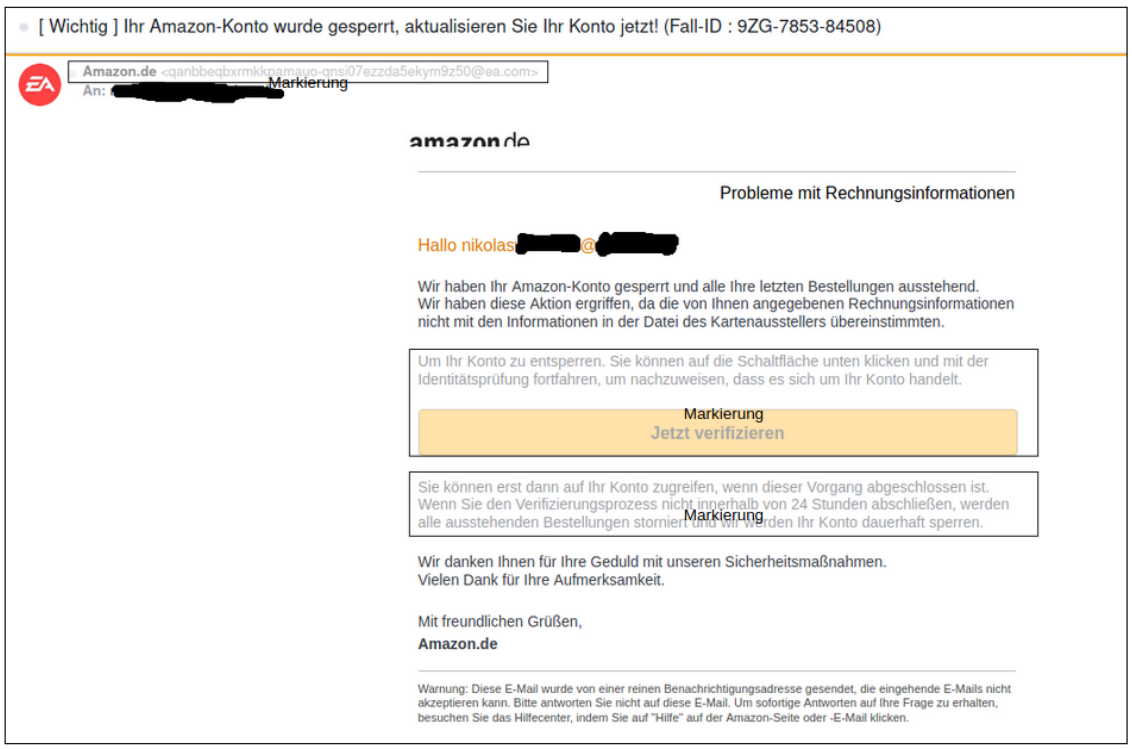
Antwort:

- Übertragungs-Protokoll $\longrightarrow$ https://
- Subdomain $\longrightarrow$ de.
- Hauptdomain $\longrightarrow$ wikipedia
- Top-Level-Domain $\longrightarrow$ .org
- Dateipfad $\longrightarrow$ /wiki/Phishing

Geprüfte Kentnisse: Aufbau von URLs

Frage: **Markieren Sie Bereiche, durch welche Sie feststellen können, dass es sich hierbei um einen Phishing-Angriff handelt. Es handelt sich hier um drei Bereiche, allerdings haben Sie unbegrenzte Markierungen zur Verfügung.**

Antwort:



Geprüfte Kentnisse: Erkennung von Phishing

Frage: **Welche Aussagen zur Zwei-Faktor-Authentifikation sind korrekt?**

Antwortmöglichkeiten:

- Eine Zwei-Faktor-Authentifikation schützt Accounts besser vor unbefugtem Zugriff als ein Passwort alleine
- *Eine Zwei-Faktor-Authentifikation verhindert den Diebstahl von Daten komplett*
- Durch Zwei-Faktor-Authentifikation werden gestohlene Zugangsdaten für Angreifende wertloser
- *In durch Zwei-Faktor-Authentifikation geschützte Accounts kann nicht eingebrochen werden*

Geprüfte Kentnisse: Verständnis der Zwei-Faktor-Authentifikation

B.3. Verschlüsselung

Frage: **Welche Aussage ist korrekt?**

Antwortmöglichkeiten:

- Verschlüsselung überführt Klartexte in Kryptotexte, damit die enthaltenen Informationen nur von bestimmten Personen genutzt werden können
- *Verschlüsselung überführt Kryptotexte in Klartexte, damit die Daten sicher vor Diebstahl sind*
- *Verschlüsselung macht Daten unleserlich, damit diese nicht mehr verwendet werden können*

Geprüfte Kentnisse: Allgemeine Funktionsweise der Verschlüsselung

Frage: **Was sind mögliche Anwendungsfälle von Verschlüsselung?**

Antwortmöglichkeiten:

- Schutz vor dem Abhören von Daten, welche per WLAN übertragen werden
- *Schutz vor Tracking*
- Signieren von Dokumenten
- Schutz von Vertraulichen Daten
- *Nachweis der Authentizität von Webseiten*

Geprüfte Kentnisse: Wissen über Anwendungsmöglichkeiten der Verschlüsselung

Frage: **Bringen Sie die zur Verschlüsselung einer E-Mail notwendigen Schritte in die richtige Reihenfolge.**

Antwort:

1. Verschlüsselungsfunktion aktivieren
2. Schlüssel erstellen
3. Schlüssel austauschen

4. Mail verfassen
5. Verschlüsselte Mail versenden

Geprüfte Kentnisse: Wissen über den Vorgang der Verschlüsselung einer Mail

B.4. Malware

Frage: **Wie kann man seinen Computer mit Malware infizieren?**

Antwortmöglichkeiten:

- *Direkte Verbindung mit dem Router*
- Infizierte Werbung
- E-Mail-Anhänge
- *Installation von Anti-Malware-Software*
- Besuch von infizierten Webseite

Geprüfte Kentnisse: Wissen über Malware-Infektionswege

Frage: **Sie erhalten eine verdächtige Mail mit einem Anhang. Was tun Sie?**

Antwortmöglichkeiten:

- *Den Anhang sofort öffnen*
- Den Absender überprüfen
- Den Anhang mit einem speziellen Tool auf Schädlichkeit prüfen
- *Sofort eine Antwort verfassen*

Geprüfte Kentnisse: Verhalten bei verdächtigen Mails

Frage: **Welche Aussagen sind korrekt?**

Antwortmöglichkeiten:

- *Das Deaktivieren von JavaScript hat nur Vorteile*

- *Ich sollte bei der Nutzung Adminrechte haben*
- Eine Malwareinfektion kann durch das Besuchen einer Webseite ausgelöst werden
- Back-ups von meinen Daten sollten nicht auf dem gleichen Computer gespeichert sein

Geprüfte Kentnisse: Prävention von Malwareinfektionen

Frage: **Was können Sie bei einer Malwareinfektion tun?**

Antwortmöglichkeiten:

- *Den Rechner herunterfahren*
- Die Systemwiederherstellung nutzen
- Das System neu aufsetzen
- Durch Anti-Virus-Programme entfernen lassen
- *Back-ups machen*

Geprüfte Kentnisse: Verhaten bei einer Malwareinfektion

Frage: *Ist die folgende Aussage wahr oder falsch?*

Anti-Virus-Programme verbessern erheblich die Sicherheit eines Computers.

Antwortmöglichkeiten:

- *Wahr*
- Falsch

C. Vortest

Frage: **Welche Aussagen treffen zu?**

Antwortmöglichkeiten:

- *Ich sollte möglichst viel zusätzliche Software zum Schutz meines Computers installieren.*
- IT-Sicherheit schützt Computer und Daten vor Schaden, Manipulation und Verlust.
- *Cyberkriminelle würden keine Endnutzenden angreifen.*
- Passwörter sind sicherer, je besser man sie sich merken kann.
- Durch den Besuch einer Website kann mein Computer mit Malware infiziert werden.

Punkte: 4

Geprüfte Kentnisse: Grundlegendes Verständnis der IT-Sicherheit

Frage: **Wählen Sie sichere Passwörter aus!**

Antwortmöglichkeiten:

- HeuteHoleIchMirDie48KinderDerKönigin!
- cef96d56f1ec720fd5de7431e09254c303b76974
- *xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx*
- *123456789*
- *arbeitszimmer*

Punkte: 12

Geprüfte Kentnisse: Bildung und Bewertung von starken Passwörtern

Frage: **Woran können Sie erkennen, dass die Webseite echt ist?**

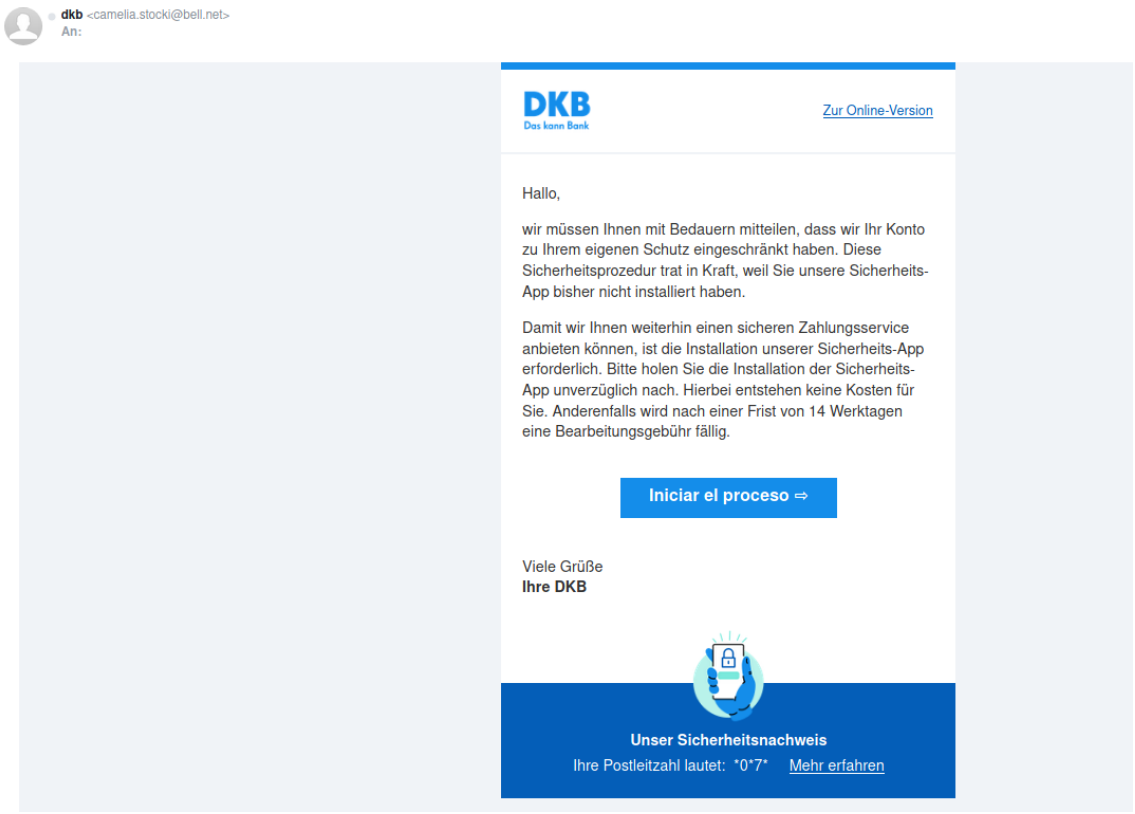
Antwortmöglichkeiten:

- An der URL
- An der Funktionalität der Links auf der Webseite
- An den abgefragten Daten
- *Am Namen*
- *Am Impressum*
- *An der Verschlüsselung*

Punkte: 14

Geprüften Kentnisse: Erkennung von gefälschten Webseiten.

Frage: **Handelt es sich bei dieser Mail um Phishing?**



Antwortmöglichkeiten:

- Ja
- Nein

Punkte: 14

Geprüfte Kentnisse: Erkennung von Phishing-Mails

Frage: **Welche Aussagen sind zutreffend?**

Antwortmöglichkeiten:

- *Bei der symmetrischen Verschlüsselung werden für das Ver- und Entschlüsseln unterschiedliche Schlüssel verwendet.*
- *Durch die Verschlüsselung wird das Schutzziel der Verfügbarkeit erreicht.*
- Bei der Entschlüsselung mit dem falschen Schlüssel entstehen nur unbrauchbare Daten.

- *Es ist nicht möglich, E-Mails zu verschlüsseln.*
- Es ist möglich, unterschiedliche Daten zu verschlüsseln.

Punkte: 6

Geprüfte Kentnisse: Grundverständnis der Verschlüsselung

Frage: **Welche Aussage trifft auf diese Webseite zu?**

Antwortmöglichkeiten:

- *Die Webseite ist verschlüsselt übertragen worden*
- *Diese Webseite kann nicht gefälscht werden*
- Die Webseite wurde nicht verschlüsselt übertragen
- *Die Funktionalität ist auch ohne JavaScript gewährleistet*

Punkte: 6

Geprüfte Kentnisse: Erkennung der verschlüsselten Übertragung von Webseiten

Frage: **Bringen Sie die zur Verschlüsselung einer E-Mail notwendigen Schritte in die richtige Reihenfolge.**

Antwortmöglichkeiten:

- Ich sollte E-Mails mit meinem privaten Schlüssel verschlüsseln.
- Ich muss vor dem Senden von verschlüsselten E-Mails meinen öffentlichen Schlüssel teilen.
- *Ich sollte E-Mails mit meinem öffentlichen Schlüssel verschlüsseln.*
- *E-Mails sind bereits von sich aus verschlüsselt.*
- *Verschlüsselte E-Mails werden langsamer an den Empfänger weitergeleitet.*

Punkte: 10

Geprüfte Kentnisse: Verschlüsselung von E-Mails

Frage: **Wodruch kann ein Computer mit Malware infiziert werden?**

Antwortmöglichkeiten:

- Werbung
- *Direkte Verbindung mit dem Router*
- Downloads
- Erhaltene Dateien
- *Anschließen von Geräten*

Punkte: 10

Geprüfte Kentnisse: Wissen über Malware-Infektionswege

Frage: **Welche Maßnahmen sind zur Prävention einer Infektion mit Malware geeignet?**

Antwortmöglichkeiten:

- Blockieren von Werbung
- Ausführen von Dateien verbieten
- Dateien unbekannter Quelle ablehnen
- *Starke Passwörter*
- *Nur HTTPS-Verschlüsselte Webseiten aufrufen*

Punkte: 12

Geprüfte Kentnisse: Prävemtionsmaßnahmen gegen Malware

Frage: **Was sollten Sie im Falle einer Malware-Infektion tun?**

Antwortmöglichkeiten:

- Ich sollte die Systemwiederherstellung verwenden
- *Ich sollte einen anderen Computer verbinden, um über diesen wichtige Daten zu retten*
- Ich sollte die CD suchen, mit welcher ich das Betriebssystem installierte, um dieses neu zu installieren
- *Ich sollte sämtlichen angezeigten Aufforderungen nachkommen*

- *Ich sollte den Computer neustarten.*

Punkte: 12

Geprüfte Kentnisse: Verhalten bei Malwareinfektionen

D. Abschlusstest

Frage: **Welche Aussagen treffen zu?**

Antwortmöglichkeiten:

- *Anti-Virus-Programme erhöhen immer die Sicherheit eines Computers*
- IT-Sicherheit schützt Computer und Daten vor Schaden, Manipulation und Verlust.
- *Nur Unternehmen, Banken und andere wichtige Institutionen werden Ziele von IT-Angriffen*
- Je weniger ein Passwort bekannt ist, desto sicherer ist es
- Ransomware ist die größte Sicherheitsbedrohung im Internet

Punkte: 4

Geprüfte Kenntnisse: Grundlegendes Verständnis der IT-Sicherheit

Frage: **Wählen Sie sichere Passwörter aus!**

Antwortmöglichkeiten:

- Die42GummibärchenInMeinemMundSindSehrLecker!
- ad3a667860b8929935b63be8ac0801dc4d66c63f
- *11111111111111111111111111111111111111111111111111111111111111*
- *password*
- *abcdefghijklmnopqrstuvwxyz123456789*

Punkte: 12

Geprüfte Kenntnisse: Bildung und Bewertung von starken Passwörtern

Frage: **Woran können Sie eine gefälschte Webseite erkennen?**

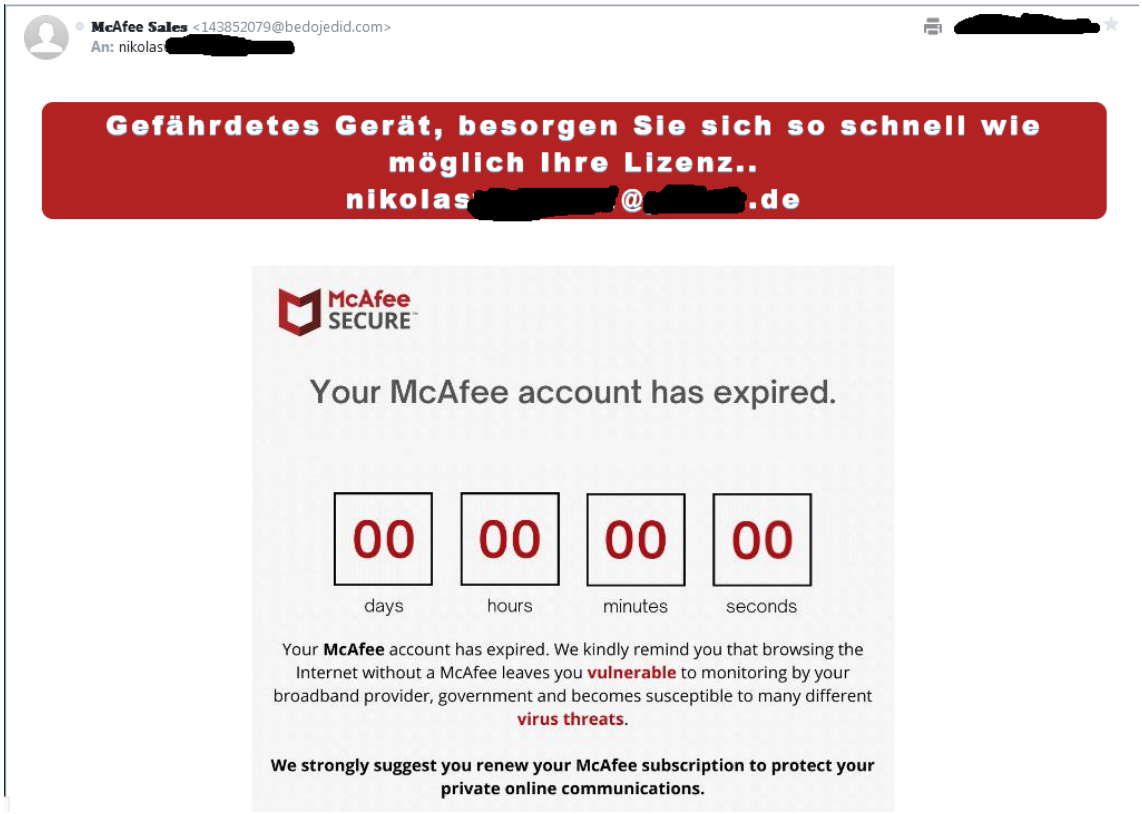
Antwortmöglichkeiten:

- An der URL
- Am Zertifikat, welches für die Verschlüsselung verwendet wird
- An der Rechtschreibung
- *An der IP-Adresse*
- *Am Impressum*
- *An der Verschlüsselung*

Punkte: 14

Geprüfte Kenntnisse: Erkennung von gefälschten Webseiten

Frage: **Handelt es sich bei der folgenden Mail um Phishing?**



Antwortmöglichkeiten:

- Ja
- Nein

Punkte: 14

Geprüfte Kenntnisse: Erkennung von Phising-Mails

Frage: **Welche Aussagen sind zutreffend?**

Antwortmöglichkeiten:

- *Asymmetrische Verschlüsselung verwendet beim Ver- und Entschlüsseln den gleichen Schlüssel*
- *Verschlüsselung dient dem Schutzziel der Authentizität*
- Schlüssel sind Informationen, welche für das Ver- und Entschlüsseln von Daten benötigt werden

- *E-Mails werden automatisch verschlüsselt*
- Man kann alle Dateien verschlüsseln

Punkte: 6

Geprüfte Kenntnisse: Grundverständnis der Verschlüsselung

Frage: **Welche Aussage trifft auf diese Webseite zu?**

Antwortmöglichkeiten:

- *Die Webseite ist nicht verschlüsselt übertragen worden*
- *Die Webseite kann nicht mit Malware infiziert sein*
- Die Webseite wurde verschlüsselt übertragen
- *Die Webseite wurde verschlüsselt übertragen und funktioniert ohne JavaScript*

Punkte: 6

Geprüfte Kenntnisse: Erkennung der verschlüsselten Übertragung von Webseiten

Frage: **Bringen Sie die zur Verschlüsselung einer E-Mail notwendigen Schritte in die richtige Reihenfolge.**

Antwort:

1. Verschlüsselungsfunktion aktivieren
2. Schlüssel erstellen
3. Schlüssel austauschen
4. Mail verfassen
5. Verschlüsselte Mail versenden

Punkte: 10

Geprüfte Kenntnisse: Verschlüsselung von E-Mails

Frage: **Wodruch kann ein Computer mit Malware infiziert werden?**

Antwortmöglichkeiten:

- Werbung
- *WLAN-Verbindung*
- Webseiten
- E-Mail-Anhänge
- *Anschließen von Geräten wie Fernsehern oder Lautsprechern*

Punkte: 10

Geprüfte Kenntnisse: Wissen über Malware-Infektionswege

Frage: **Welche Maßnahmen sind zur Prävention einer Infektion mit Malware geeignet?**

Antwortmöglichkeiten:

- Deaktivieren von JavaScript
- Möglichst geringe Nutzerrechte haben
- Mail-Anhänge ablehnen
- *Mails verschlüsseln*
- *Zwei-Faktor-Authentifikation*

Punkte: 12

Geprüfte Kenntnisse: Präventionsmaßnahmen gegen Malware

Frage: **Was sollten Sie im Falle einer Malware-Infektion tun?**

Antwortmöglichkeiten:

- Ich sollte sämtliche Verbindungen von einem infizierten Computer zu anderen Computern und dem Internet trennen.
- *Ich sollte sofort ein Back-up sämtlicher wichtiger Daten durchführen*
- Ich sollte die nötigen Vorbereitungen treffen, um das System neu aufzusetzen.
- *Ich sollte bei einer Infektion mit einer Ransomware prüfen welche Zahlungsmethoden akzeptiert werden.*

- *Ich sollte den Computer neustarten*

Punkte: 12

Geprüfte Kenntnisse: Verhalten bei Malwareinfektionen

Selbstständigkeitserklärung

Hiermit erkläre ich, daß ich die vorliegende Arbeit selbstständig angefertigt, nicht anderweitig zu Prüfungszwecken vorgelegt und keine anderen als die angegebenen Hilfsmittel verwendet habe. Sämtliche wissentlich verwendete Textausschnitte, Zitate oder Inhalte anderer Verfasser wurden ausdrücklich als solche gekennzeichnet.

Selbitz, den 7. Oktober 2022

Nikolas Weber