BERGISCHE
UNIVERSITÄT
WUPPERTAL

# Du kommst hier nicht rein!

Passwortsicherheit für Alle!

**Autor: Dennis Olbrich**

**Forschungsprojekt**

Master of Education
Teilstudiengang Informatik
Lehramt an Berufskolleg (BK)

Bergische Universität Wuppertal
Fakultät für Mathematik und Naturwissenschaften
Didaktik der Informatik
Erstgutachterin: Frau Denise Schmitz
Abgabedatum: 10. Juli 2025

Die vorliegende Arbeit steht unter einer Creative Commons Lizenz, die das Teilen und das Bearbeiten des Materials erlaubt. Die Bedingungen der Lizenz (CC BY-NC-SA 4.0) können hier eingesehen werden:

https://creativecommons.org/licenses/by-nc-sa/4.0/deed.de

# Inhaltsverzeichnis

# Abbildungsverzeichnis

# Tabellenverzeichnis

# 1 Einleitung

## 1.1 Das Projekt ComeMint

Das Verbundsprojekt *ComeMINT* ist Teil des *Kompetenzverbunds lernen:digital* und entwickelt forschungsbasierte Fortbildungsangebote für Lehrer*innen in den MINT-Fächern Mathematik, Informatik, Naturwissenschaften und Technik mit einem besonderen Fokus auf informatische Bildung (vgl. Essen, 2024). Ziel ist es, Konzepte zu erstellen, die Lehrer*innen befähigen, digitale Lehr-Lern-Prozesse didaktisch sinnvoll zu gestalten und kontinuierlich zu optimieren. Dabei werden sowohl informatische Kompetenzen als auch die fachdidaktische Integration digitaler Medien gefördert.

Die Fortbildungsmodule sind adaptiv aufgebaut und berücksichtigen die heterogenen Bedarfe der Teilnehmer*innen. Sie werden in sogenannten CommunityNets lokal, regional und bundesweit erprobt und evaluiert. Im Rahmen der begleitenden Entwicklungsforschung werden diagnostische Instrumente und Peer-Reviews eingesetzt, um Gelingensbedingungen und Transferstrategien für digitale Fortbildungsangebote im Bildungssystem zu identifizieren und zu untersuchen.

Durch den interdisziplinären Ansatz, die Integration von Themen wie Bildung für nachhaltige Entwicklung und Inklusion sowie die kritische Reflexion von Digitalisierungspotenzialen und -barrieren leistet ComeMINT einen wichtigen Beitrag zur Professionalisierung von Lehrer*innen im digitalen Zeitalter.

Für weitere Details wird auf die offiziellen Projektwebseiten verwiesen (Essen, 2024) und (Wuppertal, 2024).

## 1.2 Das Modul *Digitale Selbstverteidigung*

Ein Fortbildungsmodul, dass innerhalb von ComeMINT untersucht und weiterentwickelt wird, ist das von Denise Schmitz im Vorgängerprojekt (*ComeIn*)entwickelte Fortbildungsangebot *SPAM von der Schulleitung? - Digitale Selbstverteidigung* (kurz: Digitale Selbstverteidigung) (Schmitz, 2024). Es richtet sich an angehende Lehrer*innen und sensibilisiert sie für verschiedene Aspekte eines sicheren Umgangs mit digitalen Medien. Die Kapitel des Moduls sind didaktisch so aufgebaut, dass die jeweiligen Themen zunächst eingeführt und die damit verbundenen Risiken dargestellt werden. Daran anschließend folgen praktische Übungen, in denen die Teilneh-

mer*innen das erworbene Wissen direkt anwenden, ihr eigenes Verhalten reflektieren und ihre individuellen Kompetenzen im Bereich der digitalen Sicherheit vertiefen können. Auf die Inhalte des Moduls *Digitale Selbstverteidigung* wird im Folgenden Kapitel tiefer eingegangen.

## 1.3 Problemstellung

Im Rahmen des Projekts ComeIN wurde das Modul *Digitale Selbstverteidigung* entwickelt, das Lehrer*innen für den sicheren Umgang mit digitalen Medien sensibilisiert. Allerdings sind die ursprünglichen Lernangebote im Modul *Digitale Selbstverteidigung* kognitiv und textorientiert gestaltet. Dies kann insbesondere für Personen mit unterschiedlichen Lernstilen, Vorerfahrungen oder Sinnesbeeinträchtigungen zu Barrieren beim Wissenserwerb führen.

Gerade der Themenbereich *Passwortsicherheit* stellt in der Praxis eine besondere Herausforderung dar: Sichere Passwortgestaltung ist ein komplexes Thema mit hohen Anforderungen an das Verständnis abstrakter Sicherheitsprinzipien. Gleichzeitig sind die Konsequenzen unsicheren Verhaltens für viele Nutzerinnen oft schwer greifbar und werden häufig erst im Schadensfall (Gestohlene E-Mail-Zugänge, manipulierte Online-Konten, Datenraub etc.) deutlich. Dies erschwert die Motivation zur Verhaltensänderung und macht eine anschauliche, praxisnahe Vermittlung besonders wichtig.

Ausgehend von diesen Herausforderungen bestand der Bedarf, das bestehende Modul *Digitale Selbstverteidigung* gezielt weiterzuentwickeln, um auch für heterogene Zielgruppen einen niederschwelligen Zugang zu sicherheitsrelevanten Inhalten zu ermöglichen.

## 1.4 Zielsetzung

Ziel des Forschungsprojekts war es, eine auf dem Modul *Digitale Selbstverteidigung* basierende Lernanwendung zur Passwortsicherheit zu entwickeln, die den Ansatz der sensorischen Parallelisierung umsetzt. Durch die parallele Ansprache verschiedener Sinneskanäle (visuell, auditiv, haptisch) sollen unterschiedliche Lernvoraussetzungen berücksichtigt und Barrieren im Wissenserwerb abgebaut werden.

Im Zentrum der praktischen Umsetzung steht die Entwicklung einer prototypischen webbasierten Übung, die visuelle und auditive Elemente kombiniert, um die Lerninhalte anschaulich und verständlich darzustellen. Darüber hinaus wurde ein ergänzendes haptisches Konzept erarbeitet, das die sensorische Parallelisierung perspektivisch noch erweitern könnte. Dieses haptische Element liegt bislang jedoch nur als theoretische Idee vor und wurde im Rahmen des Projekts nicht praktisch umgesetzt.

## 1.5 Aufbau der Arbeit

Die vorliegende Arbeit beginnt mit der Darstellung der Ausgangslage des Projekts. Dabei wird das zugrundeliegende Modul *Digitale Selbstverteidigung* vorgestellt, das inhaltlich die Grundlage für die durchgeführte Forschungsarbeit bildet. Im Rahmen dieser Darstellung werden sowohl die thematischen Schwerpunkte als auch die im Modul zu entwickelnden Kompetenzen erläutert.

Im Anschluss werden die theoretischen Grundlagen der sensorischen Parallelisierung erläutert. Zunächst erfolgt eine allgemeine Einführung in das Prinzip und die didaktischen Hintergründe dieser Methode. Daran anschließend wird die Anwendung sensorisch-parallelisierter Ansätze im Kontext der Informatik näher betrachtet. Zudem wird dargelegt, inwiefern sensorische Parallelisierung zur Förderung von Bildungsgerechtigkeit beitragen kann.

Darauf folgend wird das eigentliche Forschungsprojekt beschrieben. Hier werden die im Entwicklungsprozess entstandenen Ideen, die während der Projektarbeit aufgetretenen Herausforderungen sowie die daraus resultierende finale Konzeptidee systematisch dargestellt.

Anschließend wird die entwickelte Webseite dokumentiert. Neben einer Beschreibung der Funktionalitäten und der inhaltlichen Struktur erfolgt eine detaillierte Darstellung der Umsetzung.

Im weiteren Verlauf wird ein Leitfaden zur Integration der entwickelten Übung in das bestehende Modul *Digitale Selbstverteidigung* vorgestellt. Dabei werden die didaktischen Schwerpunkte der Übung sowie konkrete Hinweise für die praktische Durchführung innerhalb des Moduls erläutert.

Abschließend werden mögliche Erweiterungen des entwickelten Konzepts diskutiert. Hierzu zählt insbesondere die theoretisch entwickelte haptische Ergänzung, die perspektivisch zur weiteren Ausgestaltung sensorisch-parallelisierter Lernzugänge beitragen kann. Die Arbeit schließt mit einem Ausblick auf den möglichen Transfer der entwickelten Ansätze in den schulischen Unterricht sowie einem persönlichen Fazit zur Projektdurchführung ab.

# 2 Die Ausgangslage: Das Modul *Digitale Selbstverteidigung*

Im Rahmen des Projekts ComeIN wurde das Fortbildungsmodul *Digitale Selbstverteidigung* entwickelt, das Lehrer*innen auf den sicheren Umgang mit digitalen Medien vorbereitet. Ziel des Moduls ist es, Lehrer*innen sowohl für Risiken als auch für Schutzmechanismen im digitalen Raum zu sensibilisieren und praktische Handlungskompetenz entwickeln zu lassen.

Das Modul ist in drei thematische Schwerpunkte untergliedert: der Faktor Mensch, Datentransfer im Netz und Schadsoftware. Zu jedem Themenbereich werden sowohl Hintergrundinformationen als auch praktische Übungen angeboten, sodass die Teilnehmer*innen ihr Wissen direkt anwenden und vertiefen können. Die praktische Umsetzung erfolgt dabei häufig in Form von Übungen, Simulationen und Reflexionsphasen.

## 2.1 Der Faktor Mensch

Den ersten und besonders umfangreichen inhaltlichen Schwerpunkt bildet der Themenbereich »der Faktor Mensch«. Hier erwerben die Teilnehmer*innen grundlegende Kenntnisse zu verschiedenen Authentifizierungsverfahren, zur sicheren Passwortgestaltung, sowie zu typischen Angriffsmethoden wie Brute-Force- oder Wörterbuchangriffe, Rainbowlisten und Social Engineering. Die Notwendigkeit starker, individueller Passwörter wird ebenso thematisiert wie der Umgang mit Passwortmanagern, die Möglichkeiten der sicheren Passwortverwaltung und die Rolle der Anbieter*innen beim Schutz gespeicherter Passwörter. In den praktischen Übungen erstellen die Teilnehmer*innen unter anderem eine eigene Passwort-Datenbank mit KeePassXC(KeePassXC, 2025), nutzen Passwortgeneratoren, prüfen eigene E-Mail-Adressen auf Datenlecks über haveibeenpwned.com(Pwned, 2025) und analysieren

die Sicherheit von Passwörtern mit verschiedenen Onlinediensten. Zusätzlich reflektieren sie, welche persönlichen Daten für mögliche Angreifende von Interesse sein könnten.

## 2.2 Datentransfer im Netz

Ein weiterer Themenblock widmet sich den Datentransfer im Netzwerk. Hier werden die unterschiedlichen Arten von personenbezogenen Daten ebenso behandelt wie die Gefahren, die sich aus der Verknüpfung von Accounts ergeben. Die Teilnehmer*innen setzen sich mit Risiken der Identitätsdiebstahls, den Mechanismen der Datenerhebung und -weitergabe sowie den Datenschutzpflichten von Anbieter*innen auseinander. Ziel ist es, ein kritisches Bewusstsein für den Umgang mit den eigenen Daten und den angebotenen Diensten zu entwickeln.

Des Weiteren beschäftigen sich die Teilnehmer*innen mit dem Aufbau und der Funktionsweise von Netzwerken und der technischen Infrastruktur des Internets. Hierzu gehören Grundlagen des Client-Server-Prinzips, der Funktionsweise von Webseiten und Datenströmen sowie der Verschlüsselung durch HTTPS und Zertifikate. Die Teilnehmer*innen lernen, wie Netzwerke abgesichert werden können, welche Gefahren durch ungeschützte Netzwerke entstehen und wie Sicherheitslücken systematisch geschlossen werden.

## 2.3 Schadsoftware

Schließlich setzt sich das Modul im Bereich Schadsoftware mit den verschiedenen Arten von Schadsoftware auseinander. Es werden unter anderem Würmer, Viren und Trojaner behandelt. Außerdem werden Cookies und Browser-Fingerprinting sowie die damit verbundenen Gefahren der Profilbildung und Überwachung thematisiert. Gleichzeitig lernen die Teilnehmer*innen auch Maßnahmen kennen, um Tracking zu reduzieren oder ganz zu vermeiden. Dabei wird immer wieder der Spannungsbogen zwischen Benutzerkomfort und Datenschutz kritisch reflektiert.

## 2.4 Exkurse

Neben den drei zentralen Themenbereichen des Moduls werden auch zwei optionale Exkurse angeboten. Diese beschäftigen sich mit dem Schutz der eigenen Gesundheit sowie dem Schutz der eigenen Umwelt.

## 2.5 Lernziele und Kompetenzen

Nach Abschluss des Moduls sollen die Teilnehmer*innen Kompetenzen im Bereich der informatischen Sicherheit entwickelt haben. Unter anderem sollen Sie etwa in der Lage sein, Angriffsarten im Internet zu identifizieren und zu erläutern, Verteidigungsmechanismen zum Schutz ihrer digitalen Daten gezielt anzuwenden und Sicherheitsrisiken im Umgang mit Informatiksystemen systematisch zu bewerten und geeignete Schutzmaßnahmen zu treffen. Darüber hinaus erwerben sie die Fähigkeit, geeignete Authentifizierungsverfahren abhängig von der jeweiligen Sicherheitsanforderung auszuwählen und professionell zu verwalten. Eine vollständige Aufzählung der zu entwickelnden findet sich in (Schmitz, 2024, S. 7)

# 3 Sensorische Parallelisierung als didaktischer Ansatz

## 3.1 Einleitung

Die Gestaltung barrierefreier und inklusiver Lernangebote stellt eine der zentralen Herausforderungen des modernen Bildungssystems dar. Im Zuge wachsender gesellschaftlicher Diversität sowie des technischen Wandels stehen Lehrer*innen zunehmend vor der Aufgabe, Bildungsangebote für heterogene Lerngruppen zugänglich und wirksam zu gestalten. Dies betrifft nicht nur Schüler*innen mit ausgewiesenen Förderbedarfen, sondern grundsätzlich alle Lernenden mit unterschiedlichen Vorerfahrungen, Fähigkeiten, Wahrnehmungs- und Verarbeitungsstilen.

Gerade komplexe Themenbereiche wie die digitale Selbstverteidigung und insbesondere die Passwortsicherheit bringen zahlreiche kognitive Anforderungen mit sich, die für viele Lernende zunächst abstrakt und schwer greifbar erscheinen. Vor diesem Hintergrund gewinnt der didaktische Ansatz der sensorischen Parallelisierung zunehmend an Bedeutung. Durch die gezielte parallele Ansprache verschiedener Sinneskanäle können Lerninhalte verständlicher, anschaulicher und nachhaltiger vermittelt werden. Sensorische Parallelisierung leistet somit einen wichtigen Beitrag zur Barrierefreiheit und fördert gleichzeitig die Qualität des Lernprozesses für alle Lernenden.

## 3.2 Begriff und Ausprägungen der sensorischen Parallelisierung

Der Begriff der sensorischen Parallelisierung beschreibt ein didaktisches Konzept, bei dem Lerninhalte über mehrere Sinneskanäle simultan und miteinander verzahnt vermittelt werden. Ziel ist es, durch die Kombination von visuellen, auditiven, haptischen und – in seltenen Fällen – auch olfaktorischen oder gustatorischen Zugängen unterschiedliche Wahrnehmungsvoraussetzungen und Lernpräferenzen von Schülerinnen zu adressieren. Die parallele Aktivierung verschiedener Sinne erhöht die Wahrscheinlichkeit, dass Lernende Inhalte besser aufnehmen, verarbeiten und langfristig erinnern können (vgl. Capovilla, 2015, S. 51ff.).

In der praktischen Umsetzung bedeutet sensorische Parallelisierung beispielsweise, dass ein abstraktes Konzept wie die Passwortsicherheit nicht allein durch textbasierte Erklärungen anschaulich wird. Stattdessen wird es durch erklärende Grafiken, schematische Darstellungen, erklärende Audiospuren, interaktive Übungen und – sofern möglich – auch durch physische Objekte veranschaulicht. Diese mehrdimensionalen Sichtweisen ermöglichen es Lernenden, Wissen auf unterschiedlichen Wegen zu erschließen, und bietet somit alternative Zugänge für Personen, die in einzelnen Sinnesmodalitäten Einschränkungen oder besondere Stärken aufweisen.

Die konkrete Ausgestaltung sensorisch-parallelisierter Lernumgebungen orientiert sich dabei an verschiedenen Materialformen: Visuelle Materialien umfassen beispielsweise Piktogramme, Grafiken oder Animationen; auditive Materialien können gesprochene Erklärungen, akustische Signale oder Hörbeispiele integrieren; haptische Materialien ermöglichen die taktile Auseinandersetzung mit Lerninhalten, etwa durch Modelle, Bewegungselemente oder taktile Hilfsmittel (vgl Kohl, 2023, S. 25ff.).

Sensorische Parallelisierung versteht sich somit nicht als bloße Wiederholung derselben Information in verschiedenen Formaten, sondern vielmehr als eine didaktisch begründete, funktionale Aufbereitung, die sowohl Redundanzen als auch komplementäre Ergänzungen schafft. Damit wird einerseits die kognitive Belastung reduziert und andererseits das Verständnis durch vielfältige Zugänge vertieft.

## 3.3 Relevanz für den Informatikunterricht

Der Informatikunterricht stellt in besonderer Weise hohe kognitive und abstrakte Anforderungen an die Lernenden. Grundlegende Konzepte wie Datenstrukturen, Algorithmen, Netzwerke oder Sicherheitsmechanismen sind oft schwer greifbar und erfordern ein erhebliches Maß an Abstraktionsvermögen. Gleichzeitig eröffnet die Informatik aber auch spezifische Chancen, um inklusiven Unterricht zu gestalten: Viele der in der Informatik entwickelten Technologien sind selbst Grundlage für barrierefreie Kommunikation und Partizipation, wie beispielsweise Bildschirmleseprogramme, Sprachausgabe-Software, alternative Eingabegeräte oder automatische Texterkennungsverfahren (vgl. Kohl, 2023, S. 4f.).

Die Integration sensorisch-parallelisierter Lernmaterialien kann hier einen doppelten Effekt erzielen: Einerseits werden Lerninhalte zugänglicher gestaltet und somit Barrieren abgebaut. Andererseits werden die Lernenden für die Bedeutung und Möglichkeiten barrierefreier Technologien sensibilisiert, die selbst Gegenstand der informatischen Bildung sind. Dies macht den Informatikunterricht zu einem besonders geeigneten Feld für die Anwendung und Weiterentwicklung sensorischer Parallelisierung.

## 3.4 Sensorische Parallelisierung als Beitrag zu Bildungsgerechtigkeit und Inklusion

Der Zugang zu hochwertiger Bildung ist international und national als fundamentales Menschenrecht verankert. Die Vereinten Nationen haben mit der Behindertenrechtskonvention (UN-BRK) und insbesondere mit deren Artikel 24 das Recht auf inklusive Bildung als völkerrechtlichen Standard definiert vgl. (vgl. Vereinte Nationen, 2006). Inklusive Bildung zielt dabei nicht allein auf die Integration von Menschen mit ausgewiesenem Förderbedarf, sondern auf die umfassende Teilhabe aller Menschen an qualitativ hochwertiger Bildung – unabhängig von individuellen Besonderheiten, sozialen Hintergründen oder Beeinträchtigungen.

Sensorische Parallelisierung unterstützt diesen Anspruch auf mehreren Ebenen. Durch die differenzierte Ansprache verschiedener Sinne wird die Wahrscheinlichkeit erhöht, dass Lerninhalte von einer möglichst großen Bandbreite an Lernenden verstanden werden können. Dies betrifft nicht nur Schüler*innen mit Sinnes- oder Lernbeein-

trächtigungen, sondern schließt auch Lernende mit unterschiedlichen Vorerfahrungen, Sprachständen oder kognitiven Stilen ein. Durch den Abbau unnötiger Barrieren wird ein fairer und chancengleicher Zugang zum Unterricht gefördert.

Gleichzeitig unterstützt sensorische Parallelisierung das Konzept des Universal Design for Learning (UDL). UDL fordert, Lernangebote von vornherein so zu gestalten, dass sie für alle Lernenden zugänglich sind, anstatt individuelle Nachteilsausgleiche nachträglich zu schaffen (vgl. (Hall u. a., 2012)). Sensorische Parallelisierung erfüllt zentrale Prinzipien dieses Ansatzes, indem sie flexible Repräsentationen von Inhalten ermöglicht, vielfältige Handlungsmöglichkeiten eröffnet und differenzierte Formen der Lernzielkontrolle begünstigt.

Somit erweist sich sensorische Parallelisierung nicht nur als ein methodisches Instrument zur Reduktion von Barrieren, sondern auch als ein normativ begründeter Beitrag zur Realisierung von Chancengleichheit und sozialer Gerechtigkeit im Bildungssystem. Durch den Einsatz solcher Ansätze im Informatikunterricht wird Inklusion praktisch erlebbar und zur gelebten Normalität im schulischen Alltag.

## 3.5 Sensorische Parallelisierung als allgemeiner Qualitätsgewinn für alle Lernenden

Sensorische Parallelisierung leistet nicht nur einen Beitrag zur Inklusion von Menschen mit dauerhaften Beeinträchtigungen, sondern verbessert grundsätzlich die Lernbedingungen für alle Lernenden. Es kann zwischen dauerhaften, temporären und situativen Beeinträchtigungen unterschieden werden (Arbeit und Soziales, 2025). Während dauerhafte Beeinträchtigungen beispielsweise in Form von Sinnes- oder Mobilitätseinschränkungen auftreten, können temporäre Beeinträchtigungen durch Verletzungen, Krankheiten oder altersbedingte Faktoren entstehen. Situative Beeinträchtigungen wiederum ergeben sich aus äußeren Umständen, etwa einer lauten Lernumgebung, schlechten Lichtverhältnissen oder sprachlichen Hürden bei mehrsprachigen Lernenden.

Durch die parallele Bereitstellung von Lerninhalten über verschiedene Sinne wird es den Lernenden ermöglicht, alternative Zugänge zu nutzen, wenn ein bestimmter Sinneskanal vorübergehend oder dauerhaft beeinträchtigt ist. So können beispielsweise akustische Erklärungen eine visuelle Überforderung kompensieren, visuelle Darstel-

lungen eine eingeschränkte Hörfähigkeit ausgleichen oder haptische Modelle die kognitive Erfassung komplexer Prozesse erleichtern.

Sensorische Parallelisierung erhöht damit insgesamt die Flexibilität des Lernangebots und trägt dazu bei, Lernbarrieren frühzeitig abzufedern, bevor sie zu tatsächlichen Lernhindernissen werden. Im Sinne des UDL entstehen so Lernumgebungen, die für alle Beteiligten zugänglicher, verständlicher und nachhaltiger gestaltet sind – unabhängig von individuellen Einschränkungen oder situativen Erschwernissen.

# 4 Das Forschungsprojekt: Von der Idee zur Umsetzung

## 4.1 Ausgangslage und Zielsetzung

Das hier vorgestellte Forschungsprojekt entstand im Rahmen von ComeMINT und soll dabei helfen, das Modul *Digitale Selbstverteidigung* sensorisch parallel zu gestalten. Initiiert wurde das Projekt durch einen Impuls von Denise Schmitz, der Autorin des Moduls *Digitale Selbstverteidigung*.

Ursprünglich war geplant, sämtliche Übungsaufgaben des bestehenden Moduls im Sinne der sensorischen Parallelisierung vollständig neu zu konzipieren. Ziel war es, für alle Themenbereiche – Passwortsicherheit, persönliche Daten im Netzwerk, Netzwerke und Tracking – barrierearme, multisensorische Lernangebote zu entwickeln. Im Verlauf der ersten Konzeptionsphase zeigte sich jedoch rasch, dass eine vollständige Überarbeitung sämtlicher Aufgaben innerhalb des verfügbaren Projektzeitraums den Rahmen sprengen würde. Umfang und Komplexität des Vorhabens wären kaum noch mit den zur Verfügung stehenden Ressourcen vereinbar gewesen. Aus diesem Grund wurde der Fokus des Projekts auf den Themenbereich der Passwortsicherheit gelegt.

Die Entscheidung für diesen Themenbereich beruhte auf mehreren Überlegungen: Zum einen stellt die Passwortsicherheit einen zentralen Baustein der digitalen Selbstverteidigung dar und besitzt hohe praktische Relevanz für die Alltagspraxis der Lernenden. Gleichzeitig handelt es sich um ein Themenfeld, dessen Inhalte häufig abstrakt bleiben und daher schwer zugänglich erscheinen. Begriffe wie Hash-Funktionen, Angriffsarten oder auch Social Engineering erfordern ein hohes Maß

an Vorwissen und Vorstellungskraft, um die dahinterliegenden Prozesse wirklich zu verstehen. Gerade dieser Abstraktionsgrad erzeugt jedoch für viele Lernende eine kognitive Barriere, die es zu überwinden gilt. Zudem wird die Bedeutung sicherer Passwörter in der Praxis vielfach unterschätzt oder gar nicht richtig verstanden, wodurch Angreifer häufig mit relativ einfachen Mitteln erfolgreich sind.

Durch diese inhaltliche Schwerpunktsetzung eröffnete sich die Möglichkeit, am Beispiel der Passwortsicherheit exemplarisch sensorisch-parallelisierte Lernzugänge zu entwickeln und diese im Rahmen einer didaktisch sinnvollen Übung praktisch umzusetzen.

## 4.2 Erste Konzeptideen

In der Anfangsphase des Projekts entstanden verschiedene Ansätze, um die abstrakten Inhalte der Passwortsicherheit anschaulich, barrierearm und multisensorisch zugänglich zu machen. Ein erster Lösungsansatz war die Entwicklung von physischen Lernmaterialien. Hierbei sollten kleine Plättchen mit Piktogrammen und Braille-Schrift eingesetzt werden, mit deren Hilfe die Lernenden Wörter und Passphrasen zusammensetzen könnten. Ergänzend dazu war angedacht, mit Hilfe einer Schablone den Ablauf einer Hash-Funktion visuell und haptisch zu veranschaulichen, um den Prozess der Einwegverschlüsselung nachvollziehbarer zu machen.

Inhaltlich erschien dieser Ansatz vielversprechend, da er eine direkte taktile Auseinandersetzung mit dem Thema ermöglicht hätte. Praktisch stellten sich jedoch bald erhebliche Hürden: Die Produktion solcher Materialien wäre mit hohen Kosten verbunden gewesen, insbesondere, wenn zusätzlich noch barrierefreie Varianten (z. B. taktile Oberflächen, Braille-Beschriftungen) hätten bereitgestellt werden sollen. Zudem wären diese Materialien nur in Präsenzveranstaltungen einsetzbar gewesen und hätten eine aufwändige Logistik für die Lehrenden erfordert.

Im Anschluss wurde die Idee verfolgt, eine spezielle Softwareanwendung zu entwickeln, die die geplanten Inhalte digital aufbereiten sollte. Jedoch zeigte sich auch hier schnell ein grundlegendes Problem: Eine eigene Software müsste auf den Endgeräten der Teilnehmer*innen installiert werden.

Dies bringt sowohl technische als auch organisatorische Herausforderungen mit sich. Unterschiedliche Betriebssysteme, eingeschränkte Installationsrechte, begrenzter Speicherplatz und individuelle Kompatibilitätsprobleme wären potenzielle Hindernisse für eine barrierefreie Anwendung.

Ein weiterer Lösungsansatz war die Entwicklung eines rein auditiven Lernangebots in Form eines Podcasts. Hierbei hätte die Thematik der Passwortsicherheit ausschließlich über akustische Erklärungen vermittelt werden sollen. Zwar hätte dieser Ansatz den Zugang für sehbeeinträchtigte Personen erleichtert, jedoch zeigte sich, dass ein rein auditiver Zugang ebenfalls hohe Anforderungen an die kognitive Vorstellungskraft stellt. Besonders bei abstrakten technischen Konzepten, wie der Funktionsweise von Hash-Algorithmen oder Angriffsszenarien wie Brute-Force- oder Wörterbuchangriffen, erwies sich die ausschließliche Nutzung des auditiven Kanals als unzureichend.

## 4.3 Schwierigkeiten und Reflexion

Der Findungsprozess gestaltete sich zunehmend anspruchsvoll. Obwohl das Thema der Barrierefreiheit und sensorischen Parallelisierung im Zentrum des Projekts stand, war es geradezu paradox, wie schwer es fiel, sich in die unterschiedlichen Perspektiven der betroffenen Nutzerinnengruppen hineinzuversetzen. Trotz eigener Seheinschränkungen (Brille) gelang es nur bedingt, sich vollständig in die Bedürfnisse von Menschen mit erheblich eingeschränkten Sinnesleistungen hineinzuversetzen. Oft waren die theoretischen Ansätze zwar gut nachvollziehbar, die praktische Umsetzung jedoch mit unerwarteten Schwierigkeiten verbunden.

Erst durch eine bewusste Distanzierung vom Problem — ausgelöst durch einen Spaziergang am Strand, der dem Kopf Raum für neue Ideen ließ — entstand ein Perspektivwechsel. Aus der Entlastung heraus entstand die entscheidende Idee, die geplante Übung auf eine Webseite zu übertragen.

## 4.4 Die finale Idee: Die Webanwendung als sensorisch-paralleles Lernangebot

Die Wahl fiel schließlich bewusst auf die Entwicklung einer webbasierten Lernanwendung. Webtechnologien bieten mehrere entscheidende Vorteile, die den Anforderungen an barrierearme, multisensorische Lernangebote besonders entgegenkommen.

Zunächst ist der Zugang zu Webseiten niederschwellig: Nahezu alle Lernenden verfügen über mobile Endgeräte, auf denen ein Webbrowser standardmäßig installiert ist. Unabhängig vom Betriebssystem oder von Geräteklassen lässt sich eine Webseite plattformunabhängig und ohne zusätzliche Installationen aufrufen. Zudem lassen sich Webseiten durch ihre Gestaltung flexibel an individuelle Bedürfnisse anpassen. Viele Endgeräte bieten systemseitig Funktionen wie Vergrößerung, Kontrastanpassung, Screenreader-Unterstützung oder Sprachsteuerung, die die Nutzung auch für Menschen mit Beeinträchtigungen erleichtern. Gleichzeitig wird kein besonderes technisches Vorwissen benötigt, um den Zugang herzustellen. Selbst in Situationen ohne stabiles WLAN kann häufig durch persönliche Hotspots dennoch auf die Lerninhalte zugegriffen werden.

Inhaltlich ermöglicht die Webseite die didaktisch geplante Verknüpfung von unterschiedlichen Sinneskanälen. Die Lernenden können interaktiv die Funktionsweise von Brute-Force- und Wörterbuchangriffen nachvollziehen, Hashfunktionen visualisiert erleben und konkrete Angriffsszenarien aus dem Bereich des Social Engineerings durchspielen. Dabei werden sowohl visuelle Erklärungen, schematische Animationen, textbasierte Erklärungen als auch auditive Elemente (durch Screenreader) kombiniert, um ein möglichst umfassendes und inklusives Lernerlebnis zu gestalten.

Mit der Realisierung der Webanwendung konnte das Ziel, einen sensorisch parallelisierten Lernzugang zum Thema Passwortsicherheit zu schaffen, in einer praktikablen, niedrigschwelligen und technisch robusten Form umgesetzt werden. Diese Lösung stellt den zentralen praktischen Beitrag des Forschungsprojekts dar und bildet die Grundlage für die nachfolgende Dokumentation der Webseite.

# 5 Dokumentation der entwickelten Webseite

In diesem Kapitel wird die entwickelte Webseite dokumentiert, die im Rahmen des Forschungsprojekts als sensorisch-parallelisiertes Lernangebot zum Thema Passwortsicherheit entstanden ist. Ziel dieser Dokumentation ist es, die Struktur und die Funktionsweise der Anwendung detailliert darzulegen und so zukünftige Erweiterungen oder Modifikationen zu erleichtern. Ergänzend zu dieser Beschreibung wird empfohlen, den Quellcode der Anwendung direkt zu konsultieren, da dieser umfangreich kommentiert ist und in Verbindung mit diesem Kapitel ein umfassendes Verständnis der Implementierung ermöglicht.

## 5.1 Struktur der Webseite

Die entwickelte Anwendung basiert auf einer webbasierten Architektur, um eine möglichst niederschwellige Nutzung auf unterschiedlichsten Endgeräten zu gewährleisten. Dabei wurde bewusst auf zusätzliche Installationen oder Abhängigkeiten von Drittsoftware verzichtet. Die Anwendung lässt sich direkt in jedem gängigen Webbrowser öffnen und kann somit auf stationären Computern, Laptops, Tablets oder Smartphones gleichermaßen genutzt werden. Diese Entscheidung trägt den zuvor beschriebenen Barrierefreiheitsaspekten Rechnung, da die Endgeräte der Nutzerinnen meist bereits individuell an deren Bedürfnisse angepasst sind (z. B. durch Vergrößerungsfunktionen, Screenreader, Sprachsteuerung oder Kontrasteinstellungen).

Die Verzeichnisstruktur der Anwendung ist klar gegliedert, um eine einfache Wartbarkeit und Erweiterbarkeit zu ermöglichen. Das Hauptverzeichnis `codebreaker_website` unterteilt sich in mehrere logisch getrennte Unterverzeichnisse:

Listing 1: Die Verzeichnisstruktur

```
codebreaker_website
|---- javascript
|     |---- modules
|     |     |---- codebreaker.js
|     |     |---- scenarios.js
|     |---- main.js
|
|---- resources
|     |---- scenarios
|     |     |---- s01_living_room.png
|     |     |---- s02_home_office.png
|     |     |---- sc_1_private.html
|     |     |---- sc_2_hash.html
|     |     |---- solutions.md
|     |---- unused
|     |     |---- s03_work_office.png
|     |     |---- s04_desktop.png
|     |---- favicon.png
|
|---- wordlists
|     |---- 10-million-password-list-top-1000000.txt
|
|---- LICENSE
|---- main.css
|---- main.html
|.... README.md
```

**javascript** Im Verzeichnis `javascript` befinden sich alle JavaScript-Komponenten, die die Funktionalität der Anwendung steuern. Innerhalb des Verzeichnisses `modules` sind spezifische Funktionen ausgelagert, die den modularen Aufbau der Anwendung unterstützen. In `main.js` werden die verschiedenen Elemente der Webseite und grundlegende Funktionen verwaltet (siehe Kapitel 5.2).

**resources** Das Verzeichnis `resources` enthält Bildmaterial, Szenario-Daten sowie vorbereitete HTML-Seiten mit H5P Inhalten zur Einbindung von Lerninhalten. Dabei wurden auch Ressourcen vorgehalten, die für mögliche zukünftige Szenarien vorgesehen sind.

**wordlists** Das Verzeichnis `wordlists` enthält Passwortlisten, die für die Simulation von Wörterbuchangriffen genutzt werden.

Ergänzend finden sich im Hauptverzeichnis die zentrale HTML-Datei main.html, das Stylesheet main.css zur Gestaltung der Benutzeroberfläche sowie begleitende Dokumente wie `LICENSE` und `README.md`.

Die bewusst schlanke und transparente Dateistruktur ermöglicht es, die Webseite auch ohne umfangreiche Vorkenntnisse im Webdevelopment zu verstehen und bei Bedarf gezielt weiterzuentwickeln.

## 5.2 Aufbau und Funktionsweise der zentralen Module

Die Logik der Webseite wird hauptsächlich durch drei JavaScript-Dateien gesteuert:

In der `main.js` werden alle globalen Variablen, Bedienelemente und Zustände der Anwendung verwaltet. Hier werden beispielsweise die Benutzerinteraktionen (z. B. Eingaben, Button-Aktivierungen oder Moduswechsel) erfasst und an die jeweils zuständigen Funktionsmodule weitergeleitet. Eine zentrale Rolle spielt dabei die `textarea`, die ein simuliertes Terminalfenster darstellt und den Lernenden eine visuelle Rückmeldung der jeweiligen Prozesse bietet. Die Interaktion über ein solches Terminal wurde bewusst gewählt, da es typische Kommandozeilenprozesse im Bereich der informatischen Sicherheit visuell nachempfindet und gleichzeitig die Brücke zwischen technischer Realität und didaktischer Vereinfachung schlägt.

In `codebreaker.js` sind die Kernfunktionen der Passwortangriffe und Hash-Berechnungen implementiert. Hier wird sowohl der Brute-Force-Angriff als auch der Wörterbuchangriff simuliert. Ergänzend dazu werden drei unterschiedliche Hash-Funktionen angeboten, die – obwohl didaktisch vereinfacht – zentrale Prinzipien der Einwegverschlüsselung veranschaulichen. Die Wahl einer simplifizierten Darstellung erfolgte bewusst, um das Grundprinzip der Hashfunktionen anschaulich zu vermitteln, ohne die Lernenden mit der mathematischen Komplexität realer Verfahren zu überfordern.

Die Datei `scenarios.js` steuert den Ablauf der interaktiven Szenarien. Hier werden Texte und Prüfmechanismen für die Szenarien verwaltet. Über diese Funktionalität wird sichergestellt, dass die Lernenden schrittweise Hinweise erhalten, Aufgaben lösen und ihre Ergebnisse im simulierten Terminal überprüfen können.

## 5.3 Funktionen der Anwendung

Die Webseite bietet derzeit drei Hauptfunktionen, die jeweils unterschiedliche Aspekte der Passwortsicherheit adressieren: den **Angriffsmodus**, den **Hashmodus** und den **Szenariomodus**.

Allen drei Modi ist gemein, dass sie über eine zentrale Eingabemaske gesteuert werden. Diese ermöglicht es den Lernenden, Passwörter einzugeben oder je nach Modi auch einen Modulo-Wert festzulegen.


Abbildung 1: Eingabemöglichkeiten der Anwender*in

Des Weiteren können die Lernenden über ein Dropdown-Menü den gewünschten Modus auswählen. Diese Auswahl beeinflusst sowohl die Darstellung der Benutzeroberfläche als auch die Funktionalität der Anwendung.

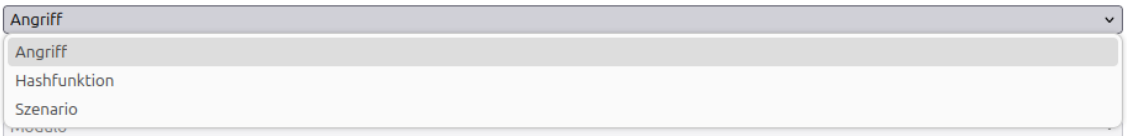


Abbildung 2: Dropdown-Menü - Modusauswahl

### 5.3.1 Angriffsmodus

Im Angriffsmodus haben die Lernenden die Möglichkeit, zwei klassische Angriffsmethoden praktisch nachzuvollziehen: den Brute-Force- und den Wörterbuchangriff. Diese Methoden sind bewusst gewählt, da sie grundlegende Angriffsstrategien im Kontext von Passwortsicherheit darstellen und in der Praxis häufig Anwendung finden.

Beim Brute-Force-Angriff wird systematisch jede mögliche Zeichenkombination ausprobiert, bis das eingegebene Passwort gefunden wurde. Aus Gründen der Veranschaulichung sind in der aktuellen Version lediglich Kleinbuchstaben und eine maximale Passwortlänge von fünf Zeichen vorgesehen. Diese Einschränkungen dienen der Verständlichkeit und der Rechenzeitoptimierung in einer webbasierten Lernumgebung. Für längere Passwörter wird eine Zeitabschätzung vorgenommen, um den exponentiellen Anstieg der Rechenzeit bei zunehmender Passwortlänge zu verdeutlichen.

Der Wörterbuchangriff greift auf eine hinterlegte Passwortliste zurück. Diese Liste simuliert, wie Angreifer mit Hilfe häufig verwendeter Passwörter systematisch versuchen, Zugangsdaten zu kompromittieren. Die Lernenden können so selbst nachvollziehen, wie unsichere Passwortmuster zur leichten Angreifbarkeit beitragen.[1].

[1] Die verwendete Wortliste basiert auf einer veralteten 10-Millionen-Passwörter-Liste. Alternative oder neue Listen sind hier zu finden: (Miessler, 2025)

### 5.3.2 Hashmodus

Der Hashmodus dient der Visualisierung von Hashfunktionen als zentralem Konzept der Passwortsicherheit. Den Lernenden stehen drei vereinfachte Varianten zur Verfügung, bei denen Modulo-Operationen auf ASCII-Codes der Passwortzeichen durchgeführt werden.

Dabei werden grundlegende Eigenschaften von Hashfunktionen – wie die Einwegfunktion und die Abhängigkeit von der Passwortlänge – anschaulich demonstriert. Durch die Möglichkeit, den Modulo-Wert selbst zu definieren, wird zudem ein gewisser experimenteller Spielraum eröffnet. Gleichzeitig wird den Lernenden bewusst gemacht, dass es sich hierbei nicht um echte, kryptografisch sichere Hashfunktionen handelt, sondern um didaktisch reduzierte Modelle zur Vermittlung des Grundprinzips.

Folgende Hashfunktionen sind implementiert:


Abbildung 3: Dropdown-Menü - Hashfunktionen

- **Modulo**: Zu jedem Buchstaben des Wortes wird der entsprechende ASCII-Code (Zahl) gebildet. Auf diesen wird eine Modulo-Operation durchgeführt. Der Modulo wird durch die Anwender*innen bestimmt. Abschließend werden die Werte der einzelnen Buchstaben zu einem Wert aufaddiert.
- **Modulo / Divide**: Zusätzlich zu **Modulo**: Abschließend wird dieser Wert durch die Länge des Passwortes geteilt. Dadurch wird verdeutlicht, dass die Länge des Passwortes einen Einfluss auf den Hashwert haben kann.
- **Modulo / Multiply**: Zusätzlich zu **Modulo**: Abschließend wird dieser Wert mit der Länge des Passwortes multipliziert. Dadurch wird verdeutlicht, dass die Länge des Passwortes einen Einfluss auf den Hashwert haben kann.

**Hinweis**: Wenn kein Modulo bestimmt wird, wird der Standardwert 5 benutzt.

### 5.3.3 Szenariomodus

Im Szenariomodus werden die erworbenen Kenntnisse in praxisnahen Anwendungssituationen erprobt. Die Szenarien kombinieren verschiedene Aspekte der Passwortsicherheit, darunter auch Methoden des Social Engineerings sowie Hash-Analysen.

Im ersten Szenario »Andreas Zuhause« müssen die Lernenden auf Grundlage verstreuter Hinweise ein Passwort rekonstruieren. Dabei wird verdeutlicht, wie persönliche Daten, die offen zugänglich oder leicht recherchierbar sind, von Angreifern zur Passwortableitung genutzt werden können.

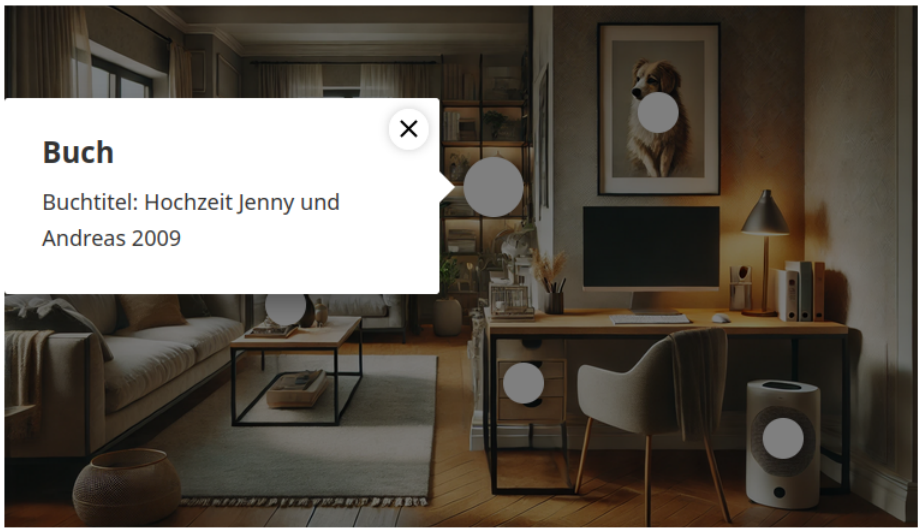


Abbildung 4: Szenario - Andreas Zuhause - Passwort knacken - Erstellt mit der Hilfe von DALL·E von OpenAI

Im zweiten Szenario »Ginseng Cloud« soll ein verloren gegangenes Passwort durch Rückrechnung eines Hashwertes wiederhergestellt werden. Hierbei werden die zuvor vermittelten Grundlagen der Hashfunktionen in einer realitätsnahen Problemstellung angewendet.

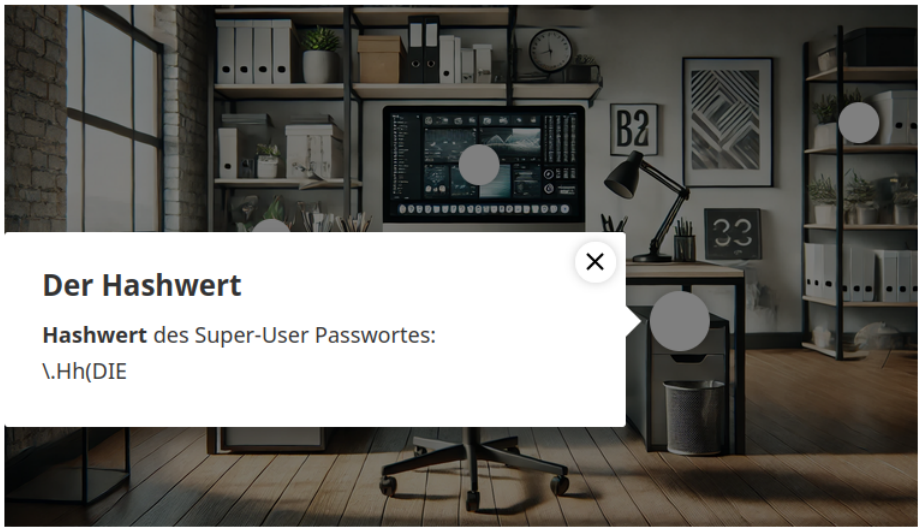


Abbildung 5: Szenario - Ginseng Cloud - Hashwert knacken - Erstellt mit der Hilfe von DALL·E von OpenAI

Beide Szenarien fördern das analytische Denken und schärfen das Bewusstsein der Lernenden für typische Schwachstellen im eigenen Passwortverhalten.

Der genaue Aufbau der Szenarien sowie die jeweiligen Hinweise und Lösungen sind in der Datei `ressources/scenarios/solutions.md` dokumentiert. Diese Dokumentation ermöglicht es Lehrenden, die Szenarien flexibel in ihre Unterrichtsplanung zu integrieren und bei Bedarf anzupassen.

## 5.4 Aufbau der Webseite und technische Begründungen

Bereits bei der Konzeption der Webseite war ein zentrales Ziel, maximale Barrierearmut mit hoher Verfügbarkeit zu kombinieren. Die Wahl einer rein webbasierten Anwendung wurde bewusst getroffen, um die systemseitigen Barrieren einer Softwareinstallation vollständig zu vermeiden. Dies erlaubt den Zugriff unabhängig vom

verwendeten Endgerät, Betriebssystem oder individuellen Administrationsrechten.

Darüber hinaus profitieren die Lernenden von der Adaptivität ihrer eigenen Geräte: Schriftgrößen, Kontrastanpassungen, alternative Eingabemethoden und Hilfstechnologien wie Screenreader werden bereits systemseitig unterstützt und greifen direkt auch auf die Webseite zu. Gleichzeitig werden keine sensiblen Daten gespeichert oder an externe Server übertragen, was datenschutzrechtliche Anforderungen ebenfalls berücksichtigt.

Die Entscheidung für eine möglichst reduzierte technische Infrastruktur spiegelt sich auch im Einsatz einfacher HTML-, CSS- und JavaScript-Strukturen wider. So bleibt die Anwendung nicht nur wartungsfreundlich, sondern lässt sich auch von Lehrpersonen ohne tiefgehende Programmierkenntnisse grundsätzlich nachvollziehen und anpassen.

## 5.5 Barrierefreiheit und Zugänglichkeit im Test

### 5.5.1 Auswahl der Barrierefreiheitsprüfwerkzeuge

Für die Überprüfung der Barrierefreiheit der entwickelten Webanwendung wurde das Analysewerkzeug WAVE (Web Accessibility Evaluation Tool) ausgewählt.

**WAVE Web Accessibility Evaluation Tool** Das WAVE-Tool (entwickelt von WebAIM) bietet eine browserbasierte Analyse von Webseiten hinsichtlich gängiger Barrierefreiheitskriterien. Es identifiziert unter anderem fehlende Alternativtexte bei Bildern, fehlerhafte oder unvollständige Überschriftenhierarchien, Kontrastprobleme, unzureichende ARIA-Attribute[2] sowie potenziell problematische Formularbeschriftungen. Darüber hinaus visualisiert WAVE die gefundenen Barrieren direkt auf der Webseite, was eine schnelle Lokalisierung und Korrektur erleichtert.

[2] ARIA-Attribute (Accessible Rich Internet Applications) sind spezielle HTML-Erweiterungen, die Menschen mit Behinderungen den Zugang zu dynamischen Webinhalten erleichtern. Sie helfen dabei, zusätzliche Informationen über Rollen, Zustände oder Eigenschaften von Elementen an Screenreader und andere assistive Technologien zu übermitteln.

WAVE orientiert sich dabei am internationalen Standard der Web Content Accessibility Guidelines (WCAG) 2.1, der aktuell als maßgeblicher Leitfaden für die Barrierefreiheit von Webinhalten gilt. Die WCAG 2.1 umfasst die vier Prinzipien (Kirkpatrick u. a., 2025):

- Wahrnehmbarkeit (Perceivable): Inhalte müssen für alle Sinne zugänglich sein.
- Bedienbarkeit (Operable): Inhalte und Navigation müssen für alle bedienbar sein.
- Verständlichkeit (Understandable): Inhalte müssen verständlich und nachvollziehbar aufbereitet sein.
- Robustheit (Robust): Inhalte müssen mit unterschiedlichen Technologien kompatibel sein.

WAVE erkennt automatisiert prüfbare Verstöße gegen diese Prinzipien und bietet zusätzlich Hinweise zu möglichen Problemstellen, die einer manuellen Überprüfung bedürfen.

### 5.5.2 Auswahlbegründung

Ein entscheidender Aspekt bei der Auswahl war die hohe System- und Plattformunabhängigkeit der entwickelten Webanwendung. Da die Anwendung webbasiert auf unterschiedlichsten Endgeräten (z. B. Desktops, Tablets, Smartphones) sowie unter verschiedenen Betriebssystemen (z. B. Linux, Windows, macOS, iOS, Android etc.) und mit unterschiedlichen Screenreadern und Hilfsmitteln genutzt werden kann, musste für die Barrierefreiheitsprüfung ein Analysewerkzeug gewählt werden, das eine möglichst geräte- und systemspezifisch neutrale Basisprüfung ermöglichen.

WAVE erlaubt es, bereits auf Quellcode- und Struktur-Ebene viele potenzielle Barrieren frühzeitig zu identifizieren, die unabhängig von konkreten Endgeräten problematisch wären. Diese automatisierten Tests liefern damit eine tragfähige Grundlage für die Erkennung allgemeiner Barrierefreiheitsprobleme, auch wenn ergänzende manuelle Tests (z. B. mit verschiedenen realen Screenreadern und Eingabemethoden) perspektivisch weiterhin sinnvoll sind.

Mit dem Einsatz dieses Werkzeuges wurde im Rahmen dieser Arbeit eine systematische Erstanalyse der Barrierefreiheit der entwickelten Webanwendung durchgeführt. Die identifizierten Optimierungspotentiale flossen fortlaufend in die Entwicklung und Anpassung der Anwendung ein.

### 5.5.3 Ergebnisse der Barrierefreiheitsprüfung

Die folgende Tabelle dokumentiert die Prüfung mit dem Tool WAVE. Dabei wurde festgehalten, ob die getesteten Seiten fehlerfrei waren. Falls sogenannte *Alarme* auftraten, wurde jeweils begründet, warum diese im konkreten Fall vernachlässigt werden konnten.

| **Datei / Testbereich** | **WAVE** | **Bemerkung** |
|---|---|---|
| Startseite (main.html) | ✓ | - |
| Szenario 1 (Andreas Zuhause) | ✓ | Es wird angemerkt, dass eine Headerstruktur und Webseitenbereiche fehlen. Dies kann vernachlässigt werden, da es ausschließlich einen H5P Inhalt gibt, in dem navigiert wird. |
| Szenario 2 (Ginseng Cloud) | ✓ | Es wird angemerkt, dass eine Headerstruktur und Webseitenbereiche fehlen. Dies kann vernachlässigt werden, da es ausschließlich einen H5P Inhalt gibt, in dem navigiert wird. |

Tabelle 1: Testprotokoll Barrierefreiheit

# 6 Integration der Übung in das Modul *Digitale Selbstverteidigung*

Die entwickelte Webanwendung zur sensorisch-parallelisierten Erläuterung von Passwortsicherheit ist als ergänzendes Element zur Vertiefung des Themenblocks Passwortsicherheit im Modul *Digitale Selbstverteidigung* konzipiert. Sie erweitert das bestehende Modul um eine praxisorientierte Übung, die es den Teilnehmenden ermöglicht, zentrale Prinzipien wie Passwortangriffe, Hashfunktionen und Social Engineering eigenständig und interaktiv zu erproben.

Die Anwendung wird dabei nach der grundlegenden Einführung in die Passwortsicherheit eingesetzt, sodass die Teilnehmenden bereits die wichtigsten Konzepte theoretisch kennengelernt haben. Ziel der Übung ist es, das zuvor Erlernte zu festigen, praxisnah anzuwenden und Zusammenhänge durch die interaktiven Simulationen besser zu verankern.

Didaktisch empfiehlt sich der Einsatz in Partner- oder Kleingruppenarbeit, um gemeinsames Nachdenken, gegenseitige Hilfestellung und Diskussionen zu fördern. Die Lehrperson steht während der Bearbeitung beratend zur Verfügung. Besonders die Szenarien sollten nach der Bearbeitung gemeinsam besprochen werden, da hier komplexere Überlegungen notwendig sind und die Lösungswege sorgfältig reflektiert werden sollten. Dies unterstützt das Verständnis für die Hintergründe von Social Engineering sowie die Funktionsweise und Problematik von Hashfunktionen, insbesondere im Hinblick auf mögliche Kollisionen und Fehlberechnungen.

Ein besonderer Schwerpunkt sollte auf der Bearbeitung und Nachbesprechung der Hashfunktionen liegen, da dieses Thema erfahrungsgemäß für viele Lernende sehr abstrakt bleibt. Die visuelle Darstellung innerhalb der Webanwendung bietet hierbei eine erste Annäherung, dennoch ist es didaktisch erforderlich, im Plenum nochmals die Risiken und Grenzen von Hashverfahren zu erläutern, insbesondere die Möglichkeit von Kollisionen, die zu fehlerhaften Zuordnungen führen können. Dies schärft das Bewusstsein für die Bedeutung kryptographischer Verfahren im Alltag und verdeutlicht gleichzeitig deren Anfälligkeiten.

Durch die Bearbeitung der Webanwendung vertiefen die Teilnehmenden verschiedene Kompetenzen, die im Modul Digitale Selbstverteidigung grundlegend vermittelt werden.

Die Integration der Übung verfolgt dabei mehrere didaktische Ziele:

- Das Verständnis von Angriffsmethoden auf Passwörter (Brute-Force- und Wörterbuchangriffe).
- Das Grundverständnis der Funktionsweise und Problematik von Hashfunktionen.
- Die Sensibilisierung für Angriffsszenarien im Bereich Social Engineering.
- Die Reflexion des eigenen Passwortverhaltens und der Passwortgestaltung.
- Das Erkennen von Sicherheitslücken im eigenen digitalen Handeln.

Die folgende Tabelle skizziert den empfohlenen Ablauf für den Einsatz der Webanwendung im Modul:

| **Phase** | **Lehr-/Lernarrangement** | **Methodisch-didaktische Hinweise** | **Medien** |
|---|---|---|---|
| Erarbeitung (20–25 min) | Partner- oder Kleingruppenarbeit | Interaktive Bearbeitung der Webanwendung; Lehrkraft steht beratend zur Verfügung | Webanwendung und eigene Endgeräte |
| Reflexion (10–15 min) | Plenum | Besprechung der Lösungswege in den Szenarien; Erklärung möglicher Hash-Kollisionen und Angriffsstrategien; Klärung offener Fragen | Moderation, Whiteboard, ggf. Präsentation |

Tabelle 2: Integration der Webanwendung in das Modul *Digitale Selbstverteidigung*

# 7 Erweiterungsmöglichkeiten und Ausblick

Die im Rahmen dieses Projekts entwickelte Webanwendung stellt bereits eine umfassende und sensorisch-parallelisierte Lernumgebung zur Vermittlung zentraler Aspekte der Passwortsicherheit dar. Dennoch ergeben sich aus der bisherigen Entwicklung weitere sinnvolle Erweiterungspotentiale, sowohl im digitalen als auch im haptischen Bereich. Diese sollen im Folgenden skizziert werden.

## 7.1 Erweiterung der Webanwendung

Die Webanwendung kann zukünftig durch zusätzliche Szenarien sowie weiterführende Simulationen im Bereich der Hashfunktionen ausgebaut werden. Ziel solcher Erweiterungen wäre es, noch komplexere Anwendungssituationen abzubilden und die Lernerfahrungen weiter zu vertiefen.

### 7.1.1 Erweiterung durch zusätzliche Szenarien

Die bisherigen Szenarien behandeln vor allem klassische Angriffsvektoren wie Social Engineering und einfache Hashberechnungen. Denkbar wäre eine Erweiterung um komplexere, realitätsnahe Szenarien, die weitere Angriffstechniken oder zusätzliche Sicherheitsaspekte thematisieren. Beispiele hierfür könnten sein:

- Mehrstufiges Social-Engineering-Szenario: Die Lernenden müssen Informationen aus mehreren Quellen zusammentragen (z. B. Social Media Profile, Geburtstage, Vorlieben), um ein möglichst stark personalisiertes Passwort zu rekonstruieren. Dies könnte die Problematik öffentlicher Datenpreisgabe noch stärker verdeutlichen.

- Szenario zu Mehrfaktor-Authentifizierung: Hierbei müssen die Lernenden erkennen, wie durch Kombination mehrerer Faktoren (z. B. Passwort, Einmalcode, biometrisches Merkmal) Sicherheitsrisiken reduziert werden können.

- Szenario zu Phishing-Angriffen: Die Lernenden analysieren typische Phishing-Mails oder -Webseiten und sollen mögliche Schwachstellen erkennen, um zu sensibilisieren, wie leicht Zugangsdaten durch Täuschung abgegriffen werden können.

Solche Erweiterungen würden die Anwendungsbreite des Lernangebotes deutlich vergrößern und zugleich aktuelle Gefährdungsszenarien praxisnah aufgreifen.

### 7.1.2 Erweiterung der Hashfunktionsvisualisierung

Auch die Simulation der Hashfunktionen könnte weiterentwickelt werden, um den Lernenden differenziertere Einsichten in die Eigenschaften kryptografischer Verfahren zu ermöglichen. Denkbar wäre unter anderem:

- Implementierung kollisionsanfälliger Hashfunktionen: Lernende könnten bewusst mit Beispielen arbeiten, bei denen zwei unterschiedliche Passworteingaben zum gleichen Hashwert führen. Dies würde die Problematik von Kollisionen anschaulich erlebbar machen.

- Visualisierung von Avalanche-Effekten: Bei echten Hashfunktionen führen bereits kleinste Änderungen im Eingabewert zu massiven Änderungen im Hashwert. Diese Eigenschaft ließe sich simulieren, um zu verdeutlichen, wie empfindlich Hashfunktionen auf kleine Eingabeveränderungen reagieren.

- Veranschaulichung der nicht-linearen Berechnungslogik realer Hashalgorithmen (z. B. durch Blockdiagramme): So könnten die Lernenden ein erstes Gefühl für die komplexen inneren Abläufe von Algorithmen wie SHA-256 entwickeln, ohne von der mathematischen Tiefe überfordert zu werden.

Solche Erweiterungen würden die Tiefe des technischen Verständnisses weiter fördern und insbesondere Lernende mit vertieftem Interesse an Kryptographie zusätzlich ansprechen.

## 7.2 Haptische Erweiterungsideen

Neben der digitalen Weiterentwicklung bietet auch die haptische Ebene vielversprechende Möglichkeiten, um die Thematik für Lernende mit unterschiedlichen Wahrnehmungsvoraussetzungen zugänglich zu machen. Insbesondere für sehbeeinträchtigte Personen könnten haptische Materialien eine zentrale Rolle spielen, aber auch für alle anderen Lernenden bieten taktile Elemente eine alternative Zugangsmöglichkeit, die kognitive Prozesse zusätzlich unterstützt.

Ein möglicher Ansatz wäre der Einsatz von Braille-Steinen oder taktilen Buchstabenplättchen, mit denen Lernende selbstständig Wörter und Passphrasen zusammensetzen können. Durch das physische Legen von Buchstabenketten werden die Prinzipien der Passwortbildung und -komplexität greifbar gemacht. Ergänzend könnten die Lernenden dabei unmittelbar erleben, wie sich längere, komplexere Passphrasen schwieriger rekonstruieren lassen als kurze, einfache Begriffe.

Eine haptische Visualisierung der Hashfunktion könnte ergänzend realisiert werden, indem das Prinzip der Einwegverschlüsselung modellhaft nachgebaut wird. Denkbar wäre beispielsweise ein mechanisches Schablonensystem:

- Für jeden Buchstaben existiert ein taktiles Eingabeelement (z. B. Würfel oder Plättchen mit Buchstaben/Braille).
- Diese Elemente werden in eine Schablone eingelegt, die jeweils mathematische Transformationen repräsentiert (z. B. »verschobene Positionen«, Modulo-Operationen, Multiplikationen).
- Am Ende der mechanischen Umsetzung ergibt sich ein Ergebnisfeld, das den Hashwert vereinfacht symbolisiert.

Auf diese Weise könnte das abstrakte Prinzip der Hashberechnung für sehende und nicht-sehende Lernende gleichermaßen erfahrbar gemacht werden. Die Lernenden könnten durch wiederholtes Legen und Variieren der Eingabewerte selbst erleben, dass kleine Änderungen am Eingangswert zu unterschiedlichen Hashwerten führen, ohne die mathematischen Hintergründe im Detail beherrschen zu müssen.

Solche haptischen Erweiterungen würden die sensorische Parallelisierung noch konsequenter umsetzen und die Barrierefreiheit des Angebots deutlich erhöhen. Zugleich eröffnen sie allen Lernenden neue, erfahrungsbasierte Lernwege und stärken so die Nachhaltigkeit des Kompetenzaufbaus im Bereich der digitalen Selbstverteidigung.

# 8 Fazit und Ausblick

## 8.1 Ausblick

Mit der vorliegenden Arbeit wurde ein praxisorientierter Beitrag zur Thematisierung von Passwortsicherheit im Kontext sensorischer Parallelisierung entwickelt. Die entstandene Webanwendung bietet dabei nicht nur einen niedrigschwelligen Zugang für Lehrer*innen im Modul, sondern könnte perspektivisch auch über die reine Lehrer*innenbildung hinaus Anwendung finden.

Gerade in einer zunehmend digitalisierten Bildungslandschaft, in der digitale Kompetenzen aller Lernenden gestärkt werden müssen, kommt der Thematik der digitalen Selbstverteidigung eine immer zentralere Bedeutung zu. Angesichts der fortschreitenden Digitalisierung schulischer und gesellschaftlicher Prozesse ist es unerlässlich, alle Schüler*innen frühzeitig für die Gefahren unsicheren Passwortverhaltens, für mögliche Angriffsszenarien und für Schutzmechanismen zu sensibilisieren.

Die in dieser Arbeit entwickelte Übung kann dabei nicht nur Informatiklehrkräften als didaktisches Werkzeug dienen, sondern bietet auch für fachfremde Lehrkräfte eine Möglichkeit, sich praxisnah mit grundlegenden Fragen der informatischen Sicherheit auseinanderzusetzen. Durch die anschauliche und interaktive Aufbereitung der Inhalte erhalten auch Lehrkräfte ohne tiefgreifende informatische Vorkenntnisse ein grundlegendes Verständnis für Sicherheitsrisiken und können diese Kompetenzen verstärkt in ihren Fachunterricht integrieren.

Perspektivisch wäre es wünschenswert, wenn digitale Selbstverteidigung als Querschnittsthema in verschiedenen Fächern verankert wird. Ziel sollte es sein, dass alle Schülerinnen — unabhängig von Fächerwahl, Bildungsweg oder persönlichem Hintergrund — die Chance erhalten, digitale Kompetenzen im Sinne von Bildungsgerechtigkeit umfassend zu erwerben. So kann langfristig eine tragfähige Grundlage für den verantwortungsvollen und sicheren Umgang mit digitalen Technologien in einer zunehmend vernetzten Welt geschaffen werden.

## 8.2 Persönliches Fazit

Die Bearbeitung dieser Arbeit stellte mich vor zahlreiche Herausforderungen und erforderte von Beginn an ein hohes Maß an Eigeninitiative, Durchhaltevermögen und Problemlösungsbereitschaft. Während der anfänglichen Konzeptionsphase war es zunächst schwierig, eine klare Idee zu entwickeln, die sowohl didaktisch sinnvoll als auch praktisch umsetzbar ist. Zahlreiche ursprünglich angedachte Lösungswege erwiesen sich als zu komplex, technisch aufwändig oder organisatorisch nicht realisierbar.

Im Verlauf der Projektarbeit ergaben sich immer wieder neue Hürden, insbesondere im Bereich der technischen Entwicklung, der Tests unter realistischen Bedingungen und der Berücksichtigung unterschiedlichster Vorgaben und Nutzerperspektiven. Gleichzeitig wurde mir im Projektverlauf zunehmend bewusst, wie vielfältig und komplex Barrieren im Lernprozess sein können — auch über klassische Behinderungen hinaus. Die intensive Auseinandersetzung mit Fragen der Barrierefreiheit und sensorischen Parallelisierung hat meine eigene Wahrnehmung für die individuellen Bedürfnisse von Lernenden deutlich geschärft.

Trotz aller Anstrengungen und Phasen der Frustration bin ich stolz auf das entstandene Ergebnis und sehe darin eine wertvolle Grundlage für meine zukünftige Tätigkeit als Lehrkraft. Ich möchte die in dieser Arbeit entwickelten Ansätze aktiv in meinen eigenen Unterricht einfließen lassen, um allen Schülerinnen — unabhängig von individuellen Voraussetzungen — die gleichen Bildungschancen zu eröffnen. Bildungsgerechtigkeit bedeutet für mich, dass jedes Kind, ungeachtet seiner Herkunft und der ihm durch die »Lotterie des Lebens« mitgegebenen Voraussetzungen, die Chance erhält, sich frei zu entwickeln und den eigenen Bildungs- und Lebensweg selbstbestimmt gestalten zu können.

# Literaturverzeichnis

Arbeit und Soziales, Bundesministerium für (2025). *Maßnahmen zur Barrierefreiheit von BMAS.de*. Zugriff am 09.07.2025.

Capovilla, Silke (2015). *Inklusion in der informatischen Bildung am Beispiel von Menschen mit Sehschädigung*. Berlin: Logos Verlag.

Essen, Universität Duisburg (2024). *Projektvorstellung – ComeMINT*. Zugriff am 9. Juli 2025.

Hall, Tracey E. u. a. (2012). *Universal Design for Learning in the Classroom: Practical Applications*. New York: Guilford Press.

KeePassXC (2025). *KeePassXC*. Zugriff am 09.07.2025.

Kirkpatrick, A. u. a. (2025). *Web Content Accessibility Guidelines*. Zugriff am 09.07.2025.

Kohl, Matthias (März 2023). »Informatikunterricht inklusiv gestalten: Entwicklung sensorisch parallelisierten Materials zur Kryptologie«. Unveröffentlicht. Masterarbeit. Remscheid: Bergische Universität Wuppertal, Fakultät 4 – Mathematik und Naturwissenschaften, Fachgebiet Didaktik der Informatik.

Miessler, Daniel (2025). *SecLists*. Zugriff am 01.05.2025.

Pwned, Have I Been (2025). *Have I Been Pwned*. Zugriff am 09.07.2025.

Schmitz, Denise (2024). *SPAM von der Schulleitung? Digitale Selbstverteidigung. Veranstaltungsmodul zur informatischen Bildung aller Lehrkräfte*. Hrsg. von der CoP Informatische Grundbildung/Digitalisierung als Lerngegenstand im Projekt COMeIN.

Vereinte Nationen (2006). *Übereinkommen über die Rechte von Menschen mit Behinderungen (UN-Behindertenrechtskonvention)*. Zugriff am 01.05.2025.

Wuppertal, DDI – Bergische Universität (2024). *ComeMINT – fortbilden durch vernetzen – vernetzen duch fortbilden*. Zugriff am 9. Juli 2025.

# Eigenständigkeitserklärung

Ich versichere, dass ich die Arbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt sowie Zitate kenntlich gemacht habe und die Regelungen des entsprechenden Paragraphen der geltenden Prüfungsordnung zu Versäumnis, Rücktritt, Täuschung und Ordnungsverstoß, insbesondere die Möglichkeit des endgültigen Verlustes des Prüfungsanspruches und des endgültigen Nichtbestehens im Fall einer schwerwiegenden oder wiederholten Täuschung zur Kenntnis genommen habe.

| | |
|---|---|
| Datum, Ort | Unterschrift |