

Umsetzungsbeispiel Passwortmanager

Beschreibung des Artefakts

Passwortmanager sind digitale Anwendungen, die Nutzende bei der Verwaltung von Nutzernamen, Passwörtern und anderen sensiblen Anmeldedaten unterstützen. Diese Zugangsdaten werden vom Passwortmanager verschlüsselt gespeichert und sind für die Nutzenden nur über ein Masterschlüssel zugänglich.

Konkret unterstützen Passwortmanager die Nutzenden dabei, für unterschiedliche Online-Dienste verschiedene Zugangsdaten zu verwenden, ohne dass sie sich diese alle selbst merken müssen.

Die verschiedenen Passwortmanager unterscheiden sich zum einen darin, ob sie als eigenständiges Programm oder als Browser-Add-on bereitgestellt werden. Zum anderen unterscheiden sie sich hinsichtlich der verwendeten Verschlüsselungsalgorithmen sowie zusätzlicher Funktionen. Dazu gehören beispielsweise die Synchronisation der Passwortdatenbank zwischen Endgeräten, die Generierung starker Passwörter oder die automatische Eingabe von Zugangsdaten. ^a

^aDer Abschnitt wurde mit [Prompt1] erstellt.

Beschreibung des Szenarios

Die entworfene Unterrichtsstunde verfolgt das Ziel, die Lernenden für die Nutzung sicherer Passwörter zu sensibilisieren und ihnen unterstützende Tools näherzubringen.

Zu Beginn der Unterrichtseinheit beschreiben die Lernenden ihr Nutzungsverhalten im Umgang mit Passwörtern. Dabei gehen sie darauf ein, ob sie sichere Passwörter verwenden und ob sie Passwörter mehrfach nutzen.

Anschließend erarbeiten die Lernenden in Partnerarbeit Merkmale eines sicheren Passworts und begründen, weshalb die Verwendung von Zahlen, Sonderzeichen sowie Groß- und Kleinbuchstaben wichtig ist.

Im Anschluss lernen sie das Artefakt Passwortmanager als Hilfsmittel zur Verwaltung von Passwörtern und Nutzernamen kennen. Dabei werden die Funktionsweise eines Passwortmanagers, seine Bedeutung für die Nutzenden sowie die praktische Anwendung thematisiert.

Zum Abschluss der Stunde formulieren die Lernenden persönliche Ziele im Hinblick auf ihr zukünftiges Nutzungsverhalten von Passwörtern und ordnen Chancen und Risiken der Nutzung von Passwortmanagern ein. ^b

^bDer Abschnitt wurde mit [Prompt2] erstellt.

Basisangaben

Fach	Informatik	Klassenstufe	9
Schulform	Gymnasium	Lernbereich	3: Netzwerk
Zeitbedarf	1 DS	Kompetenzrahmen	4.1.1; 4.1.2; 4.2.1; 5.5.2; 6.2.3

Artefaktsteckbrief „Passwortmanager“

Wofür wird es genutzt?

Ein Passwortmanager wird zur sicheren Verwaltung von Zugangsdaten verwendet (Benutzernamen, Passwörter, etc.). Dabei unterstützt er den Nutzenden im Speichern, Organisieren, und Bereitstellen dieser. Ein Passwortmanager speichert die Zugangsdaten dabei in verschlüsselter Form, sodass diese nur mithilfe eines Masterschlüssels eingesehen werden können. Passwortmanager enthalten in der Regel folgende Funktionen:

- das Speichern von Passwörtern und Benutzernamen
- das Verschlüsseln der Zugangsdaten
- das Generieren von sicheren Passwörtern
- das automatische Ausfüllen der Zugangsdaten
- die Synchronisation der Zugangsdaten zwischen Geräten
- das Speichern zusätzlicher sensibler Daten

Dadurch entsteht allerdings ein Single-Point-of-Failure. Sollte der Masterschlüssel verloren gehen, ist der Zugriff auf die Zugangsdaten nicht mehr möglich.

Wie funktioniert es?

Die meisten Passwortmanager bieten folgende Funktionen:

1. Erstellen des Masterschlüssels:
Zum Verschlüsseln der Zugangsdaten wird ein Masterschlüssel eingegeben. Auf Basis dieses Masterschlüssels wird die Zugangsdatendatenbank verschlüsselt. Das Masterpasswort wird dabei nicht als Klartext gespeichert, sondern dient zur Entschlüsselung der Zugangsdatendatenbank.
2. Speichern und Verschlüsseln der Zugangsdaten:
Für verschiedene Dienste werden die Zugangsdaten unter Nutzung des Masterschlüssels verschlüsselt gespeichert.
3. Generieren sicherer Passwörter:
Einige Passwortmanager bieten zusätzlich die Funktion, sichere Passwörter zu erstellen. Diese Passwörter haben den Vorteil, dass sie zufällig erstellt wurden und nicht durch die Präferenzen von Menschen beeinflusst sind.
4. Automatisches Anmelden:
Einige Passwortmanager bieten die Funktion, dass die Zugangsdaten beim Öffnen des jeweiligen Dienstes automatisch ausgefüllt werden, sodass die Nutzenden diese nicht abschreiben bzw. kopieren müssen.
5. Synchronisieren der Anmeldedaten:
Nutzt man den gleichen Passwortmanager auf verschiedenen Geräten, bieten einige die Funktion an, die verschlüsselte Zugangsdatendatenbank zwischen den verschiedenen Geräten zu synchronisieren, sodass die Passwörter auf allen Geräten mit dem Masterschlüssel zugänglich sind.

Umsetzung im Unterricht

Technisch- infrastrukturelle Voraussetzungen

Voraussetzung für Lehrende:

- Computer
- Interaktive Tafel oder Beamer und Whiteboard
- Passwortmanager

Voraussetzung für Lernende:

- Computer
- Internet
- Passwortmanager

empfohlene Software: KeePassXC (Open Source)

Anmerkung: Zur Auswahl des Passwortmanagers KeePassXC wurde auf verlinkten Bericht des BSI zurückgegriffen.

Curriculare Analyse

Fachlehrplan

Die geplante Unterrichtseinheit ist für den Lernbereich 3: „Netzwerke “ in der Klassenstufe 9 konzipiert und soll zum Ende des Lernbereichs stattfinden.

Sie befasst sich mit dem Lernziel „Sich positionieren zur Informationssicherheit in vernetzten Systemen“. Dabei werden die Vorschläge der rechten Seite des Lehrplans beachtet. Besonders wird dabei auf „Passwortschutz“ und „Verschlüsselung“ eingegangen.

Lernbereich 3: Netzwerke		8 Ustd.
Kennen von Grundlagen der Übertragung in Netzwerken	PAN, LAN, WAN	
- Netzwerkkomponenten	Router, Switch, Accesspoint, Modem	
- Übertragungsmedien	Kabel, Funk	
- Peer-To-Peer- und Client-Server-Prinzip		
- Konzept der Zerlegung in Datenpakete		
- Netzwerkprotokolle und -dienste	TCP/IP, SMTP, IMAP, HTTPS	
	→ Kl. 7, LB 2	
- Adressierung	DNS, Routing	
Kennen des Prinzips von symmetrischer und asymmetrischer Verschlüsselung	Schlüsseltausch-Problematik	
	Schlüsselpaare	

Sich positionieren zur Informationssicherheit in vernetzten Systemen	
- Datensicherheit und Datenschutz	Passwortschutz, Zwei-Faktor-Authentifizierung, Verschlüsselung, Zugriffsrechte → Kl. 8, LB 2
- Chancen und Risiken für die Gesellschaft	Beeinflussung von Meinungen und Einstellungen, Datenmanipulation, Nachhaltigkeit von Daten ⇒ Werteorientierung ⇒ Bildung für nachhaltige Entwicklung ⇒ Medienbildung → G/R/W, Kl. 8, LB 2

Abbildung 1: Lehrplan Informatik Gymnasium Klasse 9 LB1 Netzwerke

Der Operator „sich positionieren“ gehört dabei zur Taxonomiestufe 5: Bewerten. Der Lehrplan fordert von diesem Operator explizit, dass die Lernenden begründete Sach- und/oder Werturteile entwickeln und diese kritisch reflektieren und eventuell revidieren. Dabei wird von den Unterpunkten „Datensicherheit und Datenschutz“ und „Chancen und Risiken für die Gesellschaft“ die Punkte Datenschutz sowie Risiken für die Gesellschaft näher betrachtet.

Zur Durchführung dieser Unterrichtseinheit wird folgendes Vorwissen vorausgesetzt:

- kennen des Algorithmusbegriffs als „Handlungsvorschrift“ für den Computer
- kennen von Kriterien für sichere Passwörter
- kennen von Maßnahmen zum Datenschutz in vernetzten Systemen
- ggf. kennen von Verschlüsselungsverfahren

Nach der beschriebene Unterrichtseinheit wäre eine Anschlussmöglichkeit mit dem Aspekt der Datensicherheit fortzufahren. Es würde sich anbieten den Passwortmanager als eine Methode zur Verbesserung des Datenschutzes durch stärkere Passwörter und die Eliminierung von „Passwortzettelchen“ vorzustellen. Im Anschluss könnte man mit den Lernenden Methoden zur Verbesserung der Datensicherheit, beispielsweise RAID oder Back-Ups behandeln.

digitalisierungsbezogene Lernziele

#	MIA	K#	Qualifikationsebene	Handlungsebene
D1	M	4.1.1	Die Lernenden kennen Risiken und Gefahren in digitalen Umgebungen kennen, reflektieren und berücksichtigen	,indem sie Risiken identifizieren und nennen, die bei der Nutzung unsicherer oder mehrfach verwendeter Passwörter entstehen.
D2	A	4.1.2	Die Lernenden entwickeln Strategien zum Schutz entwickeln und anwenden und wenden diese an	Anforderungen für sichere Passwörter nennen und umsetzen.
D3	A	4.2.1	Die Lernenden nutzen Maßnahmen für Datensicherheit und gegen Datenmissbrauch berücksichtigen	sichere Passwörter erstellen und diese in einem Passwortmanager verwalten.
D4	I	5.5.2	Die Lernenden erkennen Algorithmische Strukturen in genutzten digitalen Tools erkennen und formulieren	die Verschlüsselung mittels Masterschlüssel vereinfacht erläutern.
D5	M	6.2.3	Die Lernenden analysieren und beurteilen Vorteile und Risiken von Geschäftsaktivitäten und Services im Internet analysieren und beurteilen	verschiedene Möglichkeiten der Passwortverwaltung vergleichen und deren Sicherheitsrisiken bewerten.

Unterrichtsverlaufsplanung

Legende Unterrichtsmedium Unterrichtswerkzeug Unterrichtsgegenstand

Zeit	Phase	Inhalt	SF/M	Medien/Material	LZ Nr.
5'	Motivation und Einführung	• Einstieg mit Alltagsfrage: „Wie viele Passwörter habt ihr so?“ • Weiterführende Frage: „Wer von euch benutzt seine Passwörter mehrfach?“ • ggf. Anschlussfrage: „Wieso nutzt ihr sie mehrfach?“ • (Fragen an der Interaktiven Tafel anzeigen)	FU (wenn möglich UG)	• Interaktive Tafel oder Beamer	-
3'	Problematisierung	• Frage: „Was sind sichere Passwörter? Wieso sollten wir Passwörter nur einmal nutzen?“	FU	-	-
15'	Erarbeitung	• Aufgabenstellung: Recherchiert drei Anforderungen an Passwörter und zwei Risiken wenn Passwörter doppelt genutzt werden. Notiert eure Erkenntnisse. • Die Lernenden recherchieren Anforderungen an sichere Passwörter: • Länge • vers. Zeichen • Sonderzeichen • „randomness“ • Die Lernenden recherchieren Risiken, wenn Passwörter mehrfach genutzt werden.	EA / PA	• Computer mit Webbrowser	D1
8'	Sicherung	• Vergleich der Ergebnisse im Plenum • Sicherung im digitalen Tafelbild	UG	• Interaktive Tafel oder Whiteboard	D1

12'	Erarbeitung	• Präsentation eines Beispiels für einen Passwortmanager (KeePassXC) • Anlegen eines Masterschlüssels • Verwalten von Zugangsdaten • Generieren von sicheren Passwörtern	FU	• KeePassXC • Beamer	D4
10'	Anwendung	• Lernende erstellen sich ein Masterschlüssel • Lernende legen (MockUp) Zugangsdaten an • testen die Passwortgenerierung aus • Lernende verwalten verschiedene (MockUp) Zugangsdaten	PA	• KeePassXC	D2, D3
5'	Auswertung	• Sind die generierten Passwörter sicherer? • Ist der Passwortmanager Anwenderfreundlich?	UG	-	-
7'	Erarbeitung	• Wie verläuft die Verschlüsselung im Passwortmanager (vereinfacht) • Erstellen des Masterschlüssel • Anhand des Masterschlüssel wird Verschlüsselungs-„Schlüssel“ erstellt • Entschlüsselung nur mit Masterschlüssel möglich • Zugangsdatendatenbank wird verschlüsselt gespeichert	FU	• KeePassXC	D4
5'	Sicherung	• Die Lernenden übernehmen sich das Tafelbild zur Verschlüsselung im Passwortmanager	EA	• Interaktive Tafel oder Beamer	-

10'	Übung	- Die Lernenden finden sich in Paaren zusammen - Die Lernenden erläutern sich gegenseitig an einem Beispiel die Verschlüsselung im Passwortmanager (mit Tafelbild als Unterstützung)	UG	-	D4
10'	Reflexion	- jeder schriftlich! - Die Lernenden nennen Vorteile und Gefahren bei der Nutzung von Passwortmanagern. - Die Lernenden wägen Aufwand und Nutzen der Nutzung eines Passwortmanagers ab - Die Lernenden formulieren Vorsätze für ihre zukünftige Nutzung von Passwörtern	EA	-	D2, D5

SF - Sozialform (EA: Einzelarbeit; PA: Partnerarbeit; GU - Gruppenarbeit; FU: Frontalunterricht)

Prompts und Links

Die im Folgenden aufgelisteten Prompts wurde mit ChatGPT 5.3 Instant genutzt.

Prompts:

[Prompt1]:

Verbesser Lesefluss, Rechtschreibung und Grammatik:

Passwortmanager sind digitale Anwendungen die Nutzenden in der Verwaltung von Nutzernamen, Passwörtern und anderen sensiblen Anmeldedaten unterstützt. Diese Zugangsdaten werden durch den Passwortmanager verschlüsselt abgespeichert und sind von den Nutzenden nur durch ein Masterschlüssel einsehbar. Konkret unterstützen Passwortmanager die Nutzenden darin, für unterschiedliche Online-Dienste verschiedene Zugangsdaten zu verwenden, ohne dass sich die Nutzenden all diese selbst merken müssen. Dabei unterscheiden sich die verschiedenen Passwortmanager zum einen darin, ob sie ein eigenständiges Programm sind oder ein Browser-Add-on. Zum anderen unterscheiden sich die Passwortmanager in den genutzten Verschlüsselungsalgorithmen, sowie den zusätzlichen Features wie der Synchronisation der „Passwortdatenbank“ zwischen Endgeräten, der Generierung starker Passwörter oder einer automatischen Eingabe der Zugangsdaten.

[Prompt2]:

Verbessere Lesefluss, Ausdruck, Rechtschreibung und Grammatik:

Die entworfene Unterrichtsstunde verfolgt das Ziel, die Lernenden für die Nutzung sicherer Passwörter zu sensibilisieren und ihnen Tools die sie dabei unterstützen näher zu bringen. Zu Beginn der Unterrichtseinheit beschreiben die Lernenden ihre Nutzungsverhalten von Passwörtern. Dabei gehen sie darauf ein, ob sie sichere Passwörter benutzen und ob sie Passwörter doppelt benutzen. Die Lernenden erarbeiten in Partnerarbeit Merkmale eines sicheren Passwortes und begründen, weshalb die Nutzung von Zahlen, Sonderzeichen sowie Groß- und Kleinbuchstaben wichtig ist. Im Anschluss lernen sie das Artefakt Passwortmanager als Verwaltungshilfe für Passwörter und Nutzernamen kennen. Dabei wird die Funktionsweise eines Passwortmanagers, die Rolle für die Nutzenden und die eigentliche Nutzung des Passwortmanagers besprochen. Zum Abschluss der Stunde formulieren die Lernenden persönliche Ziele im Hinblick auf ihr Nutzungsverhalten von Passwörtern und ordnen Chancen und Risiken durch die Nutzung von Passwortmanagern ein.

Links:

- **Bericht des BSI:** <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DVS-Berichte/passwortmanager.pdf>
- **Lehrplan Informatik Gymnasium:** <https://www.schulportal.sachsen.de/lplandb/index.php?lplanid=630&lplansc=fTqTlkXseYZLUMB5l3pV&token=5b324ab4e0afbfb851d478ecc14bdf97>