

Abteilung Gymnasium

Arbeitskreis Link-Ebene Wirtschaftsinformatik

Schellingstr. 155 · 80797 München · Tel.: 089 2170-2153 · Fax: -2125

E-Mail: tobias.tyll@isb.bayern.de

**WIn 10.3: Sicherheit von Passwörtern (Unterrichtssequenz)**

In diesem Material werden ausführliche Hinweise zu möglichen Unterrichtsabschnitten bei der Behandlung dieses Themas gegeben. Die gesamte Unterrichtssequenz gliedert sich dabei in folgende Teile:

* Einstieg (typische, leicht zu erratende Passwörter)
* praktische Untersuchungen (Programm „Passwortknacker“ und Bezug zur Mathematik) → Finden geeigneter Strategien für ein sicheres Passwort
* Bewertung der gefundenen Strategien
* Lernzielkontrolle / Übung
* ergänzende Sicherheitsmaßnahmen, die zum sicheren Passwort hinzukommen müssen
* Hilfe beim Finden und Merken eines sicheren Passworts

Hinweis:

Der Umfang dieser Unterrichtssequenz übersteigt die im Lehrplan vorgesehene Stundenzahl, im Blick auf die Förderung der Informations- und Datenkompetenz im Rahmen der ökonomischen Verbraucherbildung erscheint diese Ausweitung gleichwohl gerechtfertigt.

Die Materialien eignen sich alternativ auch als Grundlage für ein Projekt (10.5).

1. **Einstieg**

Als **Einstieg** bietet es sich an, an die Sicherungsmaßnahmen zum Schutz gegen Schadprogramme zu erinnern und darauf zu verweisen, dass es aber die weitere Gefahr gibt, dass Hacker ein Passwort „knacken“ → Gemeinsam überlegen, warum dies den Hackern oftmals sehr leicht fällt:

* Viele verwenden **zu einfache Passwörter** wie „Hase“, „Paul“ oder ähnliches (ggf. Recherche im Internet zum Thema „Was sind die beliebtesten Passwörter im Internet?“)
* Es gibt im Internet mittlerweile zahlreiche „**Wörterbücher**“ mit 100.000 (beliebten, einfachen Passwörtern (Stichwörter „password“, „dictionary“, „attack“); da ein moderner Computer bis zu rund **109 = 1 Milliarde Angriffe in der Sekunde** schafft (Stand: Sommer 2011), dauert es „nicht lange“, bis das Passwort geknackt ist…
* Vermeidet man Wörter aus dem Wörterbuch oder andere typische, leicht zu erratende Passwörter wie z. B. „1234“, so bleibt Angreifern nichts anderes übrig, als systematisch alle Möglichkeiten durchzuprobieren.
1. **Praktische Untersuchungen zur benötigten Zeit zum Passwortknacken**
2. **Das Programm „Passwortknacker“ (Autor: Klaus Reinold)**
* Hinweise zur Bedienung des Programms:
	+ Vorab muss eine aktuelle **Java Runtime Environment (ab Version 7)** installiert werden.
	+ Doppelklick auf „**Passwortknacker.jar**“ startet das Programm.
	+ Das zu testende Passwort sollte zunächst kurz sein (also maximal 4 Zeichen, nur Kleinbuchstaben; unter „maximale Passwortlänge“ die entsprechende Anzahl an Buchstaben eingeben), um zu demonstrieren, wie schnell das Passwort gefunden wird. Die benötigte Zeit wird in Nanosekunden angegeben (1 Mrd. ns = 1 s).
	+ Nun kann man die Länge vorsichtig um jeweils einen weiteren Buchstaben steigern und die Zunahme der Suchzeit erkennen (5 Buchstaben: weniger als eine halbe Sekunde; 6 Zeichen: rund 10 Sekunden; 7 Zeichen: rund 4 Minuten usw.).
	+ Alternativ kann man auch schon einmal ein Sonderzeichen oder eine Zahl hinzufügen und die daraus resultierende Zeitzunahme beobachten (Achtung: Hierzu muss man aber unter „Alphabet“ einstellen, welche Zeichen jetzt möglich sind!).
	+ Abbrechen kann man das Programm nur mit Hilfe des Taskmanagers!
* Um zu zeigen, wie das Programm „Passwortknacker.jar“ intern arbeitet, kann man das Programm „**Passwortknacker2.jar**“ öffnen → Auch hierzu ein paar Hinweise:
	+ Rechts unten werden die gerade getesteten Zeichenketten angezeigt (z. B. bei einem 3-stelligen Passwort, das nur aus Kleinbuchstaben besteht: „aaa“ bis „zzz“)
	+ Bei der Anzeigeverzögerung kann man die Zeit (in ms) einstellen, die zwischen den einzelnen getesteten und angezeigten Möglichkeiten vergeht (Tipp: Wert zwischen 1 und 10 wählen, kurzes Passwort, das eher am Anfang des Alphabets kommt, wie z. B. „aber“ wählen, da es sonst zu lange dauert)
1. **Selbständige Berechnungen der Schüler**

Als fächerübergreifender Unterricht (Bezug zur Mathematik) bietet es sich nun an, näher zu untersuchen

* 1. warum ein sechsstelliges Passwort aus Kleinbuchstaben so schnell geknackt werden kann bzw.
	2. wie man die Suchzeit, die ein Angreifer benötigen würde, drastisch verlängern und somit ein sicheres Passwort finden kann.

zu a) Verwendet man für ein 6-stelliges Passwort zum Beispiel die 26 Kleinbuchstaben, so gibt es insgesamt **266** = 308.915.776 verschiedene Möglichkeiten

→ Wie lange benötigt ein moderner Computer dafür, wenn er rund 1 Milliarde Möglichkeiten pro Sekunde (Stand: 2011 / 2012) testen kann?

(308.915.776 : 1.000.000.000) s ≈ 0,3 s (und das auch nur, falls er „Pech“ hat und alle Möglichkeiten durchprobieren muss)!

zu b) Zur Umsetzung im Unterricht gibt es u. a. folgende Möglichkeiten:

* Im Unterrichtsgespräch die verschiedenen Ideen „längeres Passwort“ und „mit Groß- und Kleinbuchstaben bzw. „zusätzlich Zahlen und Sonderzeichen“ (s. u.) erarbeiten und dann in drei Gruppen die unten stehenden Möglichkeiten hinsichtlich der maximalen Dauer, das Passwort zu knacken, berechnen, in eine Tabelle (s. u.) eintragen und bewerten(!) lassen
* Mehrere Gruppen überlegen jeweils für sich Strategien und präsentieren diese dann (mit den Ergebnissen zur Dauer …).
* Die drei unten stehenden Ideen im Gespräch erarbeiten und die Zeiten (ggf. nachdem man die Schüler hat schätzen lassen) in einer Tabelle (z. B. auf Folie) vorgeben → nur noch bewerten lassen

Alternative bei jedem der drei zu b) genannten Vorschläge: Statt einer Tabelle sollen die Schüler ein ihnen sinnvoll erscheinendes Diagramm mit Hilfe einer entsprechenden Software erstellen!

**Erwartungshorizont:**

1. Länge des Passworts erhöhen:
* 8 Stellen: (268 : 109) s ≈ 209 s ≈ 3,5 min
* 11 Stellen: (2611 : 109) s ≈ 42,5 d (= Tage) [Die Umrechnung „krummer“ und v. a. großer Sekundenzahlen bereitet oftmals Schwierigkeiten, ist aber eine oft gebrauchte „Kompetenz“, weshalb man diese auch in unserem Fach aufgreifen sollte]

→ Achtung: Im Durchschnitt wird der Angriff schon jeweils bei der **halben Zeit** erfolgreich sein, mit „Glück“ aber auch schon deutlich früher

1. Verwendung von Klein- und Großbuchstaben
* 8 Stellen: (528 : 109) s ≈ 15 h
* 11 Stellen: (5211 : 109) s ≈ 238 Jahre [Hinweis: ein Jahr wurde hier mit 365,25 Tagen angenommen]
1. zusätzlich noch Ziffern und Sonderzeichen

Pro Stelle gibt es nun **94** (= 2 ⋅ 26 + 10 + 32) Möglichkeiten.

* 8 Stellen: (948 : 109) s ≈ 70,5 d
* 11 Stellen (9411 : 109) s ≈ 160 436 Jahre

**mögliche Lösung in Tabellenform:**

|  |  |  |  |
| --- | --- | --- | --- |
| maximale Dauer eines Angriffs | **26 Zeichen** | **52 Zeichen** | **94 Zeichen** |
| **8 Stellen** | 3,5 min | 15 h | 70,5 d |
| **11 Stellen** | 42,5 d | 238 Jahre | 160 436 Jahre |

1. **Bewertung der Strategien**

Hieran schließt sich nun die Bewertung der Strategien an; Ziel sollte es sein, dass die Schüler erkennen, dass ein sicheres Passwort möglichst lang sein und sowohl Klein- und Großbuchstaben als auch Zahlen und Sonderzeichen enthalten sollte!

⇒ Mind. 8 Stellen werden aktuell (fast) überall gefordert, ebenso die Verwendung von Ziffern bzw. Sonderzeichen; in der Zukunft werden aber wohl 8 Stellen nicht mehr ausreichen!!

Als Ergänzung könnte man auf das Mooresche Gesetz eingehen, v. a. wenn die Frage auftaucht, ob nicht durch immer schnellere Computer bald auch bisher noch sicher erscheinende Passwörter als unsicher eingestuft werden müssten:

Annahme: Das **Mooresche Gesetz**, das von einer Verdopplung der Rechenleistung alle zwei Jahre ausgeht, würde auch weiterhin gelten:

Wie lange würde man für ein 8- bzw. 11-stelliges Passwort (mit Klein- und Großbuchstaben, Ziffern und Sonderzeichen) in 30 Jahren (maximal) brauchen?

* Verbesserung um den Faktor 215 (da 15 „Verdopplungen“!)
* Anzahl der Kombinationen, die pro Sekunde getestet werden können: 109 ⋅ 215
* maximale Dauer bei 8 Stellen: (948 : (109 ⋅ 215)) s ≈ 3 min (also im Durchschnitt nur 1,5 min!!)
* bei 11 Stellen: (9411 : (109 ⋅ 215)) s ≈ 4,9 Jahre
1. **Lernzielkontrolle**

Beurteilung der Passwortsicherheit von Gutscheinen, z. B.: AWRAEGKWBARTSDEV (Gutscheincode eines tatsächlich erhaltenen Gutscheins von buch.de im Jahr 2011)

* gut: Länge (16 Zeichen)
* schlecht: nur Großbuchstaben (26 Zeichen!)
* ggf.: (2616:109)s ≈ 1,4 Mio. Jahre
1. **Ergänzende Sicherheitsmaßnahmen**

Nicht fehlen sollte der Hinweis an die Schüler, dass ein sicheres Passwort alleine noch nicht genügt. Hierzu dienen folgende Überlegungen (die gleichzeitig den Bogen zu den allgemeinen Sicherheitsmaßnahmen, die im Umgang mit dem Internet nötig sind, spannen, und das Bewusstsein schärfen, dass es nicht reicht, „einiges“ für die Sicherheit seiner Daten zu tun):

1. Es reicht eine Sicherheitslücke bei nur einem Unternehmen, mit dem man in Kontakt steht, wodurch das Passwort einmal – zusammen mit weiteren persönlichen Daten – in falsche Hände gerät (vgl. Datenklau bei bekannten Großkonzernen / Banken → also ohne Eigenverschulden des Nutzers!). Abhilfe schafft nur, das Passwort von Zeit zu Zeit zu ändern und verschiedene Passwörter zu verwenden (Hilfe bieten spezielle Programme („Passwortsitter“), für die man sich nur ein „Masterpasswort“ merken muss → Nachteil: Wird dieses eine Passwort geknackt, kann der Angreifer auch auf alle anderen Passwörter zugreifen)
2. Webseitenbetreiber sehen es als notwendig an, weitere Sicherungsmaßnahmen zu ergreifen, z. B.:
	* Sperrung nach n Fehlversuchen (z. B. Handy-PIN)
	* Zwangspause nach n Fehlversuchen
3. Industriespionage, ermöglicht durch unvorsichtige Mitarbeiter:

*Die Firma Contitool hat aufgrund der Hinweise ihres Sicherheitsexperten alle Mitarbeiter aufgefordert, sich ein entsprechend sicheres Passwort zu überlegen. So hat sich auch Robert Durchschnitt ein „unknackbares“ Passwort, nämlich „Ibhd5HidHN4“ ausgedacht. Doch wie soll er sich dieses merken? Nachdem er schon die ein oder andere Fehleingabe in den letzten Wochen gemacht hat, ist er ziemlich genervt und überlegt, wie er dieses Problem abstellen könnte. Seine Lösungsidee, die im Übrigen auch weitere Mitarbeiter hatten, gefällt dem Sicherheitsexperten aber gar nicht…*

**→ Hierzu sollte man die Schüler selbst überlegen lassen, welche Fehler Mitarbeiter im Unternehmen häufig machen:**

* Post-it-Zettel am Bildschirm
* Ausdruck in der Schreibtischschublade, unter der Tastatur
* im Firmenhandy gespeichert
* …
1. **Finden und Merken eines sicheren Passworts**

So motiviert, wie man sich sein Passwort nicht merken sollte, bildet der Abschluss des Themas die Frage, wie man nun ein sicheres Passwort findet und auch „sicher“ merken kann.

**Aufgabe:**

Entwickeln Sie in der Gruppe eine Strategie, mit der man sich ein sicheres Passwort merken kann. Wenden Sie Ihre Strategie an und überprüfen Sie Ihr gefundenes Passwort unter [www.datenschutz.ch](http://www.datenschutz.ch) → „Passwortcheck“[[1]](#footnote-1) auf seine Sicherheit.

Folgende Kriterien müssen erfüllt sein:

* Das Resultat der Überprüfung lautet „stark“.
* Jedes Gruppenmitglied kann am Ende der Arbeitszeit das Passwort auswendig wiedergeben.

**Mögliche Strategie:**

Man denkt sich einen Satz aus und benutzt von jedem Wort nur den 1. Buchstaben. Anschließend verwandelt man bestimmte Buchstaben in Zahlen oder Sonderzeichen:
„Ich mag meine eine kleine Schwester und den Schnee!“ wird zu „Imm1kS&d\*!“.

1. https://passwortcheck.datenschutz.ch/check.php?lang=de [↑](#footnote-ref-1)