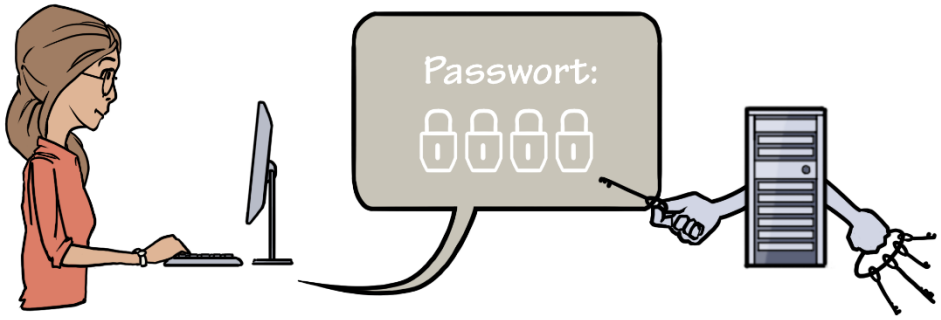
AKADEMIE FÜR LEHRERFORTBILDUNG UND PERSONALFÜHRUNG DILLINGEN

Nur für mich!

Sicherheit durch Passwörter



SCHULNETZ

Handreichung für Lehrkräfte

INHALT

IMPRESSUM

Herausgeber: Akademie für Lehrerfortbildung und Personalführung
Kardinal-von-Waldburg-Str. 6-7
89407 Dillingen

Autoren: Georg Schlagbauer, Akademie Dillingen
Markus Bader, Staatliche Berufsschule III, Fürth
Thomas Pickel, Maximilian-Kolbe-Schule Neumarkt
Wolf Gebele, Staatliche Realschule Gemünden am Main
Susanne Schaffer, Carl-von-Linde Schule, Kulmbach
Wolfgang Plank, Goethe-Gymnasium Regensburg
Christian Maushart, Bürgernetz Dillingen e. V.
Markus Rawitzer, Akademie Dillingen
Kurt Windberger, Akademie Dillingen
Peter Botzenhart, Akademie Dillingen
Markus Hahn, Regierung von Oberbayern

Grafiken: David Kremer, Augsburg

URL: http://schulnetz.alp.dillingen.de/materialien
Mail: schlagbauer@alp.dillingen.de
Stand: Dezember 2020

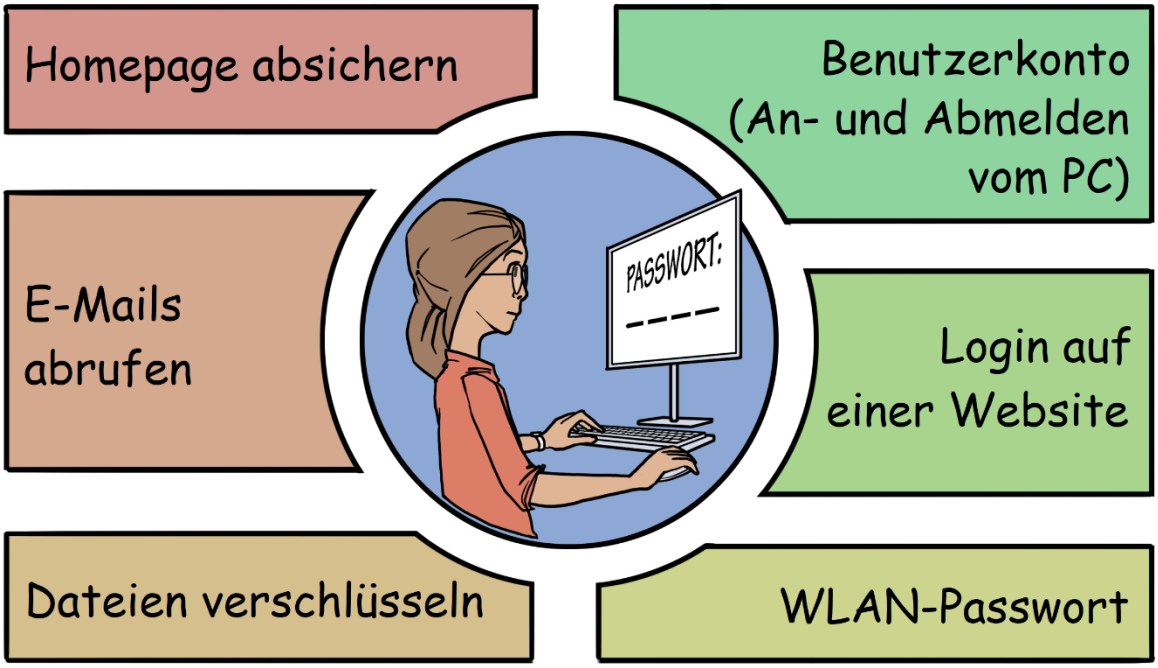
VORÜBERLEGUNGEN

Passwörter werden von vielen Anwendern als lästiges Übel betrachtet. Nur selten macht man sich Gedanken darüber, weshalb man zur Eingabe eines Passwortes aufgefordert wird oder welches Sicherheitslevel der damit abgesicherte Bereich bedarf.

Undifferenzierte Aussagen von „Fachleuten“ wie „Ein Passwort muss mindestens 12 Zeichen haben“ oder „Es kann sowieso alles geknackt werden“ helfen nicht weiter und verunsichern die Anwender nur. Viel wichtiger wäre es, zu erkennen, an welcher Stelle man wirklich ein gutes Passwort braucht, wie man damit umgeht und wo man sich das Leben etwas leichter machen kann.

Solche im Zusammenhang mit Passwörtern auftretende grundlegende Fragen sollen im Verlauf dieser Handreichung näher betrachtet und diskutiert werden.

EINSATZBEREICHE VON PASSWÖRTERN



Einige Einsatzbereiche von Passwörtern: Nicht überall braucht man eine gleiche hohe Sicherheit.

ABSICHERUNG EINER WEBSEITE MIT EINEM PASSWORT

Viele Schulen haben einen passwortgeschützten Bereich auf ihrer Homepage, weil sie zum Beispiel die Sprechstunden der Lehrkräfte veröffentlichen, diese aber nicht weltweit einsichtig machen wollen. Das Passwort wird dann über einen Elternrundbrief kommuniziert und jährlich geändert. Selbst bei einem einfachen Passwort ist mit dieser Maßnahme die Verbreitung der Webseite eingeschränkt und auch von Suchmaschinen wird eine solche Webseite nicht gefunden.

WLAN-PASSWORT

Das WLAN einer Schule soll für alle Lehrkräfte, Schülerinnen und Schüler oder auch Besucher einen Zugang ins Internet ermöglichen. In diesem Fall genügt ein gemeinsames Passwort für alle Schüler, das so gewählt wird, dass es auch auf mobilen Geräten leicht einzutippen ist. Der Personenkreis, für den das WLAN einer Schule erreichbar ist, ist ohnehin eingeschränkt, weil man sich im Gebäude oder in der Nähe des Gebäudes befinden muss.

Eine höhere Sicherheit ist beim WLAN-Zugang zu Hause erforderlich, da die Computer im Heimnetzwerk häufig nicht gut geschützt sind. Hier sollte das WLAN-Passwort nur den Familienmitgliedern bekannt und nicht zu erraten sein.

VERSCHLÜSSELUNG VON DOKUMENTEN ODER DATENTRÄGERN

Die Verschlüsselung dient dem Schutz vertraulicher Daten. Die Wahl des Passwortes entscheidet unter anderem, ob die Verschlüsselung auch automatisierten und professionellen Entschlüsselungsversuchen standhalten kann.

SPERREN DES LOKALEN COMPUTERS

In Büro- oder Verwaltungsumgebungen ist es üblich, den Arbeitsplatzcomputer zu sperren, wenn man den Arbeitsplatz kurzzeitig verlässt. Das Passwort zum Entsperren des Computers muss sehr häufig am Tag eingetippt werden. Da keine automatisierten Angriffe zu erwarten sind und der Personenkreis mit Zutritt zum Büro bekannt und in der Regel relativ klein ist, genügt ein eher einfaches Passwort.

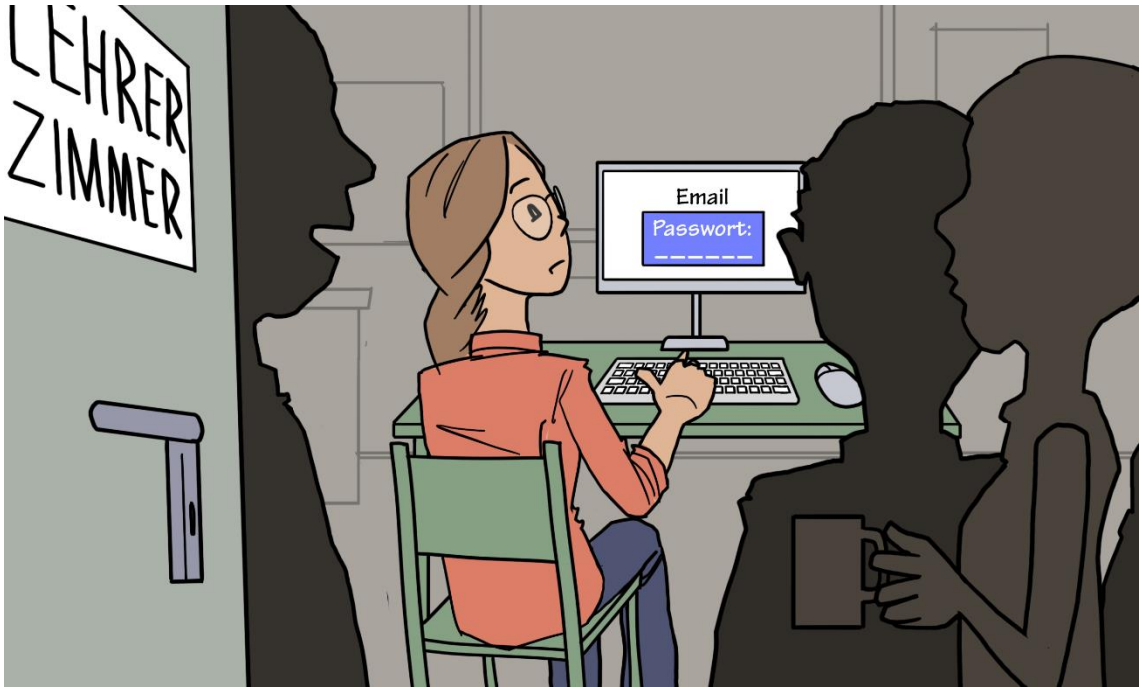
PASSWORT ZUM E-MAIL-KONTO

Der Kommunikation über E-Mail kommt eine zentrale Bedeutung zu, weil dies in Betrieben sowie in den Schulen meistens das verbindliche Kommunikationswerkzeug ist. Entsprechend groß kann das Interesse Dritter an den Zugangsdaten von E-Mails sein. Außerdem sind E-Mail-Accounts in der Regel weltweit erreichbar, wodurch der Personenkreis und das Zeitfenster für Anmeldeversuche erheblich ausgeweitet sind. Der E-Mail-Account wird von Online-Diensten auch verwendet, um Benutzer zu verifizieren oder um Passwörter zurückzusetzen. Das E-Mail-Konto sollte deshalb mit einem guten Passwort geschützt sein.

ZUGÄNGE ZU INTERNETPLATTFORMEN

Zugänge zu Internetplattformen, die sensible oder wichtige Daten enthalten, sollten entsprechend gut abgesichert sein.

AUSSPÄHEN VON ZUGANGSDATEN UND PASSWÖRTERN



Das beste Passwort hilft nichts, wenn es anderen bekannt wird.

MEHRFACHVERWENDUNG VON PASSWÖRTERN

Es ist schon mehrfach vorgekommen, dass Dritte, z. B. durch Social Engineering, an Passwort-Datenbanken von Online-Diensten gekommen sind und die darin enthaltenen Passwörter – gegebenenfalls nach deren Entschlüsselung – bei anderen Diensten ausprobiert haben. Ein sicheres Mittel dagegen ist, Passwörter nicht mehrfach zu verwenden.

Auch unseriöse Betreiber von Fake-Shops könnten alle Passworteingaben ihrer Benutzer protokollieren und diese bei anderen Online-Diensten ausprobieren.

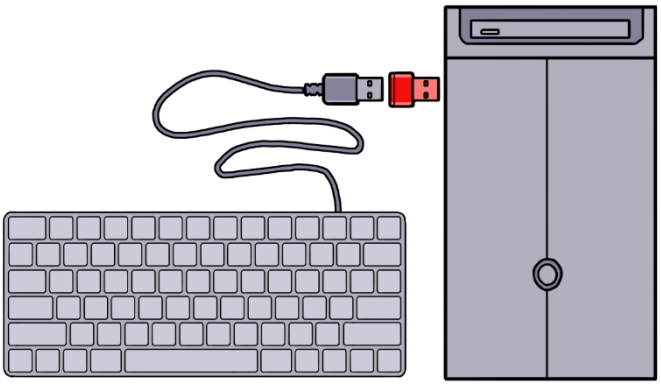
PHISHING

Über manipulierte E-Mails werden Benutzer verleitet, auf gefälschten Internetseiten persönliche Daten, wie z. B. das Passwort eines bestimmten Dienstes, preiszugeben.

SOCIAL ENGINEERING

Über einen „persönlichen“ Kontakt oder unter Vorgabe einer gefälschten Identität (z. B. Anruf einer „Sicherheitsfirma“), können Dritte die Zugangsdaten vom Anwender erhalten.

KEYLOGGER



Ein Keylogger ist eine Soft- oder Hardware, die es ermöglicht, die Eingaben direkt von der Tastatur in eine Datei zu schreiben. Die Eingaben über die Tastatur sind noch nicht verschlüsselt. Dies nutzen Keylogger aus, indem sie diese Signale direkt in eine Datei schreiben. Dazu muss der Angreifer aber direkten Zugriff auf den Computer haben, weil der Keylogger als Software entweder installiert oder als Hardware zwischen Computer und Tastatur eingesteckt werden muss. Auch zum Auslesen der gesammelten Daten ist üblicherweise ein weiteres Mal Zugriff auf den Computer erforderlich.

BRUTE-FORCE-ANGRIFF

Server, die aus dem Internet erreichbar sind, sind ständig Angriffen ausgesetzt. Interessant sind für Angreifer vor allem administrative Zugänge. Eine Möglichkeit hierfür ist der Brute-Force-Angriff, bei dem alle möglichen Zeichenkombinationen solange ausprobiert werden, bis das richtige Passwort gefunden wird.

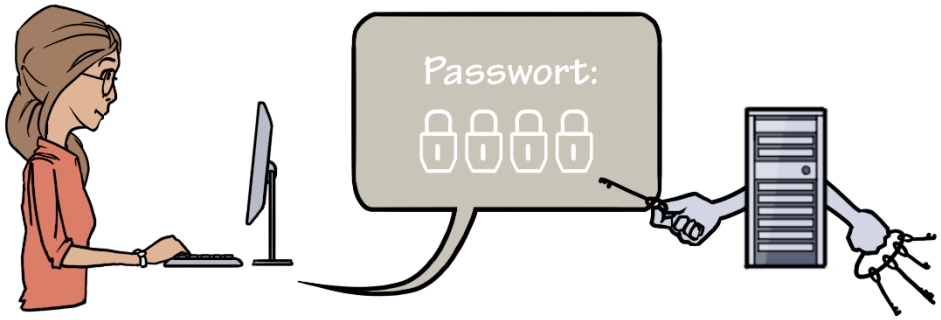
Die Grafik zeigt den in einer Log-Datei protokollierten Brute-Force-Angriff auf den ssh-Dienst, der für den Remote-Zugang zu einem Linux-Server genutzt wird. Erkennbar sind Datum, Uhrzeit und Name des angegriffenen Servers und die entsprechende Fehlermeldung, aus der auch die IP-Adresse des Angreifers hervorgeht.

```
Nov  9 11:45:19 server03 sshd[2808]: Failed password for invalid user vikas from 213.60.19.18 port 54438 ssh2
Nov  9 11:45:41 server03 sshd[2820]: Failed password for invalid user root from 218.106.92.66 port 2625 ssh2
Nov  9 11:45:52 server03 sshd[2823]: Failed password for invalid user root from 106.53.125.253 port 56938 ssh2
Nov  9 11:46:10 server03 sshd[2849]: Failed password for invalid user root from 114.220.76.22 port 44570 ssh2
Nov  9 11:46:18 server03 sshd[2851]: Failed password for invalid user root from 218.106.92.66 port 27713 ssh2
Nov  9 11:46:38 server03 sshd[2874]: Failed password for invalid user root from 123.207.175.111 port 39316 ssh2
Nov  9 11:46:45 server03 sshd[2880]: Failed password for invalid user oficina from 114.201.120.219 port 36570 ssh2
Nov  9 11:46:50 server03 sshd[2882]: Failed password for invalid user root from 142.93.254.122 port 54498 ssh2
Nov  9 11:47:07 server03 sshd[2913]: Failed password for invalid user osmc from 46.161.27.174 port 33630 ssh2
Nov  9 11:47:35 server03 sshd[2932]: Failed password for invalid user user from 106.13.50.219 port 53098 ssh2
Nov  9 11:47:56 server03 sshd[3013]: Failed password for invalid user root from 23.97.180.45 port 50682 ssh2
Nov  9 11:48:24 server03 sshd[3039]: Failed password for invalid user student from 114.220.76.22 port 46716 ssh2
Nov  9 11:48:44 server03 sshd[3074]: Failed password for invalid user root from 123.207.175.111 port 35066 ssh2
Nov  9 11:49:18 server03 sshd[3087]: Failed password for invalid user sambauser from 14.192.50.31 port 37588 ssh2
Nov  9 11:49:35 server03 sshd[3120]: Failed password for invalid user altibase from 213.60.19.18 port 53950 ssh2
```

MAN-IN-THE-MIDDLE-ANGRIFF

Bei einem Man-in-the-Middle-Angriff schaltet sich ein Angreifer zwischen die Verbindung eines Computers und dem Internet. Relativ leicht geht dies in einem öffentlichen WLAN. Wenn verschlüsselte Verbindungen (https) abgehört werden sollen, muss jedoch auch der jeweilige Computer manipuliert werden (Installation eines gefälschten Zertifikats).

SCHUTZMAßNAHMEN DER ANBIETER VON WEBDIENSTEN



Auch die Anbieter von Webseiten müssen Maßnahmen treffen, um das Ausspionieren oder Hacken von Zugangsdaten zu erschweren.

BEGRENZUNG DER ZAHL DER ANMELDEVERSUCHE

Muss der Anwender nach der Falscheingabe eines Passwortes eine gewisse Zeit bis zur nächsten Eingabe warten, erschwert dies die Möglichkeiten von Brute-Force-Attacken oder einem wahllosen Ausprobieren von Zugangsdaten. Der Zugang kann dabei für ein bestimmtes Benutzerkonto oder für eine bestimmte Absende-IP-Adresse gesperrt werden. Üblich ist es, dass nach ca. 3-5 fehlerhaften Anmeldeversuchen der Zugang für einige Minuten bis einige Stunden gesperrt wird. Dadurch ist auch bei weniger komplexen Passwörtern eine hohe Sicherheit gegeben.

Bei kritischen Zugängen, z. B. bei Online-Banking oder bei der Nutzung von EC- oder Kreditkarten, ist es auch üblich, nach zu vielen Fehleingaben den Zugang dauerhaft zu sperren.

GEOBLOCKING

Eine weitere Möglichkeit, Angriffe zu erschweren, ist das sogenannte Geoblocking. Dabei wird eine Anmeldung aus bestimmten Ländern bzw. IP-Adress-Bereichen unterbunden. Dies kann sinnvoll sein, wenn ein bestimmter Online-Zugang nur regionale Bedeutung hat oder wenn aus bestimmten Ländern immer wieder Brute-Force-Angriffe gestartet werden.

PASSWORTRICHTLINIEN

Passwortrichtlinien (z. B. Mindestlänge, Komplexität) sollen Anwender davor bewahren, zu einfache Passwörter zu verwenden. Die Passwortsicherheit wächst mit der Passwortlänge und dem verwendeten Zeichensatz. Der Zeichensatz kann aus Sonderzeichen, Zahlen, Groß- und Kleinbuchstaben gefordert werden.

ZWEI-FAKTOR-AUTHENTISIERUNG

Zur Erhöhung der Sicherheit kann ein Online-Anbieter eine Zwei-Faktor-Authentisierung aktivieren. Dies bedeutet, dass zusätzlich zum Passwort eine weitere Authentisierung verlangt wird (z. B. PIN über SMS, Code über App auf dem Smartphone, Zertifikat im Browser, Security-Token). Beim Online-Banking ist eine Zwei-Faktor-Authentisierung Standard.

VERSCHLÜSSELTE SPEICHERUNG DER PASSWÖRTER

Passwörter müssen bei einem Online-Anbieter nicht im Klartext gespeichert werden. Es genügt, wenn diese als Hashwerte (Ein-Weg-Verschlüsselung) gespeichert sind und damit nicht oder nur mit hohem Aufwand zurückgerechnet werden können.

Wenn sich ein Benutzer mit einem Passwort anmeldet, berechnet der Online-Anbieter den Hashwert des Passworts und vergleicht diesen mit dem gespeicherten Hashwert. Sind diese Hashwerte gleich, ist das Passwort korrekt.

Um aus einem Hashwert das Passwort zurückzurechnen, gibt es nur eine Methode: Ausprobieren verschiedener Passwörter, ob Sie zu dem Hashwert passen. Dies gelingt mit entsprechendem Aufwand bei kurzen Passwörtern (ca. 6-8 Zeichen) mit der Brute-Force-Methode oder bei längeren Passwörtern, wenn diese in einem Wörterbuch stehen (Wörterbuch-Attacke).

Eine praktische Möglichkeit, diese Attacken schneller durchzuführen waren lange Zeit sogenannte Rainbow-Tables. Dabei handelt sich um vorberechnete Tabellen mit Passwort-Hashes, die sehr schnell durchsucht werden können, um an das richtige Passwort zu gelangen. Eine Abhilfe dagegen ist das Password Salting, bei dem einem Passwort vor der Verschlüsselung eine zufällig generierte Zeichenkette (Salt) hinzugefügt wird. Dadurch haben auch zwei identische Passwörter verschiedene Hashwerte. Die Methode der Verwendung von Rainbow-Tables ist deshalb heute eher bedeutungslos.

Die verschlüsselte Speicherung von Passwörtern bietet für die Nutzer von Internetdiensten einen gewissen Schutz, falls die Datenbank des Online-Anbieters gehackt wird und alle gesammelten Benutzerdaten in falsche Hände geraten.

UMGANG MIT PASSWÖRTERN

ÄNDERN VON PASSWÖRTERN

Entgegen früherer Empfehlungen ist es inzwischen erwiesen, dass häufiges Wechseln eines Passworts die Sicherheit nicht erhöht. Nur bei einem konkreten Verdacht, dass ein Passwort bekannt geworden sein könnte, muss es sofort in ein vollständig anderes geändert werden.

SPEICHERN VON PASSWÖRTERN IN BROWSERN

Browser bieten die Möglichkeit, Zugänge zu Online-Diensten (Benutzername und Passwort) zu speichern und diese dem Benutzer anzubieten, wenn die entsprechende Webseite geöffnet wird. Einige Browser tun dies verschlüsselt, so dass der Zugriff nur über die einmalige Eingabe eines Passworts beim Öffnen des Browsers ermöglicht wird. Andere Browser speichern die Passwörter im Klartext. Den Komfort, Passwörter im Browser zu speichern, sollte man sich nur leisten, wenn keine andere Person Zugang zum eigenen Computer hat und wenn die entsprechenden Internetdienste keine kritischen Daten beinhalten. Auch Schadsoftware kann auf diese Weise gespeicherte Passwörter leicht auslesen.

NOTIEREN VON PASSWÖRTERN

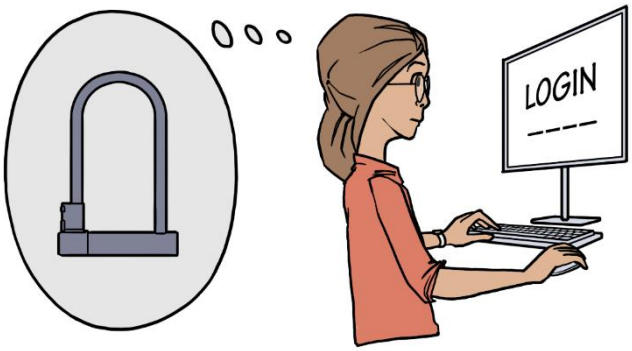
Viele Benutzerzugänge werden nur wenige Male im Jahr oder lange nicht mehr verwendet. Ein Vergessen der Anmeldenamen oder der Passwörter ist dabei normal. Entgegen früherer Meinungen ist es eine sinnvolle Maßnahme, Zugangsdaten handschriftlich zu notieren und diese an einem sicheren Ort aufzubewahren. Als Alternative zu den handschriftlichen Notizen könnte man die Passwörter in einem verschlüsselten Textdokument speichern.

PASSWORT-MANAGER

Als Passwort-Manager bezeichnet man Software oder Internet-Dienste, die dem Benutzer die Verwaltung vieler einzelner Passwörter abnehmen und die Zugangsdaten in einer Datenbank speichern. Der Benutzer benötigt nur ein einziges (sinnvollerweise möglichst komplexes) Passwort, um an die im Passwort-Manager gespeicherten Zugangsdaten zu gelangen.

Prinzipbedingt ist von Online-Diensten zur Passwortverwaltung eher abzuraten, da nie ausgeschlossen werden kann, dass der Betreiber Zugriff auf die gespeicherten Zugangsdaten hat oder diese durch Fehler in der Software öffentlich zugänglich werden.

WIE SICHER, LANG UND KOMPLEX MUSS EIN PASSWORT WIRKLICH SEIN?



Grundsätzlich kann man sagen: Je länger und komplexer ein Passwort ist, desto schwieriger ist es zu knacken. Deshalb muss bei der Frage nach der Passwortsicherheit der Komfort für Verwaltung oder Eingabe der Sicherheit gegenübergestellt werden. Bei der Risikobewertung können folgende Fragen betrachtet werden:

- Wie sensibel oder kritisch sind die Daten, die durch dieses Passwort geschützt werden?
- Wie interessant sind die Daten für andere?
- Wie lange hat ein potentieller Angreifer Zeit, um eine Brute-Force-Attacke durchzuführen?
- Wie groß und vertrauenswürdig ist der Personenkreis, der überhaupt Zugang erhalten könnte?
- Welche weiteren Sicherheitsmaßnahmen werden ergriffen, wie zum Beispiel Zwei-Faktor-Authentisierung oder die Begrenzung der Zahl von Fehlversuchen?

Im Folgenden werden dazu einige Fälle betrachtet:

EC-Karte

EC-Karten sind oft nur mit einer vierstelligen PIN aus den Zahlen null bis neun geschützt. Das sind 10^4, also 10.000 verschiedene Zahlenkombinationen. Ein Computer würde die richtige Kombination durch Ausprobieren sehr schnell finden. Allerdings muss man zu der PIN die Karte besitzen. Auch dauert es relativ lange, bis man einen zweiten Versuch für eine Eingabe vornehmen kann und das Konto wird nach drei Falscheingaben gesperrt, so dass eine vierstellige PIN für diesen Zweck sehr sicher ist.

Zugänge zu Internetplattformen

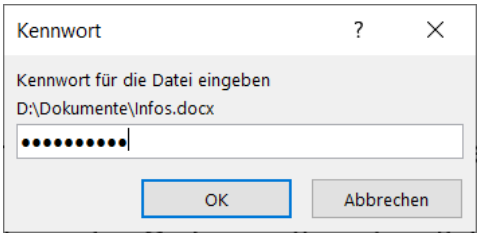
Zugänge zu Internetplattformen erfolgen in der Regel über einen Benutzernamen (bzw. E-Mail-Adresse) und über ein Passwort. Der Anbieter der Internetplattform hat gute Möglichkeiten den Zugang abzusichern. Am wirkungsvollsten ist die Begrenzung der Zahl der Anmeldeversuche. Wenn nur wenige Fehlversuche möglich sind, muss das Passwort nicht übermäßig lang und komplex sein.

Nur wenn dem Betreiber der Internetplattform die gesamte Passwort-Datei gestohlen wird und wenn dieser als Vorsichtsmaßnahme die Passwörter verschlüsselt gespeichert hat, würde ein langes und komplexes Passwort einen zusätzlichen Schutz bieten. In einem solchen Fall müssten jedoch ohnehin alle Benutzer zeitnah ihre Zugangsdaten ändern.

Viel entscheidender ist es, jedes Passwort nur bei einer einzigen Internetplattform zu verwenden.

Verschlüsselte Dokumente

Dateien oder Dokumente können mit einem der gängigen Verschlüsselungsprogrammen verschlüsselt werden. Insbesondere Office-Programme (Textverarbeitung, Tabellenkalkulation) bieten üblicherweise auch direkt eine Möglichkeit zur Verschlüsselung einzelner Dokumente. Zur Absicherung dient ein Passwort, aus dem der Schlüssel zum Entschlüsseln des Dokuments ermittelt wird. Wenn man davon ausgeht, dass das verwendete Verschlüsselungsverfahren sicher ist und das konkrete Programm keine Sicherheitslücken aufweist, hängt die Qualität der Verschlüsselung nur noch vom verwendeten Passwort ab.



Wenn ein Angreifer die verschlüsselte Datei auf seinem Computer gespeichert hat, hat er für das Entschlüsseln so viel Zeit, wie er möchte. Je nach Motivation kann er auch zusätzliche Ressourcen oder mehrere Computer einsetzten. Die Motivation hängt davon ab, was er sich von dem Inhalt verspricht. Als übliche Methoden stehen ihm dabei Brute-Force- und Wörterbuch-Attacken zur Verfügung. Der einzige Schutz gegen dieses Vorgehen ist ein möglichst langes und komplexes Passwort.

WEITERE INFORMATIONEN

BSI für Bürger – Sichere Passwörter erstellen

Bundesamt für Sicherheit in der Informationstechnik,
https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html

Passwort-Check

Bayerisches Staatsministerium für Digitales, https://www.stmd.bayern.de/service/passwort-check

Zugangsdatencheck

Auf folgenden Webseiten kann geprüft werden, ob die eigene E-Mail-Adresse bereits einmal einem Datenleck zum Opfer gefallen ist.

Hasso-Plattner-Institut, Potsdam, https://sec.hpi.de/ilc

Have I Been Pwned (HIBP), https://haveibeenpwned.com

Selbstlernkurs

Die vorliegende Handreichung ist auch als Selbstlernkurs der Akademie für Lehrerfortbildung und Personalführung verfügbar.