

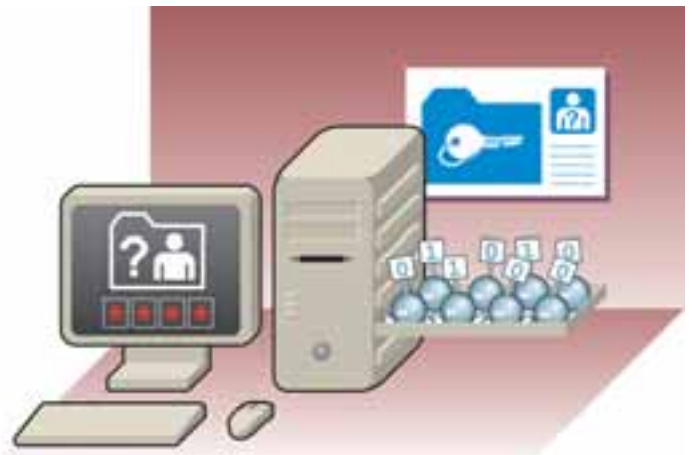
Zusammenfassung

Die Authentifizierung durch ein Passwort ist eine der ältesten Sicherheitstechniken. Sie wird nach wie vor sehr häufig verwendet und gilt als sicher, wenn dabei einige grundsätzliche Regeln eingehalten werden.

Wenn Sie Ihren Computer einschalten, Ihre Mails abrufen, eine private Website besuchen oder eine vertrauliche Datei einsehen möchten, müssen Sie meist ein Passwort eingeben, d.h. Sie werden um Authentifizierung gebeten, bevor Sie auf eine Ressource zugreifen dürfen.

Inhalt

- 1 Was ist ein Passwort? →
- 2 Welches sind die Risiken und wie lassen diese sich vermeiden? →
- 3 Wie wählt sich ein gutes Passwort? →
- 4 Wie erinnert man sich an sein Passwort? →
- 5 Hilfe, Passwort vergessen! →



1 Was ist ein Passwort?

Viele Authentifizierungstechniken beruhen darauf, dass ein Geheimnis nur demjenigen, der sich authentifizieren möchte (dem Anwender) und demjenigen, der die Authentifizierung verlangt (das Gerät, die Software), bekannt ist.

Dieses Geheimnis (Kennung) besteht entweder:

- aus etwas, das der Anwender besitzt (Karten, Abzeichen, Dokumente...)
- aus etwas, das der Anwender ist (Biometrie usw.)

- aus etwas, das nur der Anwender weiss (Passwörter usw.)
- aus einer Kombination dieser Techniken (Kreditkarten usw.)

Im Allgemeinen speichert ein System, das die Authentifizierung verlangt, ein Passwort nicht im Klartext, sondern in einer verschlüsselten Form (Hash=Verschlüsselung mittels hochkomplexer mathematischer Strukturen). Ihr Passwort und diese Hash-Funktion und nicht etwa das Passwort alleine, ermöglichen gemeinsam Ihre Authentifizierung.

2 Welches sind die Risiken und wie lassen diese sich vermeiden?

Vorsicht

Wenn jemand Ihr Passwort herausfindet, besteht das Hauptrisiko darin, dass diese Person Ihre Identität benutzt. Sie kann sich für Sie ausgeben und z.B. Ihre Mails lesen und beantworten, Ihr Mobiltelefon benutzen, Ihr gesamtes Geld auf ein anderes Bankkonto überweisen, Ihren Rechner zu kriminellen Handlungen missbrauchen, Sie überwachen oder zum Beispiel Ihren Arbeitsplatz ausspionieren, wofür Sie dann zur Verantwortung gezogen werden. Da diese Handlungen unter Vorspiegelung Ihrer Identität ausgeführt werden, müssen Sie später beweisen, dass nicht Sie für diese Handlungen verantwortlich sind. Das ist in manchen Fällen unmöglich! Sobald Sie glauben dass andere Zugriff auf Ihre Kennung haben,

informieren Sie sofort die für das System verantwortliche oder kompetente Person, Ihre Bank oder Ihren sonstigen Ansprechpartner. Welchen Sie sofort das entsprechende Passwort.

RATSCHLÄGE:

Geben Sie Ihre Kennungen so ein, dass Sie vor neugierigen Blicken geschützt sind, und verraten Sie jene niemandem. Seien Sie misstrauisch, wenn z.B. jemand behauptet, er sei der Netzwerktechniker und benötige Ihr Passwort für eine sehr dringende Arbeit. Solche Anfragen stammen in der Regel von Personen mit unlauteren Absichten!

3 Wie wählt sich ein gutes Passwort?

Im Allgemeinen besteht die Neigung, stets die gleichen bzw. leicht zu merkende Passwörter zu wählen, wie z.B. die Namen der Kinder, das Lieblingstier, das Geburtsdatum oder den Zunamen. Jemand, der Sie auch nur ein wenig besser kennt, ist daher in der Lage, Ihr Passwort zu knacken. Es ist daher ein möglichst willkürliches Passwort zu wählen.

Neben dieser Sicherheitslücke gibt es zwei andere gängige Arten von Attacken:

➔ Wörterbuchangriffe

Die in einem Wörterbuch enthaltenen Wörter sind zu meiden. Sie sind sehr anfällig, weil sie aus einem allen bekannten Wortschatz stammen. Kurz gesagt versucht der Cracker, Ihren Code zu knacken, indem er alle im Wörterbuch enthaltenen Wörter durchprobiert (solche Attacken können mit Hilfe hoch leistungsfähiger Computer-Tools durchgeführt werden).

➔ Brute-Force-Angriffe

Der Cracker versucht eine Kennung zu knacken, indem er alle möglichen Kombinationen durchprobiert. Um sich dagegen zu schützen, sollte man ein aus mindestens 8 Zeichen bestehendes Passwort wählen, das Ziffern, Buchstaben und Sonderzeichen enthält. Je länger ein Passwort ist, um so mehr Zeit benötigt der Cracker es herauszufinden und kann solange mit seinem Gerät nicht auf Ihre Informationen oder Ihren Computer zugreifen.

➔ Es ist nötig, das Passwort auswendig zu kennen. Im Übrigen gibt es spezielle Software, die hier Unterstützung bietet. Die Authentifizierungssysteme sind nämlich so konstruiert, dass sie nur eine begrenzte Anzahl falscher Eingaben zulassen, bevor der Zugang zum betreffenden Benutzerkonto vorübergehend oder ganz gesperrt wird.

➔ RATSCHLÄGE:

Merkmale eines guten Passworts:

- ➔ Mindestens 8 Zeichen (je mehr, desto besser).
- ➔ Zusammengesetzt aus Ziffern, Groß- und Kleinbuchstaben und Sonderzeichen.
- ➔ Es darf nicht auf einem Wort aus dem Wörterbuch basieren.
- ➔ Es darf sich nicht auf persönliche Daten stützen.
- ➔ Für jede verwendete Anwendung, Datei oder System ist ein anderes Passwort zu verwenden.
- ➔ Es muss willkürlich sein.
- ➔ Je nach seiner Funktion, ist das Passwort öfters zu ändern, unbedingt aber alle sechs Monate.

4 Wie erinnert man sich an sein Passwort?

Notieren Sie Ihre Passwörter nicht auf einen Zettel den Sie an den Monitor kleben oder unter der Tastatur bzw. als Telefonnummer getarnt, in Ihrer Brieftasche verstecken. Personen mit unlauteren Absichten kennen all diese kleinen Tricks. Ihr bester Trumpf sind Sie selbst und Ihr Gedächtnis. Verzichten Sie daher auf eine Notierung Ihrer Passwörter.

Falls die Liste Ihrer Passwörter zu umfangreich wird, können Sie immer noch eine Spezialsoftware zum Speichern der Passwörter verwenden. Das ist eine gute Lösung, bei der Sie jedoch auch wieder ein Passwort benötigen, damit sie funktioniert. Dieses Passwort sollte sehr sorgfältig gewählt werden, da sonst Ihre gesamten Passwörter entdeckt werden können.

➔ RATSCHLÄGE:

Ein gutes Mittel, um sich seine Passwörter zu merken, ist ein memotechnisches Verfahren wie z.B. der so genannte "magische Satz". Bilden Sie einen Satz, bei dem die Anfangsbuchstaben jedes Wortes den Zeichen Ihres Passworts entsprechen.

"Es waren einmal 3 kleine Schweinchen: Pim Pam Pum" ergibt das (hochsichere) Passwort Ewe3kS:PPP.

5 Hilfe, Passwort vergessen!

Wenn Sie Ihr Passwort vergessen haben, keine Panik! Lassen Sie sich vom zuständigen Verantwortlichen für das System sofort ein neues Passwort geben. Wenn es sich um ein Standard-Passwort handelt, nehmen Sie unverzüglich persönliche Anpassungen vor.

Bei der Authentifizierung im Internet gibt es in der Regel eine Wiederherstellungsfunktion. Es genügt, wenn Sie Ihre Identität angeben. Sie erhalten dann eine Mail mit der Wiederherstellungsfunktion, welche an die bei Ihrer Eintragung angegebene E-Mail-Adresse gesendet wird. Diese Mail ist nach Gebrauch zu löschen.