

Passwörter

1. [Überblick](#)
2. [Gute Passwörter](#)
3. [Passwort ändern](#)

1. Überblick

Schützen Sie Ihr Benutzerkonto (*Account*) mit einem **guten Passwort**, das Sie sich einfach merken können und das eine fremde Person oder ein Programm nur sehr schwer oder gar nicht (in vertretbarer Zeit) raten kann. Programme, die Passwörter "knacken" wollen (*Password Cracker*) arbeiten im Allgemeinen mit Wörterbüchern, sodass jedes Passwort, das man in einem Wörterbuch finden kann, ein schlechtes Passwort ist. "peter", "pEter", "pEter84" oder ähnliche Passwörter hat ein Programm in kürzester Zeit gefunden. Da die Rechenleistung immer größer wird, können Programme auch versuchen, alle möglichen Passwörter zu erzeugen und zu testen. Heutige Arbeitsplatzrechner (Mai 2008) können ca. 100.000.000 Passwörter pro Sekunde erzeugen und testen. Wenn Ihr Passwort nur aus fünf Kleinbuchstaben (z. B. "peter") besteht, muss das Programm nur alle Passwörter aus 26 Buchstaben mit den Längen eins, zwei, drei, vier und fünf erzeugen, um mit Sicherheit auch Ihr Passwort zu erhalten. In diesem Fall müssten also höchstens $26 + 26^2 + 26^3 + 26^4 + 26^5 = 12.356.630$ Passwörter erzeugt und verglichen werden. Das Programm hätte Ihr Passwort mit der sogenannten *Brut-Force*-Methode auf heutigen Arbeitsplatzrechnern in etwa 0,12 Sekunden gefunden. Wenn Sie ein ähnlich einfaches Passwort mit einer Länge von acht Zeichen gewählt hätten, müsste das Programm etwa $2,17 * 10^{11}$ Passwörter erzeugen und wäre damit bis zu 36 Minuten beschäftigt.

Falls Ihr Passwort Klein- und Großbuchstaben, Ziffern und Sonderzeichen (z. B. aus den folgenden zehn Sonderzeichen ", ; . : - _ ! % / #") enthält, hätten Sie bereits einen Zeichenvorrat von $26 + 26 + 10 + 10 = 72$ Zeichen. Bei einem Passwort der Länge acht müsste das Programm bei einem *Brut-Force*-Angriff bereits etwa $7,3 * 10^{14}$ Passwörter erzeugen und vergleichen, wozu es etwa 84 Tage benötigen würde. In der Regel würde das Programm Ihr Passwort wesentlich schneller finden. Wenn Sie Pech haben, befindet sich Ihr Passwort am Anfang der erzeugten Passwortliste und wird bereits nach wenigen Sekunden gefunden. Im Mittel wird ein Passwort von diesen Programmen in der halben Zeit (also etwa 42 Tagen) gefunden. Aus diesem Grund benutzen heutige Programme im Allgemeinen sogenannte *Wörterbuch-Attacken* anstelle von *Brut-Force-Attacken*, da sie damit bei vielen Passwörtern schneller zum Ziel kommen. Weitere Informationen finden Sie bei [Wikipedia](#).

In der Realität müsste das Programm Zugriff auf die Tabelle mit den verschlüsselten Passwörtern haben, da es die erzeugten Passwörter sonst nicht mit den realen Passwörtern vergleichen könnte.

[Seitenanfang](#)

2. Gute Passwörter

Ein gutes Passwort erfüllt die folgenden Anforderungen:

1. Es enthält mindestens einen Groß- und einen Kleinbuchstaben, mindestens eine Ziffer und mindestens ein Sonderzeichen.
2. Es ist mindestens acht (besser 12) Zeichen lang.
3. Es kommt ohne Berücksichtigung von Ziffern und Sonderzeichen sowie Groß-/Kleinschreibung in keinem Wörterbuch vor (auch nicht in fremdsprachigen Wörterbüchern).
4. Wenn Sie das Passwort ändern, ändern Sie mindestens drei Zeichen.

Halten Sie Ihr Passwort geheim! Ein Passwort, das Sie anderen Personen verraten oder aufschreiben und in der Nähe Ihres Rechners aufheben, ist kein gutes Passwort!

Sie können sich komplizierte Passwörter durch **Merksätze** merken, z. B. könnte der Merksatz "Mein neues Passwort ist jetzt 12 Zeichen lang" das gute Passwort "M#nP%ij12Z;l" liefern (Anfangsbuchstaben der Wörter und Sonderzeichen nach Großbuchstaben). Nehmen Sie keine bekannten Literaturzitate als Merksätze, da die auch den *Cracker*-Programmen bekannt sind.

[Seitenanfang](#)

3. Passwort ändern

Unter **UNIX**-Betriebssystemen (Solaris, Linux, Cygwin) wird das Passwort in einem Kommandozeilen-Fenster mit dem Kommando **passwd** geändert. Zuerst müssen Sie Ihr altes Passwort eingeben, um sich zu authentifizieren und dann das neue Passwort. Nachdem Sie das neue Passwort noch einmal zur Bestätigung eingegeben haben, um Tippfehler auszuschließen, wird das Passwort vom System geändert. Sie erhalten kein Echo für die eingegebenen Zeichen, sodass Sie nichts sehen, wenn Sie Ihr Passwort tippen. Das System erkennt Ihr Passwort trotzdem. UNIX verhindert auf diese Weise, dass ein anderer Benutzer bzw. eine andere Benutzerin die Länge Ihres Passworts ausspähen kann, um es einfacher brechen zu können.

Unter *Microsoft Windows 10* müssen Sie in den *Einstellungen* den Punkt *Konten* auswählen. Dort können Sie dann *Anmeldeoptionen* anklicken. Im Feld "Kennwort" klicken Sie dann auf "Ändern". Geben Sie jetzt Ihr altes Kennwort zur Authentifizierung und zweimal das neue Kennwort ein, um Tippfehler auszuschließen. Lassen Sie das Feld für den Kennwothinweis leer, da der Hinweis für alle Benutzer/innen des Rechners sichtbar ist und ihnen damit ermöglichen würde, das Passwort zu erraten. Die "Einstellungen" finden Sie, indem Sie mit der rechten Maustaste auf *Start* (unten links in der Menüzeile) und dann auf "Einstellungen" klicken.

Falls die Benutzeranmeldung über den *Novell Client für Windows* erfolgt (im Allgemeinen *Windows*-Rechner in den Rechnerräumen), drücken Sie einmal gleichzeitig die Tasten "<Strg><Alt><Entf>". Das Fenster "Novell Client für Windows" wird geöffnet. Wählen Sie "Passwort ändern" aus. Klicken Sie jetzt einmal auf den Namen des *Servers* vor Ihrem Benutzernamen und geben Sie dann Ihr altes Passwort zur Authentifizierung und zweimal das neue Passwort ein, um Tippfehler auszuschließen. Es dauert einige Sekunden, bevor das neue Passwort auf allen Rechnern benutzt werden kann.

Falls die Benutzeranmeldung auf einem **Windows Server** erfolgt (im Allgemeinen *Windows*-Rechner in den Rechnerräumen), drücken Sie einmal gleichzeitig die Tasten "<Strg><Alt><Entf>". Das Fenster "Windows Sicherheit" wird geöffnet. Wählen Sie "Kennwort

ändern..." aus und geben Sie dann Ihr altes Passwort zur Authentifizierung und zweimal das neue Passwort ein, um Tippfehler auszuschließen. Es dauert einige Sekunden, bevor das neue Passwort auf allen Rechnern benutzt werden kann.

[Seitenanfang](#)

Letzte Änderung: 02. November 2021 | [PDF-Version](#)

Der erforderliche *Acrobat Reader* zum Lesen der PDF-Datei kann z. B. kostenlos von der Firma *Adobe* bezogen werden.

