Zur Verfügung gestellt von
Mcert Deutsche Gesellschaft für IT Sicherheit
Weitere Informationen unter www.mcert.de

Wahl eines sicheren Passworts

Version 1.0
Letzte Änderung: 21. Juli 2005

Impressum
Mcert Deutsche Gesellschaft für IT-Sicherheit mbH
Vertreten durch den Geschäftsführer Stefan Gehrke
Albrechtstraße 10
10117 Berlin

Im Folgenden wird beschrieben, was ein sicheres Passwort ausmacht und wie Sie unsichere Passwörter vermeiden. Anhand von Beispielen werden zwei einfache Anleitungen für das Erstellen von sicheren, so genannten starken Passwörtern gegeben.

Inhaltsverzeichnis

1. Grundlagen der Passwortwahl

1.1. Einleitung
1.2. Beispiele für unsichere Passwörter

2. Erstellen von sicheren Passwörtern

2.1. Passwörter aus einem Satz generieren
2.2. Passwörter aus zwei kurzen Wörtern generieren
2.3. Variationen eines Basispassworts

3. Weiterführende Themen

3.1. Aufbewahren von Passwörtern
3.2. Wie Hacker versuchen, Ihre Passwörter herauszufinden

Hintergrundkästen

H1: 10 Regeln für den sicheren Umgang mit Passwörtern
H2: Etwas Mathematik

1. Grundlagen der Passwortwahl

1.1. Einleitung

Jeder, der mit Computern arbeitet, wird früher oder später ein oder mehrere Passwörter wählen müssen, um Zugang zu diversen Diensten zu erhalten. Für den Benutzer ist eine der wichtigsten Eigenschaften des Passworts, dass es sich gut merken lässt. Gut merken kann man sich einfache, prägnante Wörter oder persönliche Informationen. Genau darauf spekulieren auch Hacker - deswegen ist es wichtig, einen Mittelweg zwischen einem gut merkbaren und einem starken Passwort zu finden. Von einem starken Passwort wird dann gesprochen, wenn ein Passwort mit modernen Entschlüsselungstechniken nur sehr schwer zu knacken ist. Im Allgemeinen wird davon ausgegangen, dass Passwörter mit mehr als acht Zeichen, die Klein- und Großbuchstaben, Ziffern, Sonderzeichen und keine lexikographischen Wörtern enthalten, starke Passwörter sind.

1.2. Beispiele für unsichere Passwörter

In vielen Fällen wählen Computerbenutzer Passwörter, die Angreifer nicht einmal entschlüsseln müssen, sondern schon erraten können. Einige typische Beispiele für solche sich selbst verbietenden Passwörter sind alle Arten von Passwörtern, die auf persönlichen Daten des Benutzers basieren: z.B. der eigene Name, Namen von Kindern, Autokennzeichen oder andere Informationen, die Studien zu Ihrer Person offenbaren könnten. Genauso wenig sollten Sie Geburtstage oder Telefonnummern verwenden. Auch Umlaute im Passwort können zu Problemen führen, wenn Sie z.B. aus dem Ausland auf Mailaccounts zugreifen wollen. Beispiele für schlechte Passwörter:

Gerd, FCBayern, CheGuevara, Mausi23, B-NV966, 15072001, bienvenido1, Dylan4ever, 1dumbKopf, 867530, juan, hackme, AAAAA, Qwertz, poiuz, Ztrewq, dreg, 32isaum, hhhhhhh, 12345, ererer und so weiter.

H1 10 Regeln für den sicheren Umgang mit Passwörtern

1. Behalten Sie Ihr Passwort für sich.
2. Verwenden Sie nur starke Passwörter.
3. Keine benutzerbezogenen Daten in Passwörtern.
4. Passwörter sollten nicht an den Monitor geklebt oder in Word Dateien gespeichert werden.
5. Keine trivialen Tastaturkombinationen verwenden.
6. Nutzen Sie nicht für zwei Anwendungen dasselbe Passwort.
7. Die Qualität eines Passworts sollte dem Zweck angemessen sein.
8. Verwenden Sie nur dafür vorgesehene Programme um Passwörter zu speichern.
9. Verwenden Sie keine Umlaute im Passwort.
10. Erneuern Sie Ihre Passwörter regelmäßig.

2. Erstellen von sicheren Passwörtern

WICHTIG: Verwenden Sie auf keinen Fall die hier vorgestellten Passwörter! Erstellen Sie mit den vorgestellten Methoden auf jeden Fall ein eigenes starkes Passwort!

2.1. Passwörtern aus einem Satz generieren

Die bekannteste Methode, mit der starke und gut zu merkende Passwörter erstellt werden können, benötigt einen beliebigen Satz. Wählen Sie am besten einen Satz mit möglichst vielen Satzzeichen. Als

Beispiel wird hier der Anfang von Goethes Gedicht Prometheus gewählt: ***Bedecke deinen Himmel, Zeus, mit Wolkendunst!*** Nun wählen Sie als Passwort den ersten Buchstaben jedes Wortes, Satzzeichen bleiben bestehen. Das Ergebnis ***BdH,Z,mW!*** ist ein einfach zu merkendes, starkes Passwort.

2.2. Passwörter aus zwei kurzen Wörtern generieren

Wählen Sie zwei möglichst verschiedene Wörter. Für dieses Beispiel verwenden wir die Wörter *Saft* und *Schnur.* Verknüpfen Sie nun beide Wörter mit einem Satzzeichen. ***Saft;Schnur*** ist das Zwischenergebnis. Als nächstes ersetzen Sie je zwei Buchstaben durch Zahlen, zum Beispiel eine ‚9' an erster Stelle und eine ‚5' an siebenter Stelle. Fertig ist unser starkes Passwort: ***9aft;S5hnur***

2.3. Variationen eines Basispassworts

Für Benutzer, die sich viele Passwörter merken müssen, empfiehlt sich folgendes Verfahren: Erstellen Sie ein Basispasswort, dass Sie sich gut merken können, und verwenden Sie nun verschiedene Variationen dieses Basispasswortes. Diese Herangehensweise hat den Vorteil, dass Sie sich nicht viele Passwörter merken müssen, sondern nur Variationen eines Einzelnen. Auch hierfür ein Beispiel mit dem Passwort aus 2.1 als Basis. Verändert man den Satz folgendermaßen: ***Bedeckst deinen Himmel, Zeus, mit Gewitterwolken?*** Ergibt sich folgendes Passwort ***BdH,Z,mG?***

3. Weiterführende Themen

3.1. Aufbewahren von Passwörtern

Passwörter sind oft die einzige Möglichkeit, Informationen und Prozesse zu schützen. Deshalb ist ein verantwortungsbewusster Umgang mit Passwörtern unerlässlich. Das bedeutet in diesem Zusammenhang dafür zu sorgen, dass keine andere Person Zugriff auf das gewählte Passwort erhält. Ein beliebter Fehler: Das auf einen Zettel geschriebene Passwort an den Monitor kleben. Aber auch unter dem Tisch angebrachte, hinter der Tastatur versteckte oder in einer Word Datei gespeicherte Passwörter sind nicht sicher.

Daher gilt: Am besten ist es, sich Passwörter zu merken. Sollte es dennoch nötig sein, Passwörter irgendwo aufzubewahren, gibt es so genannte Passwort-Safe-Programme, die Ihre Passwörter verschlüsselt für Sie speichern. Diese Passwort-Safes gibt es in vielen Formen, beginnend mit einfachen kostenlosen Programmen, bis hin zum per Fingerabdruck gesicherten USB Stick.

3.2. Wie Hacker versuchen, Ihre Passwörter herauszufinden

Damit der Computer überprüfen kann, ob ein eingegebenes Passwort das Richtige ist, werden diese gespeichert. Um die Gefahr zu umgehen, dass jemand die Passwörter einfach ausliest, werden die Passwörter mit speziellen Kryptografiealgorithmen verschlüsselt. Passwörter zu knacken, bedeutet in diesem Zusammenhang also Passwörter zu entschlüsseln.
Die von Angreifern zu diesem Zweck verwendeten Programme heißen Passwort-Cracker und sind ohne Schwierigkeiten über das Internet zu beziehen. Die einfachste Art, ein Passwort zu entschlüsseln, besteht darin, alle möglichen Kombinationen von Buchstaben, Ziffern und Sonderzeichen durchzuprobieren, bis das korrekte Passwort gefunden ist. Solch ein Angriff wird Brute-Force-Angriff genannt, in Anspielung auf den Dieb, der mit purer Gewalt versucht, eine Tür aufzubrechen, anstatt zum Beispiel einen Dietrich zu benutzen.

Wegen der großen Menge von Zeichenkombinationen brauchen solche Programme aber viel Zeit, um ein Passwort zu entschlüsseln (siehe H2: Etwas Mathematik). Deutlich effektiver sind dagegen Passwort-Cracker, die Wortlisten verwenden. Das Programm probiert nacheinander Begriffe aus der

Wortliste, bis es das gesuchte Passwort gefunden hat. Umfangreiche Wortlisten mit den Basiswortschätzen vieler Sprachen sind im Internet verfügbar.

Aus diesem Grund sollten auf keinen Fall Passwörter verwendet werden, die nur aus Kleinbuchstaben bestehen oder in Wortlisten auftauchen können.

H2 Etwas Mathematik

Je nach Qualität eines Passworts variiert auch die Dauer, die ein Hacker braucht, um es auszurechnen. Hierzu ein paar Zahlen: Die Anzahl aller möglichen Kombinationen von Passwörtern, die aus fünf Kleinbuchstaben bestehen, beträgt 26 hoch 5, also 11.881.376. Ein Cracker-Programm schafft etwa eine Million Kombinationen pro Sekunde, was für das 5-stellige Passwort bedeutet, dass es in 11 Sekunden entschlüsselt ist.
Werden außer Kleinbuchstaben auch Großbuchstaben, Ziffern (0-9) sowie Sonderzeichen (&, !, ? etc.) verwendet, beträgt die Anzahl aller möglichen 5-stelligen Passwörter 82 hoch 5 = 3.707.398.432. Das entspricht ungefähr 3700 Sekunden à einer Million Kombinationen und ergibt eine Maximale Rechenzeit von einer Stunde. Deswegen sollte ein Passwort mindestens 8 Stellen besitzen. Denn 8 hoch 82 bietet immerhin 2.044.140.858.654.976 mögliche Kombinationen, was einer Rechenzeit von 64 Jahren entspricht. Auch wenn die hier angegeben Werte für Rechenleistung nur Beispielcharakter haben - schnellere Rechner oder aus mehreren Prozessoren zusammengesetzte Cluster bewältigen natürlich ein Vielfaches - ist der Unterschied zwischen 11 Sekunden und 64 Jahren bemerkenswert. Das Ausmaß dieser Differenz sollte Grund allein für die Wahl eines sicheren Passworts sein.