Auszug aus dem Buch
"FRITZ!Box - Von der optimalen Einrichtung bis zum Heimnetzwerk"
von Christoph Troche.

mitp-Verlag
978-3-95845-522-1

Ein sicheres Passwort generieren

Die Zeiten, da Hacker persönlich vor einem PC saßen und Passwörter in einen Computer hackten, sind längst vorbei. Hackerangriffe sind voll automatisierte Verfahren, in denen Rechner mit mehr als einer Milliarde Anschlägen pro Sekunde versuchen, das Passwort Ihres Netzwerks, Ihres Online-Banking-Accounts, Ihres E-Mail-Kontos und so weiter zu knacken. Auch wenn Sie es nicht merken, Ihr Netzwerk ist schon sehr oft angegriffen worden; wenn es noch nicht geknackt wurde, dann nur, weil Ihr Passwort gut genug war. Abbildung 5.4 gibt Ihnen eine Übersicht, wie lange es dauert, ein Passwort mit der Brute-Force-Methode zu erraten.

	Passwortlänge in Zeichen							
Zeichenraum	5	6	7	8	9	10	11	12
26 (a–z)	1 Sek	1 Sek	8 Sek	4 Min	2 Std	2 Tage	42 Tage	3 Jahre
52 (a–z, A–Z)	1 Sek	20 Sek	17 Min	15 Std	33 Tage	5 Jahre	238 Jahre	12400 Jahre
62 (A–Z, a–z, 0–9)	1 Sek	58Sek	1 Std	3 Tage	159 Tage	27 Jahre	1649 Jahre	102000 Jahre
96 (plus Sonderzeichen)	8 Sek	13 Min	21 Std	84 Tage	22 Jahre	2108 Jahre	202000 Jahre	19 Mio Jahre

Abbildung 5.4: So lange dauert es, ein Passwort zu knacken.

Beim Knacken von Passwörtern arbeiten Hacker im Wesentlichen mit zwei Methoden:

- Eine Methode benutzt Wörterbücher, um sie in rasender Geschwindigkeit als Passwörter auszuprobieren. Die Hacker-PCs laufen nicht einmal warm, dann ist das Passwort auch schon erraten.
- Die andere Methode, genannt Brute-Force (»rohe Gewalt«), probiert Zahlen- und Buchstabenkombinationen willkürlich. Die Zahlenkombination 1234 oder ABCD ist ebenfalls in Sekundenbruchteilen erraten. Weniger als fünf Zeichen stellen die Computer vor keine nennenswerte Aufgabe.

Tipp

Ein gutes Passwort ist mindestens acht Zeichen lang, enthält große und kleine Buchstaben, Zahlen und Sonderzeichen. Passwörter für den WLAN-Zugang sollten schon 20 Zeichen lang sein, da hier ein Offline-Angriff möglich ist: Ein Nachbar könnte beispielsweise versuchen, Ihr WLAN-Netzwerk durch einen Dauerangriff zu knacken.

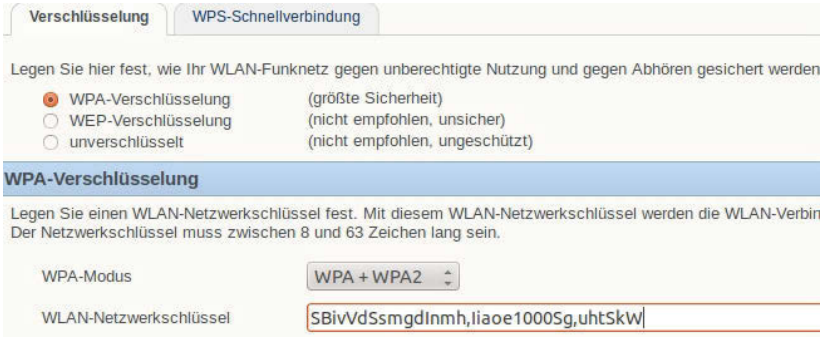

Abbildung 5.5: Dieses Passwort kann ich mir leichter merken als eine 16-stellige Zahl.

Die 16-stellige Nummer auf der Unterseite der Box kann ich mir niemals merken, Buchstabenkombination wie in diesem Bild jedoch sehr leicht: Wie? Ganz einfach: Schauen Sie doch mal nach, wie das Gedicht *Der Panther* von R. M. Rilke anfängt. Es ist eines meiner Lieblingsgedichte und den Anfang werde ich niemals vergessen. Von jedem Wort habe ich einfach nur den ersten Buchstaben genommen und aneinandergereiht. Sicherlich haben auch Sie irgendeinen Spruch oder eine Textzeile, die Sie im Schlaf herbeten können.

Ein gutes Passwort

Es sollte mindestens acht Zeichen lang sein.

Es sollte aus Groß- und Kleinbuchstaben sowie aus Sonderzeichen (?!%+ ...) und Ziffern bestehen.

Tabu sind Namen von Familienmitgliedern, des Haustieres, des besten Freundes, des Lieblingsstars oder deren Geburtsdaten usw.

Es darf nicht in Wörterbüchern vorkommen.

Es soll nicht aus gängigen Varianten und Wiederholungs- oder Tastaturmustern bestehen, also nicht asdfgh oder 1234abcd usw.

Einfache Ziffern am Ende des Passwortes anzuhängen oder eines der üblichen Sonderzeichen $! ? # am Anfang oder Ende eines ansonsten simplen Passwortes zu ergänzen, ist auch nicht empfehlenswert.

Speichern Sie das Passwort nie unverschlüsselt in Textform auf der Festplatte.

Die Buchstaben-durch-Zahlen-ersetzen-Methode

Die wichtigste Regel zum Erstellen eines sicheren Passwortes besagt, dass das beste Passwort eine rein zufällige Abfolge, bestehend aus allen Zeichen und Sonderzeichen, die Ihre Tastatur hergibt, ist. Natürlich sind diese Passwörter schwer zu merken. Wenn es sich aber um wirklich wichtige Daten handelt, sollten Sie trotzdem ein rein zufällig generiertes Wort wie z.B. *geK 7{m(6$ci* benutzen. Etwas sicherer sind zwar Passwortkombinationen aus Buchstaben und Zahlen, z.B. ist *Marion67* besser als *Marion*, aber auch diese Kombination ist nicht sicher. Ersetzen Sie doch einfach Buchstaben durch Ziffern. Dann würde aus *Marion67 Mar1on67*. Wenn Sie Ziffern verwenden, die Buchstaben ähnlich sehen, z.B. E durch die 3, O durch die 0, I durch eine 1 und die 5 durch das S ersetzen, entstehen schwer zu knackende Kennworte, die man sich trotzdem merken kann. Das Wort *Sommer* kann man sehr leicht knacken, das Wort *Somm3r* schon weniger leicht, und wenn Sie den besonders heißen Sommer 2003 *502Xm3r03* als Passwort nehmen, sind Ihre Daten sicher. (Wobei *mm* durch *2Xm* ersetzt wurde.)

So weit, so gut. Nun sollten Sie aber, und dies ist Regel Nummer zwei, ein Passwort nicht zwei Mal verwenden. Also sollten Sie sich eine Methode ausdenken, Ihr »sicheres Passwort« *502Xm3r03* dem jeweiligen Zweck zuzuordnen. Die einfachste Möglichkeit wäre es, Sie hängten diesen Zweck einfach hinten dran: Aus *502Xm3r03* wird dann für die Benutzung des großen Internetauktionshauses *502Xm3r03/ebay*. Und für Facebook eben *502Xm3r03/facebook*. Das macht es einem Hacker noch etwas schwieriger. Nicht mehr lösbar wird es, wenn Sie die Buchstaben des Zieles im Wort verstecken, z.B. an 2., 4. usw.

Position. Dann heißt das eBay-Passwort auf einmal *5eob2aXym3ro3*. Und Facebook wird mit *5foa2cXemb3orook3* erreicht. Das ist mit normalen Methoden nicht zu hacken. Sie müssen sich diese Passwörter ja nicht merken, die Eingabe erfolgt eh automatisch, nur müssen Sie sie gegebenenfalls herleiten können.

Die Anfangsbuchstabenmethode

Eine weitere beliebte Methode funktioniert so: Denken Sie sich einen Satz aus und benutzen Sie von jedem Wort nur den ersten Buchstaben (oder nur den zweiten oder letzten etc.). Anschließend verwandeln Sie bestimmte Buchstaben in Zahlen oder Sonderzeichen. Hier ein Beispiel: »*Morgens stehe ich auf und putze meine Zähne*.« Nur die ersten Buchstaben: »*MsiaupmZ*«. »*i*« sieht aus wie »*1*«, »*&*« ersetzt das »*und*«: »*Ms1a&pmZ*«.

Jeder kennt Sprichwörter wie »*das Spiel dauert neunzig Minuten und am Ende gewinnen die Deutschen«*. Indem Sie nur die Anfangsbuchstaben hernehmen, erstellen Sie daraus das Kennwort *dSd9oM&aEgdD*. Nehmen Sie einen Gedichtanfang, ein Sprichwort, irgendeinen Spruch. Sie können damit wunderbare Passwörter generieren.

Jedes Passwort sollte in regelmäßigen Zeitabständen geändert werden. Viele Programme erinnern Sie automatisch daran, wenn Sie das Passwort zum Beispiel schon ein halbes Jahr benutzen. Diese Aufforderung nicht gleich wegklicken – sondern ihr am besten gleich nachkommen! Natürlich ist es da schwer, sich alle Passwörter zu merken.

Bei vielen Softwareprodukten werden bei der Installation (bzw. im Auslieferungszustand) in den Accounts leere Passwörter oder allgemein bekannte Passwörter verwendet. Hacker wissen das: Bei einem Angriff probieren sie zunächst aus, ob vergessen wurde, diese Accounts mit neuen Passwörtern zu versehen. Ändern Sie daher unbedingt das vorgegebene Passwort sofort!

Vorsicht

Sie haben jetzt eine Reihe von Kennwörtern, verwechseln Sie sie nicht. Sie haben ein Kennwort, um auf die Benutzeroberfläche zugreifen zu können, ein Kennwort für Ihren Internetzugang (von Ihrem Internetanbieter zugesandt bekommen), ein Kennwort zur Verschlüsselung des WLAN-Netzwerks.