Passwort Check

Vielen Benutzern sind sichere Passwörter zu kompliziert und zudem müssen sich Benutzer heutzutage immer mehr Passwörter für verschiedene Systeme merken.
Man kann dann zwar argumentieren, dass Sicherheit selten bequem ist und sichere Passwörter einer der Grundsteine für eine sichere IT-Architektur und den Schutz der Daten ist, jedoch sehen dann nur wenige Benutzer dies ein.
Eine sichere und bequeme Lösung wäre der Einsatz von Hardware Tokens welche einen eindeutigen kryptographischen Schlüssel mit sehr vielen Stellen (z.B. 2048 Zeichen) generieren. Mit solch einer Lösung kann die Passwortsicherheit deutlich erhöht werden, denn das sicherste Passwort ist wertlos, wenn es von einem Trojaner mitgelesen wird. Ein weiterer Vorteil ist, das die Benutzer sich nur noch ein Passwort für das Token merken müssen. Dieser Lösungsweg ist jedoch mit Beratungs- und Kostenaufwand verbunden. Wir beraten Sie gerne über die verschiedenen Lösungsmöglichkeiten.

Für die Zwischenzeit, haben wir diese Seite geschaffen, um zu zeigen wie unsicher einfache Passwörter sind, indem wir einen Hackerangriff auf ein Passwort simulieren.

Ein Hauptproblem bei einfachen Passwörtern ist die enorme Rechenleistung moderner Prozessoren. Mit dieser Rechenleistung lassen sich einfach alle möglichen Kombinationen eines Passwortes durchprobieren, ein sogenannter Brute-Force Angriff.
Noch schneller geht das knacken wenn Ihr Passwort in einem Wörterbuch steht. Es ist heutzutage keine Problem mehr den kompletten Duden oder einen komplette Brockhaus Enzyklopädie innerhalb von Sekunden durchzuprobieren.

Aber auch ein Passwort wie zum Beispiel: "gnampf" ist mit einem sehr langsamen Prozessor (1.000.000 Versuche pro Sekunde) nach 89 Sekunden geknackt.
Mathematisch gesehen beträgt die Anzahl aller möglichen Kombinationen, von "aaaaaa" bis "zzzzzz" (Permutationen): 26^6 + 26^5 + 26^4 + 26^3 + 26^2 +26^1 = 321.272.406
Da jedoch bei "gnampf" nicht alle Kombinationen durchprobiert werden müssen, sondern nur ein Teilraum

("aaaaaa" bis "azzzzz" + "aaaaaa" bis "gnampf") reduziert sich die Anzahl der Kombinationen auf 13.087.986 und oben genannte 89 Sekunden.

Um nun ein Passwort sicherer zu machen kann man nun folgendes tun:

Die Länge erhöhen.
Bei 8 Zeichen würde sich obige Reihe um 26^8 + 26^7 verlängern."gnampfgn" würde auf dem langsamen Prozessor 16,8 Stunden benötigen.(60.565.599.628 Kombinationen)
Großbuchstaben verwenden.
Dadurch verdoppelt sich die Anzahl der möglichen Buchstaben (52^8 + 52^7...).
"Gnampf" würde 210 Minuten benötigen (12.649.272.278 Kombinationen) und "GnampfGN" hingegen schon 395 Tage. (34.203.632.241.468 Kombinationen)
Ziffern benutzten.
In Kombination mit Großbuchstaben erhöht sich die Basis um 10 auf 62^X.
"Gnampf1" würde 524 Stunden benötigen (1.887.251.570.450 Kombinationen) und "GnampfGN1" 230 Jahre. (7.254.595.036.731.610 Kombinationen)
Sonderzeichen benutzten.
Die einfachen Sonderzeichen (!\"§$%&/()=*/+-) erhöhen in Kombination mit dem obigen die Basis um 14 auf 76^X.
"Gnampf1%" würde 15,4 Jahre benötigen (485.992.196.164.779 Kombinationen) und "GnampfGN1" 89.012 Jahre. (2.807.090.925.047.570.000 Kombinationen)
Wenn Sie jetzt denken mit GnampfGN1% sind Sie auf der sicheren Seite, dann haben Sie zwar nicht ganz unrecht, jedoch rüstet der schlaue Hacker dann auf und mietet sich einfach Rechenleistung bei einem großen Buch- und Gemischtwarenhändler.
Für ca. 120 Cent pro Stunde hat er dann "einen Prozessor" mit 10.000.000.000 Versuchen pro Sekunde. Damit ist "GnapmfGN1%" "schon" in 8,90 Jahren geknackt. Mit etwas mehr Rechenleistung sinkt dieser Wert jedoch schnell wieder in Richtung Tage. Daher noch der letzte Tipp:
Erweiterte Sonderzeichen benutzten. Die erweiterten Sonderzeichen (,.:;_~@^°#|`<>{[]}\ ) erhöhen in Kombination mit dem obigen die Basis um 20 auf 96^X.
"Gnampf1%[" würde 7,5 Jahre auf dem Hochleistungsprozessor benötigen (239.111.477.655.024.000 Kombinationen) und "GnampfGN1%[" 68.877 Jahre. (2.203.651.378.066.890.000.000 Kombinationen)
Daraus folgt, dass ein Passwort welches den vollen Zeichenumfang nutzt (Basis 96) die sicherste Wahl ist.
Und letztlich ist ein komplexes Passwort, welches zur Not aufgeschrieben werden muss, besser als ein schwaches, welches Online innerhalb von Minuten erraten werden kann.
Des Weiteren sollten Sie unterschiedliche Passwörter benutzen um bei einem Datenleck nicht gleich einen Generalschlüssel zu verlieren. Variieren Sie hierbei ein sicheres Passwort, indem Sie es mit dem möglichscht verschleierten Anmeldezweck kombinieren z.B. gleGnampfGN1%[goo statt (gooGnampfGN1%[gle) oder nkGnampfGN1%[Ba statt (BaGnampfGN1%[nk).

Hier können Sie Ihr Passwort überprüfen und auch sichere Passwörter generieren lassen.
Dabei werden keine Daten gespeichert oder von diesem Server mitgelesen.
Trotz dieser Maßnahmen, sollten Sie hier nie echte Passwörter testen, da eine 100 prozentige Sicherheit nie garantierbar ist.
Variieren Sie daher ihr Passwort etwas und testen dann die Stärke dieses Passwortes.

Für die Berechnung der Brute-Force Zeit haben wir folgende Annahmen getroffen:
P4 2,5 GHz ca. 5.000.000 Versuche / Sekunde
Core 2 2,66 GHz Quad ca. 20.000.000 Versuche / Sekunde
Core i7 3,3 GHz ca. 150.000.000 Versuche / Sekunde
Grafikkarten (z.B.eine moderne Geforce) ab ca. 500.000.000 Versuche / Sekunde
Hochleistungsrechenservice ca. 10.000.000.000 Versuche / Sekunde

Passwort Überprüfung

Passwort

Löschen Absenden

Passwort Generator

Passwort Stärke auswählen: ▼

Löschen Absenden

Interessante Links zum Thema Passwortsicherheit:
Wikipedia Artikel zum Thema Passwort
Wikipedia Artikel zum Thema Brute-Force
Tipps für sichere Passwörter vom BSI

So finden Sie uns:

Gunter Kaufmann
EDV-Konzepte und Realisierung
IT Service und Systemhaus in Hamburg
Tangstedter Landstr. 157
22417 Hamburg
Impressum

Kontaktieren Sie uns:

Tel.: 040 / 530 500 63
Fax: 040 / 530 500 64

E-Mail: info@gk-edv.de

Datenschutzerklärung

IT Support Helpdesk:

Montag - Freitag: 9 - 19 Uhr
(außerhalb dieser Zeiten über Notfallnummer)

Teamviewer Quicksupport Windows