Passwort - Attacken: Wie sicher ist deins?

Gute Passwörter sind heute noch nicht mit vertretbarem Aufwand hackbar, schlechte Passwörter in Millisekunden.

- Passwort - Eine gute Wahl
- Passwort - Ausspioniert

Florian13, Zeus007, CoolBrain, nugneH, ...

- Der Hacker hat Milliarden Versuche pro Sekunde
- Die deutsche Sprache etwa 75.000 Wörter
- Englisch, Namens- und Filmlexika und griechische Mythologie sind noch ein paar 100.000 Wörter und Namen mehr - also ein paar Millisekunden mehr Arbeit
- und ein klingonisches *nugneH* (Guten Tag) bringt auch nur Millisekunden

Der Hacker weiß, daß ...

- er auf einem modernen PC mehrere Milliarden Versuche pro Sekunde hat
- die Deutsche Sprache gerade mal 75.000 Wörter kennt
- die meisten User Passwörter aus dem eigenen Sprachraum oder Englischen nehmen
- Großbuchstaben meist nur am Anfang von Passwörtern vorkommen
- Ziffern meist in Gruppen am Anfang oder Ende vorkommen
- 68% der Frauen ihren Vornamen mit einbauen (54% der Männer)
- insgesamt in über 90% der personenbezogenen Passwörter Vorname / Zuname / Kosename / Haustiername oder eine Kombination davon eingebaut sind,
- häufig ergänzt um Telefon-/ Autonummern und Jahreszahlen
- 90% der Passwörter 6-8 Zeichen lang sind
- Passwort-Spickzettel an Monitoren und unter Tastaturen kleben; 80% der aufgeschriebenen Passwörter befinden sich nämlich am Arbeitsplatz im Umkreis von 2 Metern
- gerne auch Seriennummern oder Ähnliches genommen wird, was man vom Arbeitsplatz aus sieht

Der Hacker hat Software ...

- die obiges Wissen über typische Passwortwahl implementiert hat
- die auf einem modernen PC mehrere Milliarden Versuche pro Sekunde durchführt
- mit statistisch sortierten Wörterbüchern aus mehreren Sprachen inklusive Namenskatalogen (Vornamen, Zunamen, griechische Mythologie, Filme), und Kultworten kommt

Zum Passwort-Hacken braucht es keine Ausbildung!

Einfach nach Passwort-Crackern googeln, Software downloaden, auf CD oder USB-Stick spielen, und PCs hacken.

Passwort Attacken

Brute Force Attacke (Rohe Gewalt)

Alle möglichen Kombinationen werden ausprobiert. Je länger ein Passwort ist und je mehr Zeichen möglich sind, desto länger dauert die sichere Dekodierung. Kennt der Hacker die Passwort-Regeln, vereinfacht sich seine Aufgabe, z.B:

- Wenn die minimale Passwort-Länge in einer Firma 8 Zeichen sein muß, braucht er Passwörter mit 7 und weniger Zeichen nicht probieren.
- Wenn er zusätzlich weiß, daß ein System nicht mehr als 8 Zeichen unterscheidet (wie Sun/Solaris Logins), braucht er auch keine längeren Passwörter probieren
- Wenn er weiß, daß bestimmte Zeichengruppen als Muß vorgegeben sind, verringert das die Zahl der möglichen Kombinationen

Wörterbuchangriff

Ein Passwort wird mittels einer Passwörterliste (Wörterbuch) entschlüsselt. Dabei werden einfach alle Passwort-Variationen, die in der Liste enthalten sind ausprobiert. Meist kombiniert mit Anhängen von Zahlen und Sonderzeichen und permutierter Groß-/Kleinschreibung.

Passwörter, die aus Namen, Worten einer gängigen Sprache, aus der griechischen Mythologie, aus Filmen oder Kultworten, mit angehängten oder vorausgestellten Zahlen und Sonderzeichen erstellt wurden, werden damit innerhalb weniger Sekunden geknackt.

- *Gandalf73* ist halt eine schlechte Wahl, ebenso wie
- Ikarus-207
- 1968Sabine
- SesamÖffneDich