MERKBLATT / Sind Passwörter sicher?

Machen Sie das das Passwort-Knacken nicht so einfach
Es kann jedes Passwort geknackt werden. Die Dauer ist abhängig von der Komplexität, der Länge des Passwortes und der verwendeten Hardware. Beispiele:

Der Wörterbuchangriff
Eine Software probiert jedes Wort einer Passwortliste und/oder eines Wörterbuches aus. Ein normaler PC benötigt für den kompletten Durchlauf mit Sprachen nur wenige Sekunden.

Der Brute-Force-Angriff
Als Brute-Force-Methode bezeichnet man das Ausprobieren aller möglichen Zeichenkombinationen mittels einer Software (Algorithmus), bis das Passwort gefunden ist. Auch sinnfreie Kombinationen werden getestet.

Benötigte Zeit: Ein 6-stelliges Passwort in 6,8 Sekunden geknackt
Hat das Passwort die Länge von 6 Zeichen und besteht nur aus Kleinbuchstaben, kann es aus 26 verschiedenen Zeichen bestehen, was insgesamt 308.915.000 (also fast 309 Millionen) Kombinationen zulässt. Mit einem PC sind 45.423.000 Tastenanschläge pro Sekunde möglich. Schwächere CPUs erreichen leicht immerhin die Hälfte davon. Benötigte Zeit: unter 10 Sekunden! Besteht Ihr Kennwort aus Klein- / Großbuchstaben und Zahlen, gibt es bei 6 Zeichen schon 56.800.235.000 Kombinationsmöglichkeiten. Die Zeit beträgt dann ca. 20 Minuten. Bei 7-stelligen Passwörtern werden

aus den 20 Minuten fast 22 Stunden; für 8 Zeichen fast 2 Monate; für 10 Zeichen fast 600 Jahre. Sonderzeichen und jede weitere Stelle verlängern die Berechnung um ein Vielfaches!

Die sieben häufigsten Passwort-Fehler sind:

- Zu einfaches Passwort (z.B. der Vorname oder nur Zahlen; zB. 123456789)
- Zu kurzes Passwort (weniger als acht Stellen)
- Speichern von Passwörtern
- Gleiche Passwörter bei allen Gelegenheiten
- Jahrelang das gleiche Passwort
- Notieren der Passwörter am oder um den PC
- Passwörter ungesichert abgelegt

24. Dezember 2013

Join-the-Web GmbH Internet- und Multimediadienstleistungen

www.join.the-web.ch

Mitglied P-Gruppe www.p-gruppe.ch