

ProtectStar™, Inc.

Der Zusammenhang zwischen Passwortlänge und Brute-Force-Attacken

Brute-Force-Attacken sind Versuche eines Programms, das Passwort eines anderen Programms zu brechen, indem alle möglichen Kombinationen von Buchstaben, Zahlen und Sonderzeichen ausprobiert werden. Daher ist ersichtlich, dass die Passwort-Länge bzw. die Passwort-Kombination den Zugriff auf Passwort-gesicherte Zugänge erschwert wenn nicht sogar unmöglich macht.

Wählt der Anwender ein Passwort, das bspw. nur aus **sechs Kleinbuchstaben** besteht, so steht fest, dass der derzeit (Stand: *April 2010*) schnellste Einzel-PC eines Privatanwenders ca. **1.300.000.000** (in Worten: 1,3 Milliarden Schlüssel in der Sekunde generieren kann (Quelle siehe: <http://www.orange.co.jp/~masaki/rc572/ratee.php>).

Möglich wird diese hohe Rechenanzahl pro Minute zum Beispiel mit Hilfe der CUDA Technologie in Grafikkarten von NVIDIA™ (http://www.nvidia.de/object/cuda_home_de.html#)

Der aktuell schnellste und einsatzbereite Supercomputer der Welt - der **Blue Gene/L** (Stand: *November 2008*) im **Lawrence Livermore Institut** (USA) - besitzt eine Leistung von **478,2 Teraflop**. Dies entspricht umgerechnet in Rechenoperationen pro Sekunde, dass Blue Gene/L circa **6.3 Millionenmal** schneller ist, als der schnellste Einzelplatz-Computer.

Bei einem Passwort, das aus lediglich **sechs Kleinbuchstaben** besteht, sind rein rechnerisch **308.915.776** verschiedene Buchstabenkombinationen möglich, so dass der genannte Einzelplatz-Computer im schlechtesten Fall nur **0,24 Sekunden** benötigen würde, um alle Kombinationen auszuprobieren.

Die mathematische Regel zur Berechnung der Kombinationsmöglichkeiten lautet an diesem Beispiel:

Kombinationen = 26 (hoch 6)

= 26 * 26 * 26 * 26 * 26 * 26

= 308.915.776 / 1.300.000.000 Keys/sec

= **0.24 Sekunden**

Würde man die Länge des Passwortes auf **7 Zeichen** erhöhen, so erhält man:

Kombinationen = 26 (hoch 7)
= $26 * 26 * 26 * 26 * 26 * 26 * 26$
= 8.031.810.176 / 1.300.000.000 Keys/sec
= **6,2 Sekunden**

Erhöht man die Länge des Passwortes weiter auf **8 Zeichen**, so erhält man:

Kombinationen = 26 (hoch 8)
= $26 * 26 * 26 * 26 * 26 * 26 * 26 * 26$
= 208.827.064.576 / 1.300.000.000 Keys/sec
= 160 Sekunden
= **2,6 Minuten**

Würde man bspw. als Passwort einen Satz wie "**meinnameisthase**" - aus insgesamt **15 Kleinbuchstaben** – verwenden, so erhält man:

Kombinationen = 26 (hoch 15)
= $1.677.259.342.285.725.925.376 / 1.300.000.000$ Keys/sec
= 1.290.199.494.065 Sekunden
= 21.503.324.901 Stunden
= 895.971.870 Tage
= **2.454.717 Jahre**

Im Vergleich jedoch zu dem **Blue Gene/L Supercomputer** würde dieser für das Passwort "**meinnameisthase**" ein wesentliches weniger an Zeit benötigen:

Kombinationen = 26 (hoch 15)
= $1.677.259.342.285.725.925.376 / 478$ Teraflop
= ~ 3.508.910 Sekunden = ~ 58.481 Minuten = ~ 2436 Tage
= ~ **6,6 Jahre**

Künftig verfügbare Supercomputer wie „Roadrunner“ (ein IBM Hybridsystem mit mehr als **1,026 Milliarden** Rechenoperationen pro Sekunde [**1,026 PetaFLOPS**]) im **Rüstungsforschungsinstitut National Laboratory (LANL)** benötigt für das Passwort-Beispiel "**meinnameisthase**" folgende Zeit:

Kombinationen = 26 (hoch 15)

= 1.677.259.342.285.725.925.376 / 1026 Teraflop

= ~ 1.635.093 Sekunden

= ~ 27.251 Minuten

= ~ 1135 Tage

= ~ **3,1 Jahre**

Das optimale Kennwort:

Die Forschungsabteilung von ProtectStar™, Inc. empfiehlt Anwendern, ein Passwort zu wählen, das aus folgenden Anforderungen besteht:

Passwortlänge:

- mindestens 12 Zeichen

zu verwendende Zeichen:

- Großbuchstaben (A, B, C, ... Z)

- Kleinbuchstaben (a, b, c, ... z)

- Zahlen (1, 2, 3, ... 9)

- Sonderzeichen (*, #, =, ... +)

Beispiel eines optimalen Kennworts:

#25XZc74%.Re