

DA FREUEN SICH DIE HACKER: DIE SCHLECHTESTEN PASSWÖRTER 2013

Veröffentlicht am 21. Januar 2014 von Rüdiger

Fast täglich liest man Neuigkeiten zum NSA-Skandal. Der amerikanische Auslandsgeheimdienst spähte unter anderem in Deutschland im großen Stil Internetverbindungen aus. Von russischer und chinesischer Seite kamen nicht minder schwere Attacken. Auch Kunden des Softwareunternehmens Adobe konnten sich 2013 nicht auf den Schutz ihrer Daten verlassen. Drei Millionen Kundendaten fielen Hackern in die Hände.

Der logische Schluss: Es muss mehr für die Datensicherheit getan werden. Die einfachste Schutzmaßnahme ist ein gutes **Password**. Vor diesem Hintergrund kann man bei der Wahl mancher Passwörter nur den Kopf schütteln.

HIER DIE SCHLECHTESTEN PASSWÖRTER 2013 LAUT EINER ERHEBUNG DER FIRMA SPLASHDATA:

1. 123456
2. password
3. 12345678
4. qwerty
5. abc123
6. 123456789
7. 111111
8. 1234567
9. iloveyou
10. adobe123

SplashData wertete für die Rangliste gehackte Nutzerdaten aus, die veröffentlicht worden waren. Den Leichtsinn oder die Unwissenheit dieser Nutzer mag mancher Leser amüsant finden. Wenn man über die möglichen Folgen eines Hackerangriffs nachdenkt, vergeht einem aber das Lachen. Wer etwa die Zugangsdaten zu einem **Online-Banking**-Konto in Erfahrung bringt, ist von Überweisungen in Ihrem Namen nicht mehr weit entfernt.

Gerade Unternehmer müssen sich in Acht nehmen: Ein Eindringen in Ihre Firmen-Accounts kann katastrophale Konsequenzen haben. [Sensible Daten](#) zu Ihren Kunden, Strategiepapiere und Personaldaten: Alles Informationen, die ein Firmengeheimnis bleiben müssen und den bestmöglichen Schutz verlangen.

Bei der Wahl des Passworts können Sie einen wichtigen Beitrag zur Wahrung Ihrer Geheimnisse

leisten. Ein gutes **Passwort** besteht aus mindestens acht Zeichen. Damit sind jedoch keine Zahlenfolgen wie 12345678 gemeint. Vielmehr sollten Sie Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen verwenden. Jedes dieser Zeichen darf nur einmal in dem Passwort enthalten sein. Auch wenn der Begriff „Passwort“ es nahelegt: Nehmen Sie keine Wörter als Passwort! Eine kryptische Zeichenfolge wie beispielsweise Np&“hFqß bietet da mehr **Sicherheit**.

Aber auch der Umgang mit Ihrem Passwort spielt eine Rolle: Selbst wenn Ihre Login-Daten perfekt wären, werden Sie wertlos, wenn jemand Sie herausfindet. Speichern Sie deshalb kein Passwort in einem Textdokument oder an einem anderen leicht zugänglichen Ort auf Ihrem Computer ab. Ein PC ist schnell gehackt. Laden Sie sich lieber einen kostenlosen Password-Manager wie das Programm [Keepass](#) herunter.

Unsere Media Company generiert für seine Partnerunternehmen sichere [Zugangsdaten](#). Dazu gehören kryptische Passwörter, die eine optimale **Datensicherheit** garantieren. Wenn sie Fragen zum Thema Datenschutz haben, beraten wir Sie gerne. [Sprechen Sie uns einfach](#) darauf an!