

kurzbericht | das passwort-dilemma

Passwörter hatten einmal etwas Romantisches an sich:

Der Held, der an der versteckten Pforte nach dem Passwort gefragt wird, bevor er Einlass zu den geheimen Gemächern erhält, taucht in vielen Abenteuerfilmen auf. Das allerdings war lange vor dem digitalen Zeitalter. Die Helden von damals mussten sich noch nicht überlegen, ob ihr Passwort stark genug sei, einem Bösewicht mit einem Laptop zu widerstehen, der schwache Passwörter in wenigen Sekunden entschlüsseln kann. Damals genügte ein schöner Frauenname, um einen wirksamen Passwortpakt zu schliessen.

Doch mit dieser Art von «Sesam öffne dich» ist es im Internetzeitalter endgültig vorbei. Wenn Sie auf Ihrem PC oder am Internet den Vornamen Ihrer Frau oder Ihres Liebblings als Passwort benutzen, dann ist das nicht nur leichtsinnig, sondern extrem unvorsichtig - und zwar nicht nur, wenn Sie Ihre Daten vor Ihrem Partner schützen wollen.

Die wachsende Zahl der Benutzer-Accounts und die häufigen Änderungen führen dazu, dass die meisten Menschen Probleme haben, sich ihre Passwörter zu merken. Die Folge:

- Menschen benutzen Passwörter, die einfach zu knacken sind (z. B. den Vornamen der Ehefrau)
- Viele nutzen das gleiche Passwort für mehrere Anwendungen
- 50 % der Menschen schreiben ihre Passwörter auf
- Mehr als $\frac{1}{3}$ der Nutzer verraten ihre Passwörter einem Kollegen oder Freund
- 47 % lassen ihr Passwort mindestens einmal im Jahr zurücksetzen

Passwort-Knacker machen sich ein Hobby daraus, mit immer raffinierterer Software den Zugang zu unerlaubten Daten zu erschleichen. Namen von Menschen oder Haustieren gehören genauso zu den leicht knackbaren Wörtern wie z. B. Zufallswörter aus dem Duden. Sicher sind nur so genannte starke Passwörter.

Ein starkes Passwort ist

- 8 bis 10 Zeichen lang
- besteht aus Kleinbuchstaben und Grossbuchstaben
- Sonderzeichen und Zahlen sowie
- Umlauten und Leerzeichen

Ein Beispiel gefällig? **Do=61emeJF** würde wohl den Sicherheitsansprüchen der Experten genügen

Das Passwortdilemma ist nicht ganz so prekär, wie es sich präsentiert. Starke Passwörter, an die man sich auch erinnern kann, können zum Beispiel generiert werden, indem man sich die Anfangsbuchstaben eines Satzes merkt. Ausserdem gibt es Internetdienstleister wie Passwordsitter, Passwort Vault oder Passwortdepot, die sich anbieten, unsere zahlreichen Passwörter sicher abzulegen, ohne dass wir uns ständig an sie erinnern müssen.

Was ist zu tun? Wir alle haben unzählige Passwörter und PIN-Nummern, die wir uns merken müssen. Selbstverständlich verbietet es sich, diese Zugangs-Codes aufzuschreiben und wir sollten für jeden Service ein spezielles Passwort kreieren.

Mit anderen Worten: Es wird von uns erwartet, dass wir uns 20 verschiedene Passwörter wie **Do=61emeJF** merken können und am Schluss auch noch wissen, zu welchem Portal der Schlüssel gehört.

Diese Regeln befolgen natürlich die wenigsten von uns. Aktuelle Studien zeigen, dass fast die Hälfte aller User nur ein Passwort benutzt, um den Zugang zu verschiedensten Diensten zu gewährleisten. Weitaus der grösste Teil dieser Wörter sind nicht stark genug, um dem Angriff eines Passwort-Knackers zu widerstehen.

Der einzige Haken: Ein sicheres Master-Passwort, um den Zugang zu gewährleisten, ist natürlich notwendig. Da dahinter alle anderen Passwörter versteckt sind, können wir nur hoffen, dass wir es nie vergessen! Was für Privatnutzer lästig ist, kann Unternehmen richtig Geld kosten. Experten schätzen, dass Passwort-Probleme 30-50 Prozent der Helpdesk-Kosten in einem Unternehmen verursachen.

Eine professionelle, sichere Lösung mit Single Sign On Passwort für den Benutzer drängt sich hier förmlich auf. **achermann** consulting ag berät sie gerne in solchen professionellen Lösungen.