Axel Hesse

freiberuflicher Dozent für Informatik

Freistraße 12
06295 Lutherstadt Eisleben
Tel.: 0 34 75 – 68 12 12
Mobil: 0151-40071749
E-Mail: ax-hesse@t-online.de
Web: www.ax-hesse.de

Das perfekte Passwort?

Gibt es das **perfekte Passwort?** Ein klares „**Jein“!** Aufgrund der anhaltenden rasanten Entwicklung der Technik kann auch ein perfektes Passwort theoretisch in absehbarer Zeit geknackt werden. Man sollte es einem Hacker oder Angreifer trotzdem durch die Verwendung eines starken Passwortes so schwer wie möglich machen an die begehrten Daten zu kommen – nicht nur im privaten Umfeld sondern auch in Ihrem Unternehmen.

Gestaltung eines starken Passwortes

Selbstkontrolle bzw. Selbstschutz ist der erste Schritt! Darum geben wir hier ein paar Tipps zur Gestaltung eines sicheren Passwortes. Die Gestaltung des Passwortes richtet sich dabei grundsätzlich hinsichtlich der Komplexität und Länge auch nach der **Art der zu schützenden Daten**. Man sollte jedoch Folgendes dabei beachten:

- Die Zusammensetzung des Passwortes sollte so komplex sein, dass es nicht leicht erraten werden kann.
- Das Passwort sollte jedoch auch nicht so kompliziert sein, damit der Nutzer sich dieses mit vertretbarem Aufwand merken

Axel Hesse

freiberuflicher Dozent für Informatik

Freistraße 12
06295 Lutherstadt Eisleben
Tel.: 0 34 75 – 68 12 12
Mobil: 0151-40071749
E-Mail: ax-hesse@t-online.de
Web: www.ax-hesse.de

Mindestanforderungen an ein starkes Passwort

Grundsätzlich sollten folgende Aspekte, die auch vom Bundesamt für Sicherheit der Informationstechnik (BSI) als **Mindeststandard** angesehen werden, bei der Gestaltung eines Passwortes berücksichtigt werden:

- Mindestens 8 Zeichen, wobei sich die Länge nach dem Schutzbedarf der Daten richten sollte;
- Kombination aus Groß-, Kleinbuchstaben, Sonderzeichen und Ziffern (3 von 4 Kriterien sollten erfüllt sein; technische Umsetzung am Idealsten);
- Keine Verwendung von Trivialpasswörtern, die leicht zu erraten sind; bspw. fortlaufende Ziffern, Name des Haustieres, Geburtsdatum, oder einer Kombination dieser;
- Keine Fortlaufenden Passwörter, bspw. Kennwort1, Kennwort 2.

Es sollte beachtet werden: Je einfacher das Passwort gewählt ist, umso schneller kann dieses geknackt werden!

- Bei einem aus **5 Zeichen** (3 Kleinbuchstaben, 2 Zahlen) bestehenden Passwort kann durch automatisches Ausprobieren aller Kombinationen innerhalb von **0,03 Sekunden** einen Treffer bedeuten.
- Bei einem Passwort bestehend aus **9 Zeichen** (bestehend aus 2 Großbuchstaben, 3 Kleinbuchstaben, 2 Zahlen, 2 Sonderzeichen) benötigt das System ca. **9 Jahre** bis es geknackt ist. In der Zwischenzeit hat man hoffentlich das Passwort gewechselt.

zu allen anderen Passwörtern. Ansonsten sollte davon abgesehen werden, das Passwort niederzuschreiben.

Quelle: https://www.datenschutzbeauftragter-info.de/