Inhalt

Sicherer Einsatz von Passwörtern - Einführung

In unserer digitalen Welt ist der Schutz unserer persönlichen Daten wichtiger denn je. Passwörter sind eine der häufigsten Methoden, um unsere Konten und Informationen zu sichern. Leider sind sie oft auch das schwächste Glied in der Datensicherheitskette.

Wie in so vielen Bereichen gilt auch in der Unternehmens-IT: Die Technik kann nur so gut sein, wie der Mensch, der sie benutzt. Für Angreifer bedeutet dies: Der Bediener eines IT-Systems ist grundsätzlich ein leicht zu überwindendes Hindernis, weil auf die menschliche Schwäche Verlass ist. Dies beginnt eben bereits mit der Vergabe von Passwörtern. Das Hasso Plattner-Institut (HPI) veröffentlicht jedes Jahr die Top 10 der beliebtesten deutschen Passwörter.

Dauerbrenner unter den Top 3 sind dabei seit Jahren die Zahlenkombinationen „12345789“, „12345678“ oder schlicht das Wort „hallo“. Leichter kann man es einem Cyberangreifer nun wirklich nicht machen. Dies gilt vor allem dann, wenn man das Passwort gleich für mehrere – oder am besten für alle Zugänge zu IT-Systemen im Unternehmen nutzt.

Grundsätze sicherer Passwörter

Und deshalb ist es wichtig, sich bei der Vergabe von Passwörtern an die folgenden Grundsätze zu halten.

Länge und Komplexität

Ein sicheres Passwort sollte mindestens zwölf Zeichen lang sein. Denn es gilt die einfache Regel: Je länger das Passwort, desto schwieriger ist es für Angreifer, es zu knacken. Diese verwenden in der Regel die so genannte Brute-Force-Methode, einen kryptografischen Hack-Algorithmus, der darauf beruht, alle möglichen Kombinationen zu testen, bis die richtige entdeckt wird. IT-Experten haben einmal berechnet, wie lange so ein Algorithmus benötigt um unterschiedliche Passwörter zu knacken.

Die Ergebnisse sind in der nachfolgenden Tabelle zusammengefasst:

	Passwort mit acht Zeichen	**Passwort mit zehn Zeichen**	**Passwort mit zwölf Zeichen**
Nur Kleinbuchstaben	0,19 Millisekunden	ca. 10 Sekunden	mehrere Wochen
+ 1 Großbuchstabe	30 Minuten	Ein Monat	Fünf Jahre
+ 1 Nummer	Eine Stunde	Sechs Jahre	2000 Jahre
+ 1 Sonderzeichen	Ein Tag	50 Jahre	63000 Jahre

Vermeidung von gängigen Mustern und Wörtern

Womit wir bei den Lieblingspasswörtern der Deutschen wären. Die Länge allein nützt nur wenig, wenn Sie einfache Muster wie "123456" oder "abcdef" verwenden. Sie sollten darüber hinaus keine leicht zu erratenden Informationen wie Geburtsdaten oder Namen von Familienmitgliedern verwenden.

Verwendung von Sonderzeichen, Zahlen und Groß-/Kleinbuchstaben

Ein gutes Passwort sollte also aus einer Kombination aus verschiedenen Zeichenarten bestehen. So ist beispielsweise "P@ssw0rd!23" sicherer als "password123".