Sicherheit durch Passwörter

Informationen und Daten sind für Kriminelle und Spione bares Geld wert – sie betreiben einen großen Aufwand, um Sicherheitslücken in Software aufzuspüren.

Ob dienstlich oder privat beim Online-Banking oder für ein soziales Netzwerk – für viele Anwendungen müssen Sie ein Passwort vergeben, denn es schützt die Daten und hinterlegten Inhalte. Entwenden oder entschlüsseln Kriminelle ein Passwort, hat das Konsequenzen:

Daten können gestohlen, manipuliert oder gelöscht werden. Im schlimmsten Fall stiehlt jemand sogar Ihre Identität. Cyberkriminelle und Spione sind deshalb sehr daran interessiert, an Passwörter und die damit geschützten Inhalte zu gelangen.

Schützen und sichern Sie die Informationen und die Daten Ihres Betriebes, indem Sie komplexe Passwörter vergeben.

Passwörter - Speicherung

Systeme verschlüsseln Passwörter nach der Eingabe und legen sie so ab, das Kriminelle sie nicht auslesen können.
Diese Verschlüsselung funktioniert nur in eine Richtung – aus dem Schlüssel kann man das Passwort nicht „zurückrechnen“. Fremde können daher nur durch Ausprobieren an ein Zugangspasswort gelangen.

Manchmal betreiben sie aber auch eine Vorabrecherche:
Denn der Name, das Geburtsdatum oder das Autokennzeichen könnten im Passwort enthalten sein.

Bei ungezielten Angriffen probieren Hacker zunächst nicht geänderte, standardisierte Zugangsdaten, Wörter, die im Wörterbuch stehen, und häufige Ersetzungen mit Sonderzeichen aus. Erst danach testen sie Zufallskombinationen (Brute Force Angriff) – wie bei einem Zahlenschloss, bei dem man die Nummer vergessen hat. Je komplexer also ein Passwort ist, desto mehr Möglichkeiten müssen die Angreifer testen

Passwortlänge	Zeit (maximal)
4 Zeichen	5 Millisekunden
6 Zeichen	39 Sekunden
8 Zeichen	3 Tage
10 Zeichen	61 Jahre

Gute Passwörter

Greifen Sie für ein Passwort auf alle Möglichkeiten der Tastatur zurück:
Allein mit Klein- und Großbuchstaben gibt es 52 Möglichkeiten für jede Stelle eines Passworts; zusammen mit Zahlen und Sonderzeichen sind es über 80.

Das bedeutet, dass Sie mit jedem zusätzlichen Zeichen den Aufwand für Hacker erhöhen, um das Passwort zu knacken.

Vergeben Sie für jedes Portal ein anderes Passwort und verwenden Sie für jedes Portal ein anderes Passwort und verwenden Sie privat keine dienstlichen Unternehmens-Passwörter.

Beachten Sie bitte stets Folgendes:

- Ihre Passwörter sollten mindestens acht Stellen haben.
- Nutzen Sie Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen
- Bilden Sie keine sinnvollen Wörter/Sätze und verwenden Sie keine persönlichen Angaben.
- Ändern Sie Ihre Passwörter regelmäßig.
- Trennen Sie dienstliche und private Passwörter. Merken Sie sich Ihre Passwörter und legen Sie diese nirgendwo ab.
- Geben Sie Ihre Passwörter nicht weiter – weder an Vorgesetzte noch an Kollegen.

Bilden Sie Passwortsätze

Ein Passwortsatz hilft Ihnen, sich ein komplexes Passwort einfach zu merken. Bilden Sie hierfür einen Satz – etwa aus einem Gedicht oder zu einer persönlichen schönen Erinnerung. Beispiel:

Mein sicherer Passwortsatz aus 12 Buchstaben, Sonderzeichen und Zahlen!

Von diesem Satz nehmen Sie die Anfangsbuchstaben, Satzzeichen und vorhandenen Zahlen. **MsPa12B,SuZ!**

Falls es komplexer sein soll, ersetzen Sie die Buchstaben durch Zahlen oder Sonderzeichen, die ihnen optisch ähneln (E durch 3, a durch @, B durch 8, …). **MsP@128,SuZ!**

Für unterschiedliche Dienste können Sie deren Anfangsbuchstaben noch an einer beliebigen Stelle in den Satz einbauen: zum Beispiel für die Anmeldung bei Windows „Wi“.
MsP@Wi128,SuZ!

Ihrer Kreativität sind dabei keine Grenzen gesetzt.

Was ist bei Gefährdung oder Verdacht zu tun ?

Wenn Sie glauben, dass mit Ihrem Passwort unberechtigt auf Informationen und Daten zugegriffen worden sein könnte, oder Sie gehackt worden sein könnten: informieren Sie unseren Sicherheitsbereich wir helfen Ihnen

per E-Mail an:
Sicherheit@IT-Concepts.net
oder rufen Sie an unter:
Tel. **0531 - 38728521**

Ansprechpersonen bei der
IT-Sicherheit

Florian Thurmann
IT-Sicherheitsbeauftragter
Telefon: **0531 - 38728521**

E-Mail: Sicherheit@IT-Concepts.net

Herausgeber:
IT-Concepts.net
Am Horstbleek 53, 38116 Braunschweig

Fotos: Vlad Kochelaevskiy
Bild-Nr: 106484327
Quelle: Shutterstock

Stand: 01/2019

IT – Concepts.net

Leistung & höchste Qualität
sind unsere Stärke

Sichere Passwörter vergeben

IT-Sicherheit informiert