

CSBW

CYBER
SICHERHEITS
AGENTUR
BADEN-WÜRTTEMBERG

Sichere Passwörter

So wie der Schlüssel das Zuhause vor ungebetenen Gästen schützt, so schützen Passwörter unsere Accounts. Komplexe und lange Passwörter bieten einen besseren Schutz vor unberechtigten Zugriffen. Wichtig ist dabei aber auch, die Passwörter niemandem mitzuteilen und für jeden Account ein eigenes Passwort zu benutzen.

Je länger
und komplexer ein
Passwort ist, umso
schwieriger ist es
zu knacken



Die gängigsten Angriffs-Methoden:

Brute Force

Bei dieser Methode werden alle möglichen Zeichenkombinationen nacheinander ausprobiert, bis das richtige Passwort gefunden wurde. Es wird buchstäblich „rohe Gewalt“ angewendet.

Dictionary Attack

Bei diesem Angriff werden Begriffe aus Wörterbüchern einzeln oder kombiniert verwendet. Ergänzt mit persönlichen Daten (Name, Geburtsdatum etc.) führt ein solcher Angriff häufig sehr schnell zum Erfolg.

Social Engineering

Das Opfer wird durch Manipulation und vorgegaukelte Fakten dazu gebracht, das eigene Passwort preiszugeben. Oft kommen dabei sogenannte Phishing-E-Mails zum Einsatz.

So erstellen Sie ein sicheres Passwort:

- ▶ Verwenden Sie keine persönlichen Daten, weder von Ihnen noch von Verwandten oder Haustieren.
- ▶ Verwenden Sie keine Muster wie *asdfgh*, *123456*, *qwertzu* etc. Wählen Sie stattdessen eine willkürliche Mischung aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen.
- ▶ Kreieren Sie Ihr Passwort z.B. aus den Anfangsbuchstaben eines Satzes. Beispiel:
CSBW: Prävention ist der beste Schutz gegen Cyberangriffe!
Entspricht: **CSBW:PidbSgC!**
Zusätzlich Buchstaben durch Sonderzeichen oder Zahlen ersetzen z.B. S=\$, B=8:
Ihr Passwort: **C\$8W:Pidb\$gC!**
- ▶ Nutzen Sie für Ihr Passwort am besten 12 Zeichen oder mehr.

Wie können Sie sich nun all die komplexen Passwörter merken?

Ganz einfach: Nutzen Sie einen Passwort-Manager!

- ▶ Ein Passwort-Manager unterstützt Sie bei der Verwaltung Ihrer Passwörter.
- ▶ Sie tragen dort Ihre Passwörter ein und müssen sich nur noch ein komplexes Passwort merken: Ihr Hauptpasswort, auch „Master-Passwort“ genannt.
- ▶ Der Passwort-Manager kann auch komplexe und sichere Passwörter nach Ihren gewünschten Kriterien (z.B. Länge, Zeichen etc.) erstellen.
- ▶ Die Daten müssen Sie bei einem Login nicht selbst eintippen, da der Passwort-Manager diese für Sie eintragen kann (Auto-Type).
- ▶ Damit Sie Ihre bereits genutzten Passwörter im Blick behalten, verfügt der Passwort-Manager über eine Passwort-Historie.

Auf einen Blick!

Warum Ihr Passwort durch viele verschiedene Zeichen sicherer wird.

Je länger das Passwort ist und je mehr unterschiedliche Zeichen verwendet werden, desto länger benötigt ein Computer, um alle möglichen Zeichenkombinationen auszuprobieren. Ihr Passwort wird somit immer sicherer!

Hier am Beispiel eines Brute-Force-Angriffs:

		Im Passwort verwendete Zeichen				
		0-9	a-z	a-z A-Z	0-9 a-z A-Z	0-9 a-z A-Z Sonderzeichen
Anzahl Zeichen	4	Sofort	Sofort	Sofort	Sofort	Sofort
	5	Sofort	Sofort	Sofort	Sofort	Sofort
	6	Sofort	Sofort	Sofort	1 sek	5 sek
	7	Sofort	Sofort	25 sek	1 min	6 min
	8	Sofort	5 sek	22 min	1 h	8 h
	9	Sofort	2 min	19 h	3 Tage	3 Wochen
	10	Sofort	58 min	1 Monat	7 Monate	5 Jahre
	11	2 sek	1 Tag	5 Jahre	41 Jahre	400 Jahre
	12	25 sek	3 Wochen	300 Jahre	2.000 Jahre	34.000 Jahre
	13	4 min	1 Jahr	16.000 Jahre	100.000 Jahre	2 Mio. Jahre
	14	41 min	51 Jahre	800.000 Jahre	9 Mio. Jahre	200 Mio. Jahre
	15	6 h	1.000 Jahre	43 Mio. Jahre	600 Mio. Jahre	15 Mrd. Jahre

Daten zusammengetragen von: <https://www.security.org/how-secure-is-my-password/>