ALLGEIER CyRis

10 Tipps

für sichere Passwörter

Das Haustier, der Name des Partners oder simple Zahlenfolgen: Bei der Wahl von Passwörtern herrscht oftmals Nachlässigkeit. Die Auswirkungen vom Passwort-Diebstahl sind jedoch vielfältig – gerade für Unternehmen. Sie reichen vom unrechtmäßigen Abschluss von Verträgen über die illegale Nutzung von E-Mail-Programmen, Messaging-Diensten oder sozialen Netzwerken bis hin zur Durchführung von Online-Banküberweisungen.

1 Um sich Passwörter leicht merken zu können, setzt ein Großteil der Belegschaft auf einfache Lösungen. Am sichersten sind jedoch Passwörter mit Zahlen und Sonderzeichen sowie mit Groß- und Kleinschreibung. Optimale Länge: mindestens acht Zeichen, besser mehr.

2 Oft werden für unterschiedliche Plattformen dieselben Zugangsdaten verwendet. Dies hat zur Folge, dass sich Cyberkriminelle mit der Erbeutung Zugang zu unterschiedlichen Systemen, Anwendungen etc. verschaffen können. Daher sollten stets verschiedene Passwörter erstellt werden.

3 Ein absolutes No-Go: die Post-its. Oftmals werden Passwörter auf Zetteln notiert und ungeschützt im Büro liegen gelassen. Dies stellt ein erhebliches Sicherheitsrisiko dar.

4 Vom regelmäßigen Ändern von Passwörtern raten Experten zunehmend ab. Der Grund: Die Aufforderung, Passwörter laufend zu ändern, verleitet dazu, Systematiken zu verwenden, die einem simplen Schema folgen: Start1, Start2, Start3 etc.

5 In Unternehmen werden Passwörter oft per E-Mail oder im Chat versendet. Auch das sollte unbedingt vermieden werden, denn es ist nicht auszuschließen, dass sich Externe hierauf Zugriff verschaffen und Passwörter leicht abgreifen können.

6 Mit Passwortmanagern können Zugangsdaten generiert und zentral in Datenbanken verschlüsselt abgelegt werden. Um Zugriff auf das jeweilige Nutzerkonto zu erhalten, bedarf es eines Hauptpasswortes, das besonders zu schützen ist.

7 Zur Reduktion von Passwörtern benötigt nicht jeder Mitarbeiter Zugriffsrechte auf alle Unternehmensanwendungen. Entsprechend sollten Zugriffsrechte je nach individuellen Tätigkeiten verteilt sein.

8 Die Zwei-Faktor-Authentifizierung basiert auf der doppelten Absicherung von Zugangsdaten. Sie bietet sich vor allem bei besonders schützenswerten Informationen an, also beispielsweise auch zur zusätzlichen Absicherung eines Hauptpasswortes für einen Passwortmanager.

9 Für Unternehmen empfiehlt sich ein Regelkatalog, der den Umgang mit Passwörtern vorgibt. Die Inhalte sollten in regelmäßigen Abständen thematisiert werden.

10 Die Kenntnisse der Belegschaft sollten ständig überprüft und laufend aktualisiert werden. Hier helfen Awareness Schulungen: Sie vermitteln in kurzen Einheiten das notwendige Wissen.

Für mehr Informationen und aktuelle Themen besuchen Sie unsere Website, den Allgeier-Blog und folgen Sie uns bei LinkedIn.

Allgeier CyRis GmbH | Hans-Bredow-Straße 60 | 28307 Bremen | Telefon: +49 421 43841 0 | info@allgeier-cyris.de | www.allgeier-cyris.de