Computacenter

# SENSIBILISIERUNG FÜR INFORMATIONSSICHERHEIT – UMGANG MIT INFORMATIONEN

## Passwörter

# PASSWÖRTER

## Einführung

**‘Passwörter’**

In diesem Abschnitt erfährst Du, was ein sicheres Passwort ausmacht. Darüber hinaus lernst Du, wie Du ein starkes Passwort erstellst und es sicher speicherst.

Passwörter sind persönliche und geheime digitale Schlüssel. Mit ihnen sichern wir Computer, Netzwerke, digitale Benutzerkonten und vieles mehr.

Daher sind gute Passwörter und deren sichere Verwahrung für uns besonders wichtig.


Jeder Computacenter-Mitarbeiter erhält ein persönliches Zugriffskonto mitsamt den zugehörigen Berechtigungen, die erforderlich sind, um seine beruflichen Aufgaben zu erfüllen.

Jeder Mitarbeiter ist für die eigenen Anmeldeinformationen verantwortlich. Aus diesem Grund werden Deine Konten durch Kennwörter geschützt, die selbst Dein Administrator nicht kennt.

Jeder, der Zugriff auf deine Anmeldeinformationen hat, hat auch die Möglichkeit, in Deinem Namen Schaden anzurichten. Wenn jemand Schaden anrichtet und dabei deine Anmeldedaten verwendet, könnte es sein, dass Du ebenfalls zur Rechenschaft gezogen wirst.

# Szenarien


Das sicherste Passwort in diesem Fall ist „!Mh@ll?iFwW@5.."

Idealerweise werden bei einem sicheren Passwort alle der folgenden Zeichen zufällig miteinander kombiniert:

- Großbuchstaben
- Kleinbuchstaben
- Ziffern
- Sonderzeichen.

Im Allgemeinen sollte es...

- … so lang wie möglich sein (mindestens 8 Zeichen).
- … nicht in einem Wörterbuch zu finden sein.
- … nicht aus einer Reihe zusammenhängender

Zeichen bestehen, so wie sie auf der Tastatur nebeneinander liegen.

# Fachberatung

Wie erstellt man also ein starkes Passwort?

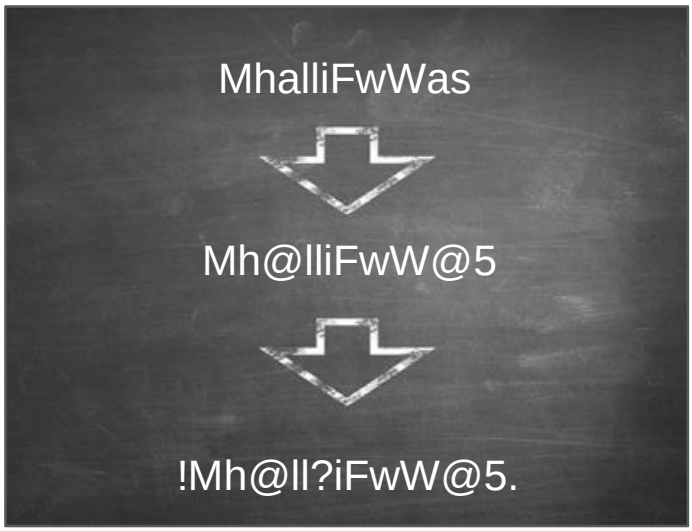
Experten empfehlen Folgendes: Schreibe einen beliebigen Satz auf, nehme dann die Anfangsbuchstaben von jedem der Wörter, mache aus einigen von ihnen Großbuchstaben und mische sie mit Ziffern und Sonderzeichen.


Zeilen aus deinen Lieblingssong oder -gedicht oder Sätze, die Du dir selbst ausgedacht hast, eignen sich hierfür besonders gut, weil Du Dir sie sehr einfach merken kannst. Nehmen wir einmal diese Zeile aus einem bekannten Kinderlied: „Mary had a

little lamb, its Fleece was White as snow.“

Wenn wir nur die ersten Buchstaben jedes Wortes betrachten, ergeben diese ein „sinnloses“ Wort.

Dieses Wort allein ist aber noch nicht besonders sicher. Uns fehlen noch Ziffern und Sonderzeichen.




Wir könnten in unserem Beispiel „s“ durch „5“ und „e“ durch „€“ ersetzen. Das lässt sich gut merken.

Jetzt ergänzen wir noch am Anfang ein „!“, in der Mitte ein „?“ und am Ende einen „.“

Damit haben wir ein ziemlich gutes Passwort kreiert.

Wichtig ist jedoch immer, dass Du Dir eine eigene Geheimschrift ausdenkst oder ein eigenes Muster zurechtlegst, mit dem Du Deine Passwörter erstellst.

## Speichern Sie Ihre Passwörter

Computacenter stellt seinen Nutzern KeePass zur Verfügung. Dies ist ein genehmigtes, verschlüsseltes Tool zur Verwaltung von Passwörtern und die einzige zulässige Möglichkeit für Nutzer, ihre Kennwörter zu speichern.

## Biometrische Authentifizierung

Die biometrische Authentifizierung, beispielsweise per Fingerabdruck oder Gesichts- bzw. Spracherkennung, ist eine genehmigte alternative Authentifizierungsmethode. Falls Geräte und Software es erlauben, kann sie deshalb ersatzweise anstatt von Passwörtern oder PINs eingesetzt werden.

Bei Computacenter wird die biometrische Authentifizierung genutzt für

- Mobilgeräte
- Zugangskontrolle für einige Standorte

## Kennwörter von privilegierten Konten (Admin)

Zusätzlich zu den Standardbenutzerkonten erhalten einige Mitarbeiter privilegierte Administratorkonten, die es ihnen erlauben, ihre beruflichen Aufgaben (z. B. in der Entwicklung oder in der Verwaltung und Überwachung von IT-Systemen, -Services oder -Lösungen) zu erledigen.

Privilegierte Konten dürfen nur für die Funktionen genutzt werden, die in Zusammenhang mit Deiner beruflichen Position stehen und nicht mit dem Standardbenutzerkonto erledigt werden können. Dies bedeutet, dass es nicht verwendet werden darf, um damit Routineaufgaben, wie z. B. Zugriff auf Internet oder E-Mails, zu erledigen.

Denke daran, dass für die Passwortverwaltung dieser privilegierten Konten (Admin) innerhalb Deiner Abteilung zusätzliche Vorschriften gelten könnten, siehe Informationssicherheitsrichtlinien für bestimmte Rollen & Aufgaben.

# Zusammenfassung

In diesem Abschnitt hast Du Folgendes gelernt:

- Kennwörter sind digitale Schlüssel und Du musst Deinen Zugriff auf Unternehmensnetzwerk durch Dein eigenes Passwort schützen.
- Es gibt Vorschriften für die Erstellung eines sicheren Passworts.
- Du musst Dein Passwort sicher aufbewahren.
- Die biometrische Authentifizierung ist eine zulässige alternative Anmeldemethode, vorausgesetzt Geräte und Software lassen es zu
- Es könnten für die Passwortverwaltung von privilegierten Konten (Admin) innerhalb Deiner Abteilung zusätzliche Vorschriften gelten

**Datenschutzverletzungen und Informationssicherheitsvorfälle:**

Solltest Du den Verdacht haben, dass Dein Passwort in die falschen Hände geraten sein könnte oder dass sich jemand anderes bei deinem Konto angemeldet hat, musst Du umgehend einen Informationssicherheitsvorfall über das NGSD melden.