Richtlinie

Passwörter und Zugangsdaten

# Hinweise zu Passwörtern

## Passwörter spielen in den Konzepten der Datensicherheit nach wie vor eine zentrale Rolle und dienen der Legitimation der Benutzer. Oftmals werden Passwörter zusammen mit dem Benutzernamen als einziges Authentifizierungsmerkmal verwendet. Der Zugang zu bestimmten Informationen oder Rechnerressourcen wird ebenso über Passwörter reguliert wird wie der Zugriff auf ganze Netze.

## Mit Passwörtern geschützte Ressourcen haben dabei höchst unterschiedliche Sicherheitsanforderungen. Wer etwa ein Passwort zur Teilnahme an einem Web Forum benötigt, muss hieran nicht dieselben Anforderungen stellen wie an ein Passwort für einen ins Firmennetz integrierten Rechner mit weitreichenden Zugriffsrechten.

## In den letzten Jahren sehen sich PC-Nutzer in ihrem beruflichen und auch privaten Umfeld einer ständig steigenden Flut an passwortgeschützten Diensten und Bereichen ausgesetzt. Neben dem Rechner-Passwort werden weitere Passwörter etwa für E-Mail-Postfächer, für Verschlüsselungstools oder den Zugriff auf geschützte Netzwerkressourcen benötigt. Auch bei der Nutzung von Internet-Diensten (Online-Shops, Online-Banking etc.) werden oftmals Passwörter zur Authentifizierung des Anwenders genutzt. Viele Nutzer neigen daher dazu, durch Vereinfachungsstrategien dieser Passwort-Flut besser zu begegnen.

## Dies darf jedoch keinesfalls dazu führen, dass für sicherheitssensitive Bereiche im Unternehmen solche Passwörter verwendet werden, die aufgrund fehlender Komplexität oder zu einfacher Gestaltung keinen ausreichenden Schutz bieten.

## Grundsätzlich muss bei der Passwortwahl ein Kompromiss zwischen zwei Anforderungen gefunden werden. Zum einen muss das Passwort möglichst lang und komplex sein, damit es ausreichend Sicherheit bietet, auf der anderen Seite muss es handhabbar bzw. praktikabel bleiben, etwa indem es sich leicht auswendig lernen lässt.

# Handlungsanweisungen

## Je sensitiver die zu schützenden Ressourcen, desto größer müssen die Anforderungen an die Sicherheit der Passwörter sein. Um höheren Sicherheitsansprüchen zu genügen, sollte ein Passwort aus mindestens acht Zeichen bestehen. Je länger das Passwort, desto schwerer ist es zu knacken. Neben Buchstaben und Ziffern sollten im Passwort auch Sonderzeichen verwendet werden. Bei den Buchstaben sollten in jedem Fall Groß- und Kleinbuchstaben benutzt werden.

## Auf keinen Fall dürfen dabei Namen oder sonstige reale Wörter aus welchen Sprachen auch immer verwendet werden, da diese zu leicht zu erraten sind und bei ernsthaften Angriffen stets zuerst ausprobiert werden. Auch nebeneinanderliegende Tasten (qwertz, yxcvb) bieten keinerlei Sicherheit.

## Begriffe oder Namen aus dem persönlichen Umfeld des Nutzers sollten in keinem Fall verwendet werden, auch nicht in abgewandelter Form, etwa indem diese Namen durch vor- oder nachgestellte Zahlen erweitert werden (etwa Julia87, 31\_Klaus).

## Um sich komplexe Passwörter besser zu merken, kann man auf bestimmte Eselsbrücken, zurückgreifen. So kann man z.B. Passwörter aus Gedichtzeilen, Liedtexten oder Buchtiteln herleiten, indem man zunächst die Anfangsbuchstaben hintereinander notiert und diese dann zusätzlich noch durch weitere Maßnahmen verfremdet. Ausgehend von WrssdNuW? (Wer reitet so spät durch Nacht und Wind?) könnte man z.B. bestimmte Buchstaben durch Ziffern ersetzen (etwa alle Vokale in ihrer Reihenfolge durch 1,2, 3 etc., was hier dann zum Passwort WrssdN1W? führt. Es sind aber auch beliebige andere Variationen möglich (Weglassen von Vokalen, Versetzen der Buchstaben um eine Stelle im Alphabet etc.). Anstelle eines komplizierten Passworts muss man sich hier nur noch die Konstruktionsregel merken, was wesentlich leichter sein dürfte.

## Ein und dasselbe Passwort sollte nicht für unterschiedliche Einsatzbereiche verwendet werden. So angenehm es ist, sich nur ein Passwort merken zu müssen, so groß sind hier die Missbrauchsmöglichkeiten, wenn dieses Passwort in die falschen Hände gerät.

## Passwörter dürfen in keinem Fall an unberechtigte Dritte weitergegeben werden. Um den Zugriff auf wichtige Bereiche oder Ressourcen anderen Berechtigten zu ermöglichen, können die Passwörter an sicherer Stelle hinterlegt werden.

## Eine schriftliche Fixierung der Passwörter ist nach Möglichkeit zu vermeiden. Sollte sich dies als nicht praktikabel erweisen, sollten die Passwörter in jedem Fall an einem sicheren Ort verwahrt und niemals öffentlich zugänglich sein. Besteht der Verdacht, dass unberechtigte Personen ein Passwort in Erfahrung gebracht haben könnten, ist dieses unverzüglich zu ändern bzw. bei den jeweiligen Administratoren ein neues Passwort anzufordern.

## Passwörter sollten regelmäßig gewechselt werden. Je sensitiver die hierüber geschützten Daten sind, desto kürzer sollte die Nutzungsdauer eines Passworts sein.

# Tipps für die Bildung von Passwörtern!

## Verwenden Sie Zeichen aus den folgenden drei Gruppen:

* Buchstaben, z. B. A, B, C... und a, b, c...,
* numerische Zeichen, z. B. 0, 1, 2, 3, 4, 5, 6, 7, 8, 9,
* Symbole (alle Zeichen außer Buchstaben und numerische Zeichen), z. B. !§$%&/()

## Benutzen Sie nur Passwörter, die aus mindestens 6 Zeichen bestehen.

## Ändern Sie Ihr Passwort regelmäßig (Tasten Strg + Alt + Entf). Bei Verdacht auf Missbrauch informieren Sie unverzüglich Ihren Fachvorgesetzten oder die IT-Abteilung.

## Halten Sie Ihr Passwort geheim. Geben Sie das Passwort nicht an Kollegen oder an Administratoren weiter.

## Schreiben Sie Ihr Passwort nicht auf einen Zettel, den Sie im Büro unverschlossen aufbewahren.

## Geben Sie Ihr Passwort auch nicht telefonisch an Personen weiter, die sich als Administratoren oder Vorgesetzte ausgeben.

## Speichern Sie Ihr Passwort nicht auf programmierbaren Funktionstasten oder in einer Datei auf dem PC.

## Vermeiden Sie Passwörter, die leicht "ausgespäht" werden können: Namen von Ortschaften (Muenchen2005, HAMBURG), Geburtsdaten (10011958), Auto- und Telefonnummern (FR-AA123, 0761123456). Namen von Familienangehörigen, Freund(inn)en und Haustieren, (z. B.: Linda, Peter, Hasso)

## Passwortgenerationen, wie michael01, michael02 usw., bieten ebenfalls nicht den nötigen Schutz.

# Bestätigung

Mit der Unterschrift bestätigen Sie, dass Sie sämtliche Regelungen verstanden haben und sich an die hier beschriebenen Ausführungen halten werden. Rückfragen wurden umfassend beantwortet.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Ort, Datum leserliche Unterschrift