Passwortvergabe, -wahl und -verwaltung

Die verwendeten Benutzerkennungen bestehen in der Regel aus Namen oder Namensteilen der Mitarbeiter und sind damit allen anderen Beschäftigten bekannt. Umso wichtiger ist es deshalb, dass die zu den Benutzerkennungen gehörenden Passwörter nur dem Berechtigten bekannt sind, anderen Personen gegenüber geheim gehalten werden und nicht leicht zu erraten sind. Daher müssen Kennwörter gewisse Anforderungen erfüllen.

So sollten auf **keinen Fall** Trivialpasswörter oder Passwörter verwendet werden, die einen Bezug zum Besitzer aufweisen (z. B. Namen, Geburtsdatum oder Telefonnummern). Stattdessen sollten Passwörter verwendet werden, die nicht einfach zu erraten sind.

Zusätzlich sollten zur Erhöhung der Sicherheit **Ziffern und Sonderzeichen** eingestreut werden. Solche komplizierten Passworte lassen sich natürlich nur durch häufige Benutzung merken. Deshalb sollte sich jeder Anwender nach jedem Passwortwechsel mehrmals hintereinander anmelden, um sich so das Kennwort besser einprägen zu können.

Natürlich **muss** jedes **Passwort auch in regelmäßigen Zeitabständen geändert werden**. Der Anwender sollte sein Passwort regelmäßig (z. B. nach 90 Tagen) ändern.

Bei der Vergabe und bei der Verwendung von Passworten sollten insbesondere folgende Sicherheitsgrundsätze beachtet werden:

Passwortaufbau (für Anwender)

Ein Passwort soll

- mindestens acht Zeichen lang sein
- nicht nur Buchstaben beinhalten sondern aus Groß- und Kleinbuchstaben, Sonderzeichen (Satzzeichen u. ä.) und Zahlen bestehen
- möglichst kein Wort sein, das im Duden oder in einem anderen Wörterbuch aufgeführt ist
- nicht aus einem Trivialpasswort bestehen (z. B. Namen von Prominenten, Passwort)
- nicht aus Zeichen aufgebaut sein, die auf der Tastatur nebeneinander liegen (z. B. 123456)
- nicht das gleiche Zeichen mehrfach hintereinander enthalten (z. B. AAAA)
- keinen Bezug zum Benutzer erkennen lassen (z. B. nicht Benutzerkennung, Name, Geburtsdatum, Kraftfahrzeugkennzeichen, usw.)

Passwörter dürfen auch nicht auf Zetteln notiert und keiner anderen Person (auch nicht dem Vorgesetzten oder dem Systemverwalter) mitgeteilt werden.

Passwortvergabe und – verwendung (für EDV-Abteilungen)

- Zu jeder Benutzerkennung muss ein eigenes Passwort gehören.
- Die Passwortvergabe muss durch den Benutzer selbst erfolgen.
- Das Passwort darf nur dem Benutzer bekannt sein.
- Die Passworteingabe sollte verdeckt erfolgen.
- Voreingestellte Passwörter (z. B. im System- und Anwendungsbereich) sind sofort zu ändern.
- Das eingesetzte Betriebssystem bzw. die Anwendungssoftware sollte über die Möglichkeit verfügen, Regeln für den Passwortaufbau, die Passwortvergabe und -verwendung sowie die Passwortverwaltung zu erstellen und deren Einhaltung sicherzustellen.

- Ein Initialpasswort darf nur zur Erstanmeldung berechtigen.
- Sofort nach der Erstanmeldung sollte ein Passwortwechsel maschinell erzwungen werden.

Passwortverwaltung (für EDV-Abteilungen)

- Passwörter sollten maschinell einwegverschlüsselt im System hinterlegt werden.
- Das neue Passwort sollte zur Sicherheit ein zweites Mal eingegeben werden.
- Das Passwort muss durch Benutzer jederzeit selbst geändert werden können.
- Besteht der Verdacht, dass das Passwort einer anderen Person bekannt wurde, ist es unverzüglich zu ändern.
- Eine regelmäßige Passwortänderung sollte nach ca. 90 Tagen systemtechnisch erzwungen werden.
- In besonders sensiblen oder besonders gefährdeten Bereichen sollte - soweit nicht Einmal-Passwörter verwendet werden - der Passwortwechsel ggfs. häufiger erzwungen werden.
- Die Mindestlebensdauer eines Passwortes sollte einen Tag betragen.
- Die letzte Passwortänderung sollte dem Benutzer mit Datum und Uhrzeit angezeigt werden.
- Eine Passworthistorie ist systemtechnisch zu führen.
- Passworte dürfen nicht auf Funktionstasten gelegt bzw. in einem Makro gespeichert werden.
- Passworte dürfen nicht auf Zetteln notiert und keiner anderen Person (auch nicht dem Vorgesetzten oder dem Systemverwalter) mitgeteilt werden.

Sonstiges (für EDV-Abteilungen)

- Die Anzahl an aufeinander folgenden Fehlversuchen ist systemtechnisch zu begrenzen.
- Nach mehrfachen erfolglosen Anmeldeversuchen sollte eine systemtechnische Sperrung der Benutzerkennung und/oder des Endgerätes erfolgen.
- Eine Entsperrung darf nur durch berechtigte Personen (z. B. Systemverwalter) möglich sein.
- Alle erfolglosen Anmeldeversuche sind zu protokollieren und auszuwerten
- Systempasswörter und wichtige Kennungen sind in versiegeltem Umschlag zugriffssicher zu hinterlegen.
- Passwörter sind in vernetzten Systemen verschlüsselt zu übertragen.
- Die Benutzer sind über die Modalitäten zur Passwortauswahl und –vergabe zu informieren.