Hinweise zum Umgang mit Passwörtern

Werden personenbezogene Daten mit Hilfe von Computern verarbeitet, so ist sicherzustellen, dass nur berechtigte Personen darauf zugreifen können und dies auch nur im dienstlich notwendigen Umfang. Notwendig ist daher, dass sich derjenige, der auf personenbezogene Daten zugreifen will, zunächst gegenüber dem Computersystem identifiziert und seine Zugriffsberechtigung nachweist. Dies geschieht in der Regel durch Eingabe einer Benutzerkennung und eines Passwortes.

Erfährt jemand die Benutzerkennung und das Passwort einer anderen Person, so kann er sich damit unter fremdem Namen anmelden und auf Daten und Programme zugreifen, die nicht für ihn bestimmt sind. Da Benutzerkennungen vielfach nicht geheim sind, kommt der Geheimhaltung der persönlichen Passwörter die entscheidende Rolle zu, wenn es darum geht, den Zugriff unberechtigter Personen auf personenbezogene Daten zu verhindern.

Folgende Regeln sollten daher beachtet werden, um die Sicherheit der Passwörter zu wahren:

1. ***Es sind individuelle Kennungen und Passwörter zu verwenden.***

   Jeder Benutzer erhält eine eigene Benutzerkennung und ein eigenes Passwort, das nur von ihm benutzt werden darf. Passwörter, die von mehreren Personen benutzt werden (Gruppenpasswörter) sind zu vermeiden, denn sie lassen sich nicht in gleicher Weise geheim halten wie individuelle Passwörter. Ferner lässt eine Gruppenkennung, die beispielsweise in Protokollen sicherheitsrelevanter Ereignisse erscheint, keinen eindeutigen Rückschluss auf den Verursacher zu.

2. ***Ein Passwort muss geheim gehalten werden. Es darf nirgendwo aufgeschrieben und keiner anderen Person - auch nicht dem Systemverwalter oder dem dienstlichen Stellvertreter - mitgeteilt werden.***

   Ansonsten könnten Systemverwalter oder Stellvertreter beispielsweise unter fremder Kennung Daten verändern, wobei das Protokoll der Datenänderung den Inhaber der persönlichen Kennung als Urheber der Änderung ausweist. Ebenso könnten unter fremdem Namen E-Mails versandt werden, die beim Empfänger den Eindruck hinterlassen, sie seien von dem Inhaber der persönlichen Kennung versandt worden.

   Eine Ausnahme gilt lediglich für betriebswichtige Passwörter wie Administrator-Passwörter; diese können in einem verschlossenen Umschlag in einem Tresor aufbewahrt werden.

3. ***Triviale Passwörter sind zu vermeiden.***

   Dazu zählen etwa Namen oder Vornamen, die Benutzerkennung, das Geburtsdatum, das Kfz-Kennzeichen, die Telefonnummer oder andere Angaben aus dem persönlichen Umfeld des Benutzers, die auch anderen Personen bekannt sein können. Solche Passwörter sind leicht zu erraten.

4. ***Ein Passwort sollte aus mindestens acht Zeichen bestehen. Innerhalb des Passworts sollte mindestens ein Sonderzeichen (wie z.B. ?, #, !) enthalten sein. Es sollte sowohl Groß- als auch Kleinbuchstaben sowie Ziffern enthalten.***

   Dadurch wird es erschwert, Passwörter durch Ausprobieren herauszufinden. Um sich ein solches Passwort trotzdem merken zu können, kann es beispielsweise von einem Merksatz abgeleitet werden. So kann man sich etwa anhand des Satzes "**S**ichere **P**asswörter **s**ollten **m**indestens **a**us **8 Z**eichen **b**estehen**!**" das Passwort **SPsma8Zb!** merken.

5. ***Hat ein Systemverwalter einem Benutzer ein neues Passwort eingerichtet, so muss der Benutzer dieses Start-Passwort bei seiner ersten Anmeldung ändern.***

   Um möglichst schnell zu erreichen, dass das mit der Benutzerkennung verbundene Passwort nur dem Benutzer bekannt ist, sollte diese erste Anmeldung umgehend nach Einrichtung des Start-Passworts erfolgen.

6. ***Ein Passwort ist regelmäßig zu ändern.***
   Das neue Passwort sollte sich von den früher verwendeten unterscheiden.

   Dies verhindert, dass derjenige, dem ein fremdes Passwort bekannt wurde, dieses zu späteren Zeitpunkten wiederholt für unberechtigte Zugriffe nutzen kann. Um sicherzustellen, dass die Änderung tatsächlich erfolgt, sollte ein automatischer Verfall der Passwörter realisiert werden. Um den Ausschluss früher verwendeter Passwörter zu gewährleisten, sollte der Computer zumindest jeweils die letzten fünf früheren Passwörter in einer sog. Passwort-Historie speichern und deren Wiederverwendung ablehnen.

7. ***Ein Passwort muss umgehend geändert werden, wenn der Verdacht besteht, dass es einer anderen Person bekannt wurde.***

8. ***Passwort-Änderungen müssen von den jeweiligen Benutzern selbst durchgeführt werden können.***

9. ***Nach mehreren fehlerhaften Anmeldeversuchen unter derselben Benutzerkennung muss die Kennung für die weitere Benutzung gesperrt* werden.**

   Diese Sperre ist erforderlich, um ein systematisches Durchprobieren aller möglichen Passwörter zu verhindern (sog. Brute-Force-Attacken). Die Sperre sollte nach drei bis fünf Fehlversuchen greifen und so lange bestehen bleiben, bis sie von einem Systemverwalter aufgehoben wird.

10. ***Anmeldefehlversuche sind zu protokollieren.***

    Erfolglose Anmeldeversuche können auf einen Eindringversuch hinweisen. Die entsprechenden Protokolle sind regelmäßig auf sicherheitsrelevante Vorkommnisse hin zu überprüfen. Nach Möglichkeit sollten mehrfach hintereinander auftretende Anmeldefehlversuche unter einer Benutzerkennung

einen Alarm beim Systembetreuer auslösen (z. B in Form einer E-Mail).

11. ***Alle Passwörter von System- oder Anwendungssoftware, die vom Hersteller voreingestellt wurden, sind nach der Installation des Systems umgehend zu ändern.***

    Da die Hersteller oft die gleichen Passwörter bei der Auslieferung ihrer Produkte voreinstellen, sind diese einem großen Personenkreis bekannt. Zudem sind die entsprechenden Kennungen vielfach mit umfassenden Berechtigungen verbunden. Deshalb sind die Passwörter umgehend zu ändern.