Sicherheitsregeln im Umgang mit Daten

Vergabe sicherer Passwörter

Ein gutes Passwort sollte mindestens 10 Zeichen lang sein und aus Buchstaben, Ziffern und Sonderzeichen bestehen. Um sich dennoch eine ganze Reihe unterschiedlicher Passwörter merken zu können, kann man zum Beispiel ein Grundpasswort verwenden und mit einem Schema erweitern, das von dem verwendeten Dienst abhängt. Das Grundpasswort sollte in keiner Beziehung zu dem Benutzer stehen. Da es bei jedem Login eingegeben wird, kann kann man sich auch ein kompliziertes Passwort merken.
Das Grundpasswort sollte aus einer zufälligen Reihe unterschiedlicher Zeichen bestehen, z. B.:

.p4K-7,Mn5

Vermeiden sollte man Anführungszeichen und das kaufmännische Und (&), weil diese Zeichen manchmal nicht zulässig sind. Man kann sich auch eine Eselsbrücke bauen. Beispielsweise das Kinderlied „**E**s **t**anzt **ein** **B**i-**B**a-Butzemann in unserm Haus herum“ könnte zu dem folgenden Gerüst führen:
Et1B-b!@28 (! Wäre der Butzemann, @ zu Hause und 28 die eigene Hausnummer)
Dieses Grundpasswort kann man dann um einen dienstabhängigen Teil ergänzen, z. B. für den privaten bzw. beruflichen E-Mail-Account:

.p4K-7,EMailPrMn5 bzw. **.p4K-7,EMailBerMn5**

1. Erstelle ein Passwortschema und zwei Beispiele für mögliche Passwörter.

   Beispiel: 2p3gF.5-D=2 (Merkhilfe: „Zwei plus Drei gleich Fünf. Fünf minus Drei gleich Zwei“)

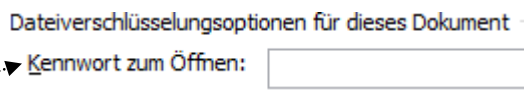
   *2p3gF**In**.**Me**5-D=2 Für den **In**stand **Me**ssaging Dienst*

   Ein Passwortschema ist allemal besser als dasselbe Kennwort mehrfach zu verwenden. Wenn ein Krimineller aber ein oder mehrere Kennwörter in die Finger bekommt, kann er das Schema erraten. Besser ist es, rein zufällige Kennwörter zu verwenden, die man sich aber unmöglich merken kann.

2. Im Augenblick kannst du dir eventuell noch alle Accounts bei Internetdiensten merken, die du nutzt. Das wird sich aber im Laufe deines Lebens ändern: Recht schnell wirst du den Überblick verlieren und kannst unmöglich alle Dienste im Kopf behalten, bei denen du Datenspuren hinterlässt.
   Diese Daten verwaltest du aber bestimmt **nicht** in den Kontakten deines Smartphones, denn darauf gewährst du diversen Apps Zugriff. Für den Anfang kannst du das natürlich handschriftlich erledigen. Besser ist es aber, die Möglichkeiten zu nutzen, die eine elektronische Verwaltung bietet, indem du neue Daten hinzufügen und überflüssige Daten löschen kannst.
   - Erstelle im Textverarbeitungsprogramm eine Tabelle, in der du Zugangsdaten verwalten kannst. Sollte durch eine Zwei-Faktor-Authentifizierung z. B, noch eine PIN erforderlich sein, solltest du dir diese merken bzw. getrennt aufbewahren.

Beschreibung	Internetadresse	Benutzername	Kennwort	Sonstiges
Name des Dienstes	www.meindienst.de	E-Mail	.p4K-7,Mn5	Zertifikatsdatei: zert15-19.pfx

   - Auch Dokumente können ganz einfach verschlüsselt gespeichert werden, indem ein Kennwort eingegeben wird, das den oben beschriebenen Standards entspricht.
     Dieses Kennwort musst du dir natürlich merken!
     In MS Word 2010 findest du das im Menü:
     Speichern unter -> Tools -> Allgemeine Optionen...



   Nicht eindeutig zu beantworten ist die Frage, ob man dieses Dokument auch ausdruckt.
   Hier sollte man entscheiden, wie zuverlässig man ein Dokument vor fremdem Zugriff aufbewahren kann – mit dem Personalausweis, Führerschein oder Kreditkarte wirst du dich ohnehin irgendwann dahingehend organisieren müssen.
   - Eine weitere Alternative ist die Verwendung eines Passwortmanagers. Informiere dich zu diesem Thema, wäge die Vor- und Nachteile der Methoden zur Organisation sicherer Passwörter ab, die du jetzt kennengelernt hast, und triff eine Entscheidung, wie du in Zukunft vorgehen möchtest.

Checkliste

3. Arbeite das Kapitel Lerninhalte 04 nochmals durch und ergänze die Checkliste für Sicherheitsregeln im Umgang mit Daten.
   - **Automatische Updates** für das Betriebssystem und Anwendungsprogramme aktivieren.
   - Wo dies nicht möglich ist, ***regelmäßig auf Updates prüfen***.
     – nicht nur den PC und das Smartphone: Bei allen netzwerkfähigen Geräten (z. B. WLAN-Router, Smart-TV und Streaming-Clients für Video oder Audio) besteht ein Angriffspotential für Kriminelle.
   - **Antivirenprogramme** verhindern, dass infizierte Dateien gespeichert oder ausgeführt werden – zuverlässig aber nur bekannte Schadprogramme. Insbesondere das Virenschutzprogramm muss

     also stets aktuell sein.
   - *Nicht (mehr) benötigte Software deinstallieren.*
   - *Aktivieren der **Dateinamenerweiterungen**.*
   - ***Nie** eine Datei bzw. den Dateianhang einer E-Mail **öffnen**,*

     wenn die Herkunft nicht ganz sicher ist.

     Vergewissere dich im Zweifelsfall bei dem angegebenen Absender.
   - *Automatisches Ausführen von Makros*

     in Anwendungsprogrammen deaktivieren.
   - *Überprüfe regelmäßig die Auslastung der CPU*

     sowie die Netzwerk- und Festplattenaktivitäten.
   - *Achte im Internet auf eine sichere*

     ***Verschlüsselung der Kommunikation**.*
   - *In unverschlüsselten WLANs*

     keine personenbezogenen Daten senden.
   - *Sichere **Passwörter** verwenden*

     – und für jeden Dienst ein anderes.
   - *Wenn möglich, verwende*

     mehrfach abgesicherte Login-Verfahren
   - *Regelmäßige **Backups** anfertigen.*
   - *Werden **Datenträger** entsorgt oder verkauft,*

     *vorher mechanisch zerstören oder **sicher löschen**.*

- Überlege mit dem Anfertigen eines Backups nicht hin- und her, sondern tue es – und das regelmäßig! Dann kannst du immer noch weiter überlegen, welche Form des Backups du weiterhin wählst.
- Das wirksamste Mittel gegen Missbrauch von Daten ist **Datensparsamkeit**: Nicht existierende Daten können auch nicht missbraucht werden. Überlege also gut, **ob** und **welche** Daten du **wo** hinterlässt.
- Nach einem Softwareupdate oder dem Hinzufügen neuer Funktionalitäten kann es vorkommen, dass die **Datenschutzeinstellungen** zurückgesetzt bzw. so vorkonfiguriert sind, dass möglichst viele Daten abgeschöpft werden können. Kontrolliere also auch die Datenschutzeinstellungen im Betriebssystem, in den Anwendungsprogrammen und bei Internetdiensten regelmäßig.