10/3.3 Passwort-Manager

Passwortsicherheit

Die Vielzahl an Passwörtern, die sich ein Anwender merken muss, und die erforderliche Komplexität der Passwörter bereiten vielen Computernutzern Schwierigkeiten. Deshalb werden Passwörter notiert, nicht stark genug gewählt und für viele Applikationen und Benutzerkonten gleichzeitig genutzt. Abhilfe kann ein Passwort-Manager schaffen, wenn er richtig ausgewählt und eingesetzt wird. Der Datenschutzbeauftragte sollte deshalb den Einsatz von Passwort-Managern prüfen.

10/3.3.1 Passwortsicherheit und Passwort-Manager

Passwörter merken oder sicher speichern

Ob am Bildschirmrand, unter der Tastatur oder in der Schublade, an vielen Arbeitsplätzen findet man Notizzettel mit Passwörtern. Ein klarer Hinweis darauf, dass es vielen Computernutzer schwerfällt, sich Passwörter in ausreichender Anzahl und Qualität zu merken.

Auch wenn man das Notieren von Passwörtern nicht gutheißen kann, lassen sich dennoch nachvollziehbare Gründe dafür finden. Verschiedene Sicherheitsstudien zeigen, dass die Mehrzahl der Mitarbeiter für über 20 verschiedene Anwendungen jeweils ein Passwort benötigt, zum Beispiel für den Netzwerkzugang, für den lokalen Arbeitsplatzrechner, für das E-Mail-Konto, für den FTP-Zugang (File Transfer) sowie für zahlreiche Online-Dienste.

Häufige Passwort-Probleme

Da dies die Gedächtnisleistung schnell überfordern kann, sind die Folgen absehbar:

- Fast 40 Prozent der Mitarbeiter merken sich ihr Passwort nicht, sondern speichern es im Browser oder als Textdatei auf dem Rechner, oder sie halten es als Notiz auf einem Zettel vor.

- Weniger als jeder Fünfte vergibt für jeden Zugang ein anderes Passwort.
- Fast die Hälfte der Mitarbeiter sucht Passwörter so aus, dass sie leicht zu merken sind.
- Fast 20 Prozent der Mitarbeiter nutzen den Namen ihres Haustiers oder ihr Geburtsdatum als Passwort.
- Volle fünf Prozent der Mitarbeiter wählen das Standard-Passwort „123456“.
- Mehr als die Hälfte aller Mitarbeiter ändern die Passwörter nur sehr selten.
- Fast die Hälfte der Mitarbeiter geben ihre Passwörter an andere Personen weiter.

Passwort-Manager könnte Abhilfe schaffen

Besser als eine ungeschützte digitale Passwort-Liste auf dem Computer-Desktop oder eine ausgedruckte Passwort-Liste in der Schublade erscheint ein professioneller **Passwort-Manager**, also eine Softwarelösung, die die Passwörter speichern und verwalten kann und dabei die Passwortliste verschlüsselt vorhält.

Allerdings sind Passwort-Manager nicht unumstritten. Während die Anhänger der Passwort-Manager argumentieren, nur so könnten starke Passwörter trotz Vergesslichkeit durchgesetzt werden, verweisen die Gegner auf die Gefahr, dass nicht nur der Verlust des Passworts für den Passwort-Manager (des sogenannten **Master-Passworts**) den Verlust aller Passwörter bedeutet, sondern dass auch das Master-Passwort in den Händen Unbefugter einen Generalschlüssel für alle Systeme darstellt.

Damit der Datenschutzbeauftragte den Einsatz eines Passwort-Managers prüfen kann, sollte er die grundsätzlichen Funktionen und Einschränkungen einer solchen Softwarelösung kennen.

10/3.3.2 Funktionen eines Passwort-Managers

Verschlüsselte Passwortliste

Die wesentliche Funktion eines Passwort-Managers besteht darin, eine verschlüsselte Passwortliste oder Passwortdatenbank anzubieten. Für die Entschlüsselung wird das Master-Passwort benötigt. Damit die Zuordnung der Passwörter in der Liste oder Datenbank zu den Anwendungen erleichtert wird, bieten Passwort-Manager in der Regel eine Kategorisierung für die Passwörter (zum Beispiel E-Mail oder Online-Banking).

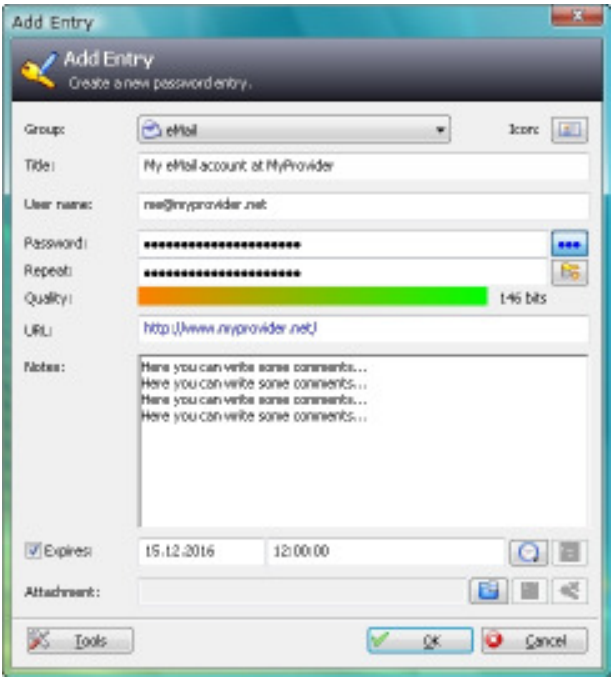

Abbildung 10/3.3-1: Passwort-Manager bieten meist eine Gruppierung der gespeicherten Passwörter an (Beispiel: KeePass)

Verschlüsselungsstandard entscheidend

Wegen der hohen Bedeutung der Passwörter für die Datensicherheit sollte nur ein Passwort-Manager zum Einsatz kommen, der einen hohen Verschlüsselungsstandard wie AES (Advanced Encryption Standard) 256 Bit nutzt.

Login über den Passwort-Manager

Gerade für Benutzerzugänge von Online-Diensten ist es nützlich, wenn das Login über eine Funktion des Passwort-Managers erfolgt, das Passwort also sicher zur Login-Seite des Online-Dienstes übertragen wird und nicht abgetippt werden muss. Dadurch lassen sich zum Beispiel mögliche Keylogger umgehen. Hierfür bieten verschiedene Passwort-Manager auch eine Funktion „virtuelle Tastatur“ an.

Unterstützung bei der Passwortwahl

Allein durch eine sichere Speicherung werden Passwörter jedoch nicht besser, also stärker und komplexer. Deshalb bieten mehrere Passwort-Manager auf dem Markt auch eine integrierte Funktion zur Passwortgenerierung an (siehe Abbildung 10/3.3-2).

Importfunktion für Passwörter

Falls bereits an anderer Stelle Passwörter gespeichert wurden, können viele der Passwort-Manager auch einen Import zur Verfügung stellen, sodass eine zentrale Sammlung der Passwörter möglich wird.

Backup auch für Passwortlisten

Damit die Passwörter nicht Opfer eines Datenverlusts werden, sollte auch die Passwortdatenbank regelmäßig gesichert werden. Verschiedene Lösungen im Bereich Passwort-Manager haben dafür eine eigene Backup-Funktion.

Mobile Variante des Passwort-Managers

Nicht nur für Außendienstmitarbeiter können die mobilen Varianten eines Passwort-Managers hilfreich sein, bei denen die Passwortdatenbank verschlüsselt auf einem USB-Stick liegt. Dadurch ist keine Installation des Passwort-Managers auf dem lokalen Rechner erforderlich. Allerdings sollte auch hier das regelmäßige Backup nicht vergessen werden, da USB-Sticks leicht verloren gehen können. Zudem gibt es auch mobile Passwort-Manager, die sich auf einem Smartphone oder PDA betreiben lassen.

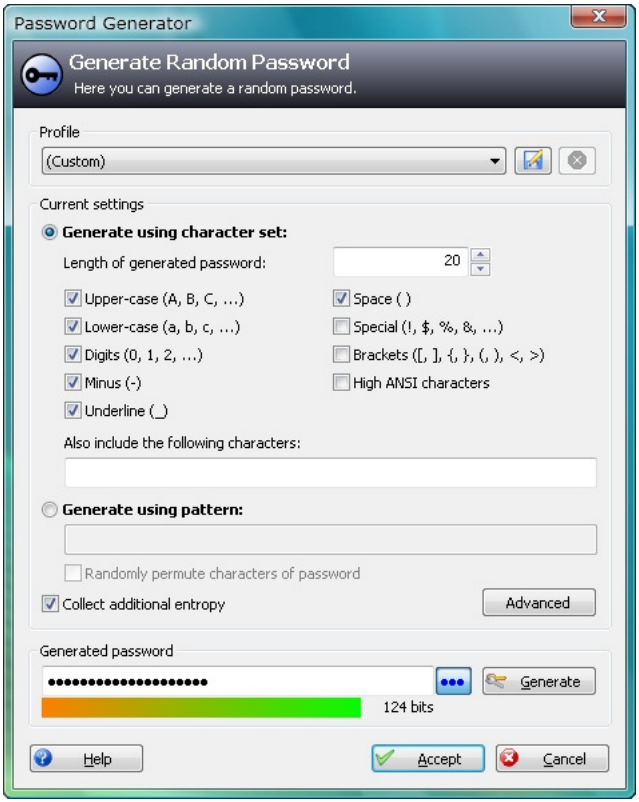

Abbildung 10/3.3-2: Einige Passwort-Manager unterstützen bei der Passwort-Wahl durch einen integrierten Passwortgenerator (Beispiel: KeePass)

Kriterienkatalog für die Auswahl eines Passwort-Managers

Der Datenschutzbeauftragte sollte die Auswahl und den möglichen Einsatz eines Passwort-Managers begleiten und dabei folgende Anforderungen mit dem Einkauf oder der IT-Leitung besprechen.

Anforderung	Erfüllt	Nicht erfüllt
Hoher Verschlüsselungsstandard	☐	☐
Gruppierung für Passwörter	☐	☐
Integrierter Passwortgenerator	☐	☐
Import externer Passwortlisten	☐	☐
Integrierte Backup-Funktion	☐	☐
Optional: Mobile Version	☐	☐

Tabelle 10/3.3-1: Anforderungen an einen neuen Passwort-Manager

10/3.3.3 Praxishinweise zu Passwort-Managern

Passwort-Manager ja, aber ...

Wenn man als Datenschutzbeauftragter nun gefragt wird, ob man einen Passwort-Manager einsetzen solle oder nicht, sollte man zuerst darauf hinweisen, dass es gute Methoden gibt, sich starke Passwörter zu überlegen, die man sich auch merken kann.

Ein Passwort-Manager ist also keine Pflicht und in vielen Unternehmen sogar verboten. Aber unter bestimmten Voraussetzungen kann ein Passwort-Manager eine sinnvolle Maßnahme der Datensicherheit sein.

Hohe Anforderungen an einen Passwort-Manager

Nicht jeder Passwort-Manager verdient seinen Namen, ganz gleich, ob kostenloses Open-Source-Produkt oder kommerzielle Lösung. Eine zentral vorgehaltene Passwortliste ist besonders gefährdet und stellt ein besonders lohnendes Angriffsziel für Datendiebe dar. Wird das Master-Passwort geknackt, stehen alle Zugänge genauso offen wie beim Missbrauch des Hauptschlüssels einer Schließanlage. Passwort-Manager müssen deshalb selbst umfassend geschützt und die Passwortlisten durchgehend stark verschlüsselt werden.

Auch der Passwort-Manager muss geschützt werden

Eine ganz wesentliche Schutzmaßnahme für den Passwort-Manager wird in der Praxis meist vergessen. Denn wer den Mitarbeitern einen Passwort-Manager geben will, da sie sich keine starken Passwörter merken, sollte damit auch beim Passwort-Manager selbst rechnen, der ohne entsprechende Passwort-Prüfung mit einem zu schwachen Master-Passwort versehen werden könnte.

Abbildung 10/3.3-3: Passwort-Manager werden dann zum Datenrisiko, wenn das Master-Passwort selbst nicht ausreichend stark gewählt ist. Einige Passwort-Manager helfen bei der Prüfung der Passwortstärke für das Master-Passwort (Beispiel: KeePass)

Passwort-Manager sollten also immer nur dann eingesetzt werden, wenn sich das Master-Passwort absichern lässt, am besten über eine **Zwei-Faktor-Authentifizierung**. Zum Master-Passwort gehört dann noch ein Hardware-Token oder eine Chip-Karte.

Passwort-Manager bietet nur eingeschränkte Hilfe

Zudem sollte klar sein: **Gegen eine unsichere Verwendung von Passwörtern, wie das Hereinfallen auf Phishing-Mails oder das Abfangen von Passwörtern bei der unverschlüsselten Übertragung ins Internet, helfen einfache Passwort-Manager nicht.** Deshalb dürfen Anti-Phishing-Funktionen, SSL-Verschlüsselung und Anti-Malware-Software auf keinen Fall fehlen, auch wenn professionelle Passwort-Manager zum Einsatz kommen.

10/3.3.4 Prüfansätze für den Datenschutzbeauftragten

Für den sicheren Einsatz eines Passwort-Managers werden folgende Hinweise gegeben. Im Idealfall sollten alle Fragen mit „Ja“ beantwortet werden können.

Prüfansätze	Ja	Nein
Nutzt der Passwort-Manager selbst ein Verschlüsselungsverfahren nach dem Stand der Technik?	☐	☐
Werden die im Passwort-Manager gespeicherten Passwörter nicht ungeschützt in der Zwischenablage belassen, wenn der Anwender ein Passwort aus dem Passwort-Manager kopiert, um es in eine Anwendung zu übernehmen?	☐	☐
Ist der Passwort-Manager gegen Brute-Force-Attacken (Ausprobieren einer hohen Anzahl von Passwörtern) geschützt, bricht er also nach einer geringen Zahl von Fehlversuchen für das Master-Passwort ab?	☐	☐
Unterstützt der Passwort-Manager bei der Erzeugung sicherer Passwörter?	☐	☐
Prüft der Passwort-Manager auch die Stärke importierter Passwörter?	☐	☐
Lassen sich die gespeicherten Passwörter innerhalb des Passwort-Managers nach Anwendungen sortieren?	☐	☐
Ist der Passwort-Manager einfach zu bedienen, um gefährliche Bedienungsfehler zu vermeiden?	☐	☐
Bietet der Passwort-Manager einen Schutz gegen Keylogger (zum Beispiel eine virtuelle Tastatur)?	☐	☐
Werden sichere Backups von dem Passwort-Manager gemacht, damit nicht durch Verlust der Passwort-Datenbank alle gespeicherten Passwörter verloren gehen?	☐	☐
Lässt sich der Passwort-Manager mit einer Zwei-Faktor-Authentifizierung kombinieren, um die Abhängigkeit vom Master-Passwort zu senken?	☐	☐