

Passwörter

Erstellen – Verwalten - Sichern

1. Wo sind Passwörter zwingend
2. Die häufigsten Passwort-Fehler
3. Erstellung sicherer Passwörter
4. Verwaltungsprogramme
5. Passwörter speichern
6. Sichtbarmachung der Sternchen
7. Passwörter aushebeln
8. Das Windows-Passwort

1. Wo sind Passwörter zwingend ?

Für alle Konten auf Internetseiten ist ein Passwort zwingend erforderlich.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt, **keinesfalls ein Einheitspasswort** zu verwenden, die Passwortlänge sollte mindestens 8 Zeichen, für den WLAN-Schutz WPA/ WPA2 sogar 20 Zeichen betragen.

Die Zeichen sollten sich aus einer **Mischung von Gross- und Kleinbuchstaben, Ziffern und Sonderzeichen** zusammensetzen.

Begriffe aus Wörterbüchern, Namen von Familienangehörigen oder Tieren sind **ungeeignet**.

Auf ein Windows-Anmeldekennwort kann u.U. als Alleinnutzer verzichtet werden. Auf Rechnern, die von mehreren Personen genutzt werden, sollte ein BIOS-Passwort eingerichtet werden.

2. Die häufigsten Passwort-Fehler

Das Passwort ist **zu kurz** – ein Passwort aus 6 Kleinbuchstaben ist mit der Brute-Force-Methode in 10s geknackt, bei 8 Zeichen aus groß und klein in ca. 2 Monaten.

Das Passwort ist **zu einfach** – Worte aus Wörterbüchern, Namen, Geburtstage, systematische Ziffern- oder Zeichenfolgen (123456 oder abcdef u.ä.) sind unbrauchbar.

Speichern oder **Aufschreiben** – ein einigermaßen sicheres Passwort lässt sich kaum merken.

Jahrelang **das gleiche** Passwort – regelmäßige Änderung des Passwortes.

Ein und dasselbe Passwort für alles – für jeden Zugang ein anderes Passwort benutzen.

Quelle: PC-Welt 3/10

3. Erstellung sicherer Passwörter

Wenn alle vorgenannten Bedingungen eingehalten werden sollen steht man vor einem Problem.

Entweder ich generiere ein sicheres Passwort, das ich mir nicht merken kann oder ein merkbare aber dann unsicheres.

Wer könnte sich z.B. das folgende mit 25 Zeichen merken ?

1.=FdhdGg2.=gswH3.=swddJh

Die Generierung basiert auf einer Anregung aus der PC-Welt 6/11 – es sind die Anfangsbuchstaben der ersten drei Textzeilen eines bekannten Kinderliedes. Textsicherheit und Zeichenabfolge ist dafür Voraussetzung.

Für dieses Verfahren gibt es sicherlich viele Varianten.

Und um welches Lied handelt es sich ?

4. Verwaltungsprogramme

Will man sich die Merkkapazität für andere wichtige Dinge aufsparen helfen nur Verwaltungsprogramme.

Diese Programme beinhalten häufig auch Generierungsfunktionen für Passwörter, die lassen sich aber auf gar keinen Fall mehr merken.

Zu **empfehlen** ist dabei eine sogenannte **Portable-Version**, die sich auf einem Stick ohne Installation unterbringen lässt.

1-abc.net Password Organizer

Password-Safe

KeePass bzw. **KeePassPortable**

Lastpass

Password Depot

Sticky Password

Die meisten dieser Verwaltungsprogramme gleichen sich funktionell.

Es handelt sich um Datenbanken.

Jeder Eintrag entspricht einem Datensatz.

Erfasst werden u.a. Benutzername, Passwort, Internetadresse, Beschreibungen und Kommentare, Serverdaten ...

Die hochwertigeren Programme enthalten einen Passwortgenerator.

Einstellbar sind die Passwortlänge und die benutzten Zeichenarten (auch Sonderzeichen).

Manche Programme zeigen die Verschlüsselungstiefe an.

Alle Datenbanken sind durch ein Master-Passwort geschützt.

5. Passwörter speichern

Firefox und auch der MS-Internet-Explorer bieten die Möglichkeit Passwörter zu speichern.

Auch Outlook und Outlook-Express bieten für die Passwörter der E-Mail-Konten diese Möglichkeit an.

Die Entscheidung für eine Speicherung ist sehr sorgfältig abzuwägen, das hängt auch vom Speicherort ab, lokal also auf dem eigenen Rechner oder auf dem Server im Netz.

Am sichersten ist es von einer Speicherung abzusehen.

Benutzt man ein portables Verwaltungsprogramm auf einem Stick geschieht die Speicherung ohnehin auf diesem und ist nur bei einem Verlust des Sticks problematisch.

6. Sichtbarmachung der Sternchen

Um die meist als Punkte oder Sternchen dargestellten Passwörter real sichtbar zu machen gibt es eine Reihe von Hilfsprogrammen. Die Benutzung beschränkt sich aus Rechtsgründen auf die Arbeit mit **eigenen Dokumenten**.

Ob sich die Zeichen real darstellen lassen hängt vom Verschlüsselungsverfahren ab und der Speicherung auf dem lokalen Rechner.

Bei der Benutzung eines Verwaltungsprogramms erübrigt sich ein derartiges Programm. Damit ist man auch rechtlich auf der sicheren Seite. Die Verwaltungsprogramme erlauben die Ein- oder Ausblendung der Verschlüsselung.

Kopieren des Passworts ist nur bei eingeblendeter Darstellung möglich, ausser das Programm bietet die Möglichkeit an.

7. Passwörter aushebeln

Rechtlich ebenfalls eingeschränkt ist die Benutzung von Programmen zum Knacken von Passwörtern. Sie beschränkt sich **ausschliesslich** auf mittels Passwort geschützter **eigener Dateien**.

Viele Programme bieten einen Passwortschutz an, so z.B. die Komponenten von MS-Office, diverse Backup-Programme, Komprimierungsprogramme u. a.

MS-Excel bietet auch das Schützen der Arbeitsblätter und der Arbeitsmappe an.

Für jede Anwendung ist in der Regel ein anderes Hilfsprogramm notwendig.

8. Das Windows-Passwort

Das Windows-Passwort schützt ein Benutzerkonto und freigegebene Netzwerkressourcen vor unberechtigtem Zugriff.

Das Anlegen und Einrichten von Benutzerkonten und die Netzwerkkonfiguration erfordern Administratorrechte.

Für das Windows-Passwort lassen sich umfangreiche Sicherheitsregeln festlegen.

Zur Sicherheit lässt sich ein Passwort-Rücksetz-Datenträger anlegen (auch für eingeschränkte Konten möglich).

Eigene Netzwerk-Kennwörter können verwaltet werden.

Über den Befehl „Ausführen“ und der Eingabe **control userpasswords2** lassen sich weitere Passwort-Optionen einstellen.

Quellen

Bundesamt für Sicherheit in der Informationstechnik (BSI)

PC-Welt Jahrgänge 2010 und 2011

Internet www.softwareload.de

Internet www.microsoft.de