Passwortschutz

Passwortqualität

Die Erstellung eines guten Passwortes ist nicht einfach. Einerseits soll ein Passwort gut merkbar, **andererseits darf es nicht zu offensichtlich** sein. Komplizierte Passwörter, welche man sich aufschreiben muss, sind ungeeignet. **Passwörter die in eine persönliche Verbindung mit dem Anwender gebracht werden können sind genauso schlecht.** Sie sind viel zu leicht zu erraten oder durch Ausprobieren zu knacken. **Vielmehr ist die Länge der Passwortes ein entscheidendes Sicherheitsmerkmal.**

Gelegenheit macht Diebe

Noch vor wenigen Jahren galt: Besteht das Passwort nur aus sechs (6) zufälligen Zeichen, dauert das Knacken der Wortes mit geeigneten „Knackprogrammen" 1,5 Tage (!). Die Verwendung von acht (8) zufälligen Zeichen dauert dagegen schon 25 (!) Jahre. Heute geht das alles noch viel schneller, vorausgesetzt, man hat dazu die „erforderliche" kriminelle Energie und ein entsprechend ausgereiftes Programm. Eine absolute Passwortsicherheit gibt es nicht!

Gute Passwörter erkennt man also daran, dass sie mehr als sechs Zeichen haben. Optimal sind 8 oder mehr Zeichen *(Buchstaben, Zahlen, Sonderzeichen)*. Gedankenbrücken erleichtern das Behalten des Passwortes. Je „wertvoller" der Inhalt einer Datei ist, umso mehr Zeichen sollte das Passwort haben.

Regel beim Umgang mit Passwörtern

- Passwort nicht weitergeben.
- Passwort regelmäßig wechseln.
- Passwort nicht notieren.
- Passwörter nie ohne geeignete Verschlüsselung speichern oder weitergeben.
- Passwort bei der Eingabe nicht „abspicken" lassen.

Beispiele für „geeignete" Passwörter

Acht bzw. 12 Zeichen bestehend aus Ziffern, Buchstaben und Sonderzeichen:

Bitte beachten: nicht jedes System nimmt alle Zeichen an! Die Beispiele sollen nur das Grundprinzip darstellen!

*a1b2c3#	&xyz&123
*„wort"#	*aabbcc#
~mon@t01	§rechte§
8=2*vier	iß@was!
@ttent@t	„4you4me
pc_st@rt	go_to_me
0m4_m4m4	0p4_p4p4
j4hr2oo5	=nur4u2=

aus	wird
harald	81r1l4
marie	m1ri5
Otto	02to
Finanzamt 2010	F2nzmt_2o1o
Vertraulichkeit	5rtrulichkit