



Passwort-Tipps

Kapitel 1

Ein gutes Passwort sollte für den *Ersteller* einfach und logisch sein. Somit verringert sich die Gefahr, dass er sein Passwort vergisst. Ein Passwort, welches dem Benutzer in Erinnerung bleiben soll, benötigt nur eine *einzig*e Gedächtnisstütze, z.B. eine bedeutsame *persönliche* (nicht allgemein rekonstruierbare!) Vorstellung, Farbe oder Ortschaft - und schon erinnert er sich [0].

Passwörter müssen orthographisch durchaus nicht korrekt geschrieben werden. Dazu finden Sie ein paar Anregungen in einer weiteren Tabelle [1].

Eigene Schreibvarianten kann man sich etwa mit Bezug auf die englische Sprache zu Nutze machen. Dazu vergleiche auch Tabelle [2].

Ganz persönliche Erlebnisse lassen sich mit einfacher Verschlüsselung in Passwörtern „verewigen“ [3]. Natürlich dürfen nicht allgemein nachvollziehbare Daten (z.B. Geburtstage) verwendet werden. Daten müssen durch leichte Verschiebungen und umschreibende Zeichen verfremdet werden. So kann etwa 27 auch 2007 bedeuten.

(Die folgenden Beispiele sollten selbstverständlich nicht unverändert übernommen werden.)

[0]Beispiel

Passwort	Gedächtnisstütze	Lösung
2muchW	Stress	zu viel Arbeit

[1]Beispiel für mögliche Passwörter

Passwort	Korrekte Schreibweise	Weitere Möglichkeiten
treesTarrHotel	three, star	3stArOtel / HoteLSTaR3

[2] Englische Wörter, welche ähnlich (nicht unbedingt gleich) tönen.

tree (Baum)	three (drei)
to* (nach, zu) too (auch)**	two (zwei)
know (wissen)	now (jetzt)
night (Nacht)	knight (Ritter)

* I'd like to go to London (...würde gerne nach London gehen)

** A: I like tea. B: Me too. (A: Ich mag Tee B: Ich auch)

[3] Erlebnisse werden zu Passwörtern

3073PaRisUsI	am 3.3.07 gab Paul Susi den Verlobungsring
5275KewinRedli	am 5.5.07 trug Cevin einen roten Pulli
jK2755stef	am 5.5.2007 (oder auch 27.5.05) trafen sich Jacky und Steffi
Dav11999Z45	seit 1.1.1999 kenne ich David / seit 45 Tagen leben wir zusammen.

Kapitel 2 - Weitere Techniken für Passwörter

Bis jetzt fuhr der User eigentlich immer gut mit einem Passwort in der Länge von etwa acht Zeichen (numerisch, alphabetisch und mit Sonderzeichen). Aber wenn man wirklich sicher sein möchte, kann ein Passwort nie genug lange sein. Genau hier liegt der Hund begraben, denn je länger das Passwort ist, umso eher vergisst der Benutzer das kostbare Wort.

Für je einen Tag, Monat, ein Jahr, Ereignis, eine Situation oder ein Gebäude denkt man sich jeweils ein bis drei Sonderzeichen plus ein alphabetisches Zeichen aus.

Montag	#
Februar	%F
1997	(?)7
Verlobung)*()
sass/Stuhl	_/ _
Berliner Mauer	-- --

Nun lassen sich mit Hilfe dieser Zeichen ganze Sätze verschlüsseln, aber für den Verfasser bleiben sie logisch.

Als die Berliner Mauer sich öffnete, sass ich in einem Café in Berlin.	ad-- --soe_ /iieCiB
Am Tag unserer Verlobung trug sie ein rotes Kleid	aTu)* (tSrK
Seit ich ein Emailkonto habe, schreibt mir Kim täglich	sieE@KhsmKt

Kapitel 3 – Passwort, Passwort-Satz

Um die Sicherheit zu steigern, kann der Benutzer also seine Passwörter verlängern. Dazu möge er sich die Techniken der ersten beiden Kapitel zunutze machen. Mit Hilfe von Kapitel 1 und 2 lassen sich schon mal sichere Passwörter erstellen. Nun gibt es eine weitere Methode, Passwörter sicherer zu machen [4].

Nehmen wir mal an, Sie verwenden nur Kleinbuchstaben und Ziffern. Das Passwort wäre 6 Zeichen lang; das gäbe 36^6 Möglichkeiten. Mit Gross- und Kleinschreibung plus Ziffern käme man auf 62^6 .

Gemäss [4] werden die Passwörter 18 und mehr Zeichen lang. Mit der oben erwähnten Methode wären es nun 62^{18} Variationen, und zwar ohne Sonderzeichen.

[4] Passwort-Sätze

Bei Technik 1 wird jede dem Passwort zugrunde liegende Worteinheit mit dem Anfangsbuchstaben derselben begonnen. Bei Technik 1b wird jede dem Passwort zugrunde liegende Worteinheit mit dem Anfangsbuchstaben der **ersten** Worteinheit begonnen. Technik 2 variiert zwischen dem 1. und dem 2. Buchstaben der jeweiligen Worteinheit. Technik 2b = Technik 2, analog zu Technik 1b.

Mehr dazu in den folgenden Beispielen.

Beispiel Technik 1

Merksatz	1+2; 1+3; 1+3; 1+5; 1+8; 1+5; 1+2; 1+4;1+3
Wer mit dem Strom schwimmt, erreicht die Quelle nie	WemtdmSrsteidiQlne

Beispiel Technik 1b

Merksatz	1+2; 1+4; 1+7; 1+8; 1+10; 1+12; 1+14,1+15+16
Wer mit dem Strom schwimmt, erreicht ...	WeWmWdWeWSWrWmWsc

Beispiel Technik 2

Merksatz	1+3;1+4; 1+2; 2+3;1+2+5
Eine Hand wäscht die andere	EnHdwäieanr

Technik 2b erklärt sich nun von selber.

Man kann die Passwort-Formel auch selber gestalten. Um eine saubere Technik 1 oder 2 beizubehalten, sollte man auf deren Basis aufbauen. Es liessen sich in analoger Schematik eine Technik 3 oder 4 etc. erstellen, aber diese würden auch für den Ersteller immer schwieriger zu entschlüsseln.

Zeichen wie diejenigen in Kapitel 2 lassen sich natürlich in alle Passwörter einbeziehen.