Inhalt

Die Entscheidung ist gefallen. Die Wahl zum **beliebtesten schlechten Passwort** ist zu Ende.

Im Prinzip hat sich nicht viel geändert. Spitzenreiter ist und bleibt das Wort **password**, dicht gefolgt von **123456** und **12345678**. Neu in der Rangliste der schlechtesten Passwörter dürfen wir die Begriffe **welcome**, **jesus**, **ninja**, **mustang** und **password1** begrüßen. Man braucht nicht unbedingt ein Programm, um zu erahnen, dass diese Passwörter unglaublich schlecht sind und damit selbstverständlich

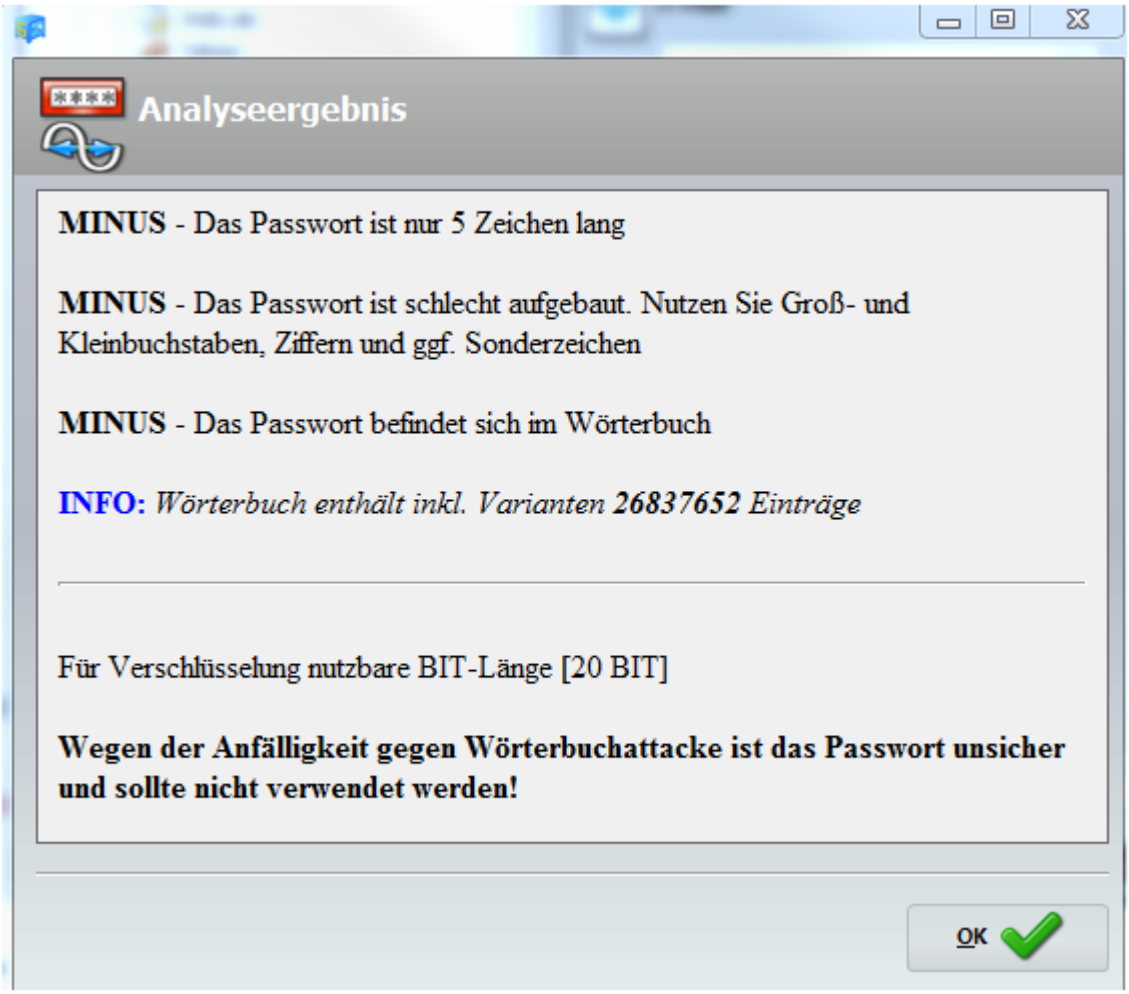
preisverdächtig. Dennoch ist es interessant zu sehen, was zum Beispiel die **Passwort-Analyse** des ArchiCrypt Passwort Safes zu den Begriffen meint.

Computergestützte Passwort-Analyse *

Password *

**123456 und 12345678 *

Ninja *



Alle weiteren Passwörter der Liste liefern identisch miserable Bewertungen. Wer den Artikel Der fiese Wörterbuchangriff gelesen hat, weiß warum. Es handelt sich ausnahmslos um Zeichenfolgen, die genau so in einem Wörterbuch zu finden sind. Wir Deutschen, hier insbesondere die etwas ältere Generation, wissen inzwischen um die Wichtigkeit eines guten Passwortes. Im Artikel Wie sicher ist mein Passwort konnte man lesen:

> Die Gruppe der bis 25-Jährigen verwendet Passwörter, die nur halb so sicher sind, wie die aus der Gruppe der über 55-jährigen Deutschen.

Keine absolute Aussage, sondern eine relative. Trotzdem sind wir Deutschen insgesamt deutlich vorsichtiger im Umgang mit Zugangsdaten. Das sollte uns aber nicht in Sicherheit wiegen. Man muss sich nur einmal selbst an die Nase packen oder

sich im näheren Verwandten- und Bekanntenkreis etwas umhören. Klar sichert Oma Elfriede das WLAN mit dem Passwort Ihres Enkels ab.

So wähl man ein sicheres Passwort *

Wenn Sie wieder einmal beim Nachsinnen über ein neues Passwort für den Internetshop Nr. 2078 dem nur allzu natürlichen Drang nachgeben, doch den Namen von Waldi dem treuen Jagdgefährten zu nutzen, bedenken Sie die Folgen, die es hat, wenn sich jemand Zugang zu diesem Shop mit Ihrem Namen verschafft. Zunächst einmal könnte er gehörig Ärger machen, indem er auf Ihren Namen Produkte bestellt. Möglicherweise wird der Versand auch noch auf eine Packstation umgeleitet, deren Daten man sich bei jemand anderem besorgt hat. Wenn Sie bei Ihrem Drang, möglichst einfach zu merkende Passwörter zu verwenden, allerdings ständig zum selben Passwort greifen, werden Sie Ihr blaues Wunder erleben!

Das blaue Wunder *

Das blaue Wunder tritt in diesem Fall nicht in der Textilfärberei durch suboptimale chemische Umwandlungen ans Tageslicht, sondern gibt sich wie folgt zu erkennen: Verschafft sich jemand Zugang zu einem aus Ihrer Sicht zunächst vollkommen unwichtigen Dienst, hat er mindestens das Wissen, dass das herausgefundene Passwort als Schlüssel verwendet wird. Dies genügt, damit Ihr Passwort Teil einer Liste wird, die im Internet frei oder gegen Bares zu haben ist. Mit diesen Listen wird dann auf WEB-Seiten automatisiert versucht, Zugang zum jeweiligen Dienst zu bekommen. Haben Sie das Passwort jetzt nicht nur zur Absicherung des Online-Tagebuchs von Waldi genutzt, sondern auch bei Amazon, eBay, Zalando, Facebook etc. wird es extrem unangenehm. Ist Ihr Mailpostfach mit diesem Passwort gesichert, steht sogar dem kompletten Identitätsdiebstahl nichts mehr im Wege. Die **Passwort-vergessen Funktion** vieler Internetseiten macht es möglich. Es genügt die Angabe der E-Mail Adresse und fluchs wird ein neues Passwort per E-Mail verschickt. Nach und nach kann man sich so Zugriff zu allen Diensten und Konten verschaffen, die Sie nutzen.

Das sicherste Passwort der Welt *

… ist mindestens 12 Zeichen lang, enthält Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen, steht in keinem Wörterbuch und …

existiert genau ein
Mal und darf von mir aus Sicherheitsgründen hier nicht genannt werden J

> Folgende Idee an sich ist gut: Man merkt sich ein einzelnes sicheres Passwort und verwendet dann nur noch dieses.

Aber auch dieses sichere Passwort verliert schlagartig seine Poolposition und wandert in die Liste der schlechten Passwörter, sobald sich jemand durch die Hintertür Zugang zu einer Passwortdatenbank eines Anbieters verschafft. Wer jetzt, ob der Sicherheit seines Passwortes, darauf vertraut hat, dass niemand das Passwort erraten kann, steht ebenfalls mit heruntergelassener Hose im feuchten Herbstwind.

Die Folgen sind tragisch: Das Passwort wurde nicht erraten, sondern entwendet. Dem entwendeten Passwort droht das gleiche Schicksal wie dem erratenen Passwort. Es wird gnadenlos missbraucht und in die Liste der Passwörter übernommen, mit der dann automatisiert versucht wird, Zugriff zu interessanten Internetdiensten zu bekommen. Ihr Passwort, so sicher es auch gewesen sein mag, ist jetzt nichts mehr wert.

Diebstahl von Passwörtern und Zugangsdaten … *

… ist kein seltenes Randphänomen. Wir kennen alle die Pressemeldungen über entwendete Daten von Pornoseiten und Sony. Wahrscheinlich ist dies nur die Spitze eines Eisberges. Nicht immer dürften Anbieter und damit die, zu Hütern sensibler Daten Verurteilten, Kenntnis davon haben, dass Daten entwendet wurden. Die Zahl derer, die den Mantel des Schweigens über den Diebstahl von Kundendaten ausbreiten, dürfte ebenso hoch sein. Der drohende Ansehensverlust dürfte solche Firmen daran hindern.

Tipps zum Umgang mit Passwort und Zugangsdaten *

Ich habe bereits zahlreiche Tipps zu diesem Thema verfasst.

Wie sicher ist mein Passwort? und Der fiese Wörterbuchangriff sind Pflichtlektüre!

- Legen Sie sich Profile auf Internetseiten nur dann an, wenn dies unumgänglich ist.
- **Verwenden Sie Passwörter nie mehrfach, sondern legen Sie für jeden Zweck ein neues sicheres Passwort an.**
- Verwenden Sie nur Passwörter, die **sicher aufgebaut** sind. Hier kann man sich auch abweichend von den recht häufig gemachten Empfehlungen auf sicherem Boden bewegen.

> Klar wird ein Passwort Wh77&%%gü!hh wohl zur Kategorie sicher gehören. Aber denken Sie, ein Passwort wie **MausApfelAuto12** sei schlecht?

So etwas wie **MausApfelAuto12** kann man sich merken und man ist auf der sicheren Seite. Zumindest die Daten für die wichtigsten Seiten und Dienste im Internet hat man dann auch unterwegs ohne elektronische Helferlein parat. Will man die Gesamtheit seiner Passwörter so anlegen und sich merken, wird man jedoch, vorausgesetzt, man ist nicht Anwärter auf den nächsten Gedächtnisweltmeistertitel, auf Hilfsmittel zurückgreifen müssen. Hier sind softwaretechnische Hilfemittel (Passwortmanager) unverzichtbar.

Quellen: http://mashable.com/2012/10/23/worst-passwords/

Studie der Universität Cambridge

Weiterführende Informationen:

Sicherheit eines Passwortes20

