Inhalt

„**Wie sicher ist mein Passwort?**“ Diese Frage ist inzwischen existenziell geworden? Wer schwache Passwörter verwendet, der setzt sich einer großen Gefahr aus!

Was denken Sie, wenn ich Ihnen sage, dass ich die beiden **Passwörter 123 und 456** einfach liebe?

Wie sicher ist mein Passwort?

Auf unseren **Entwicklungsrechnern** wird man haufenweise Dateien finden, die mit den Passwörtern **123** und **456** verschlüsselt sind. Ich liebe diese griffigen kleinen Passwörter, weil sie zur gleichen Zeit so unglaublich einprägsam und so schnell einzugeben sind. Damit habe ich bereits das zum Ausdruck gebracht, was den meisten

Menschen wichtig ist.

Passwörter sollen primär leicht zu merken sein und man soll sie unkompliziert eingeben können.

Die Forderung nach Sicherheit hat sich gefälligst diesen Primärforderungen unterzuordnen.

Was im Umfeld von Softwareentwicklung vollkommen legitim ist – schließlich werden die Dateien nur im Rahmen unzähliger Tests verschlüsselt, und nicht, um sensible Daten vor unbefugtem Zugriff zu schützen – wird zum echten Problem, wenn man diese Herangehensweise im Alltag wählt. Nämlich dann, wenn tatsächlich sensible Daten geschützt werden sollen. Thematisch passt eine neue Studie der Universität Cambridge perfekt. Weltweit wurden **70 Millionen Passwörter** untersucht. Heraus kamen sehr interessante Erkenntnisse, die nicht nur allgemeine Aussagen zulassen, sondern auch **regionale und altersbedingte Besonderheiten bei der Passwortwahl** aufzeigen.

Das meistgenutzte Passwort der Welt *

Die Formulierung der Überschrift gibt schon klar zu erkennen, dass es sich bei einem Passwort, welches weltweit sehr häufig zum Einsatz kommt, kaum um ein sicheres handeln kann. Das Passwort erfüllt allerdings die oben angesprochenen Primärforderungen. Es ist nicht zu lange, kann schnell eingegeben werden und man kann es sich ganz toll merken.

> **Das international meistgenutzte Passwort lautet**
>
> **123456**

Im wirtschaftlichen Umfeld werden weltweit die Passwörter **password1**, **welcome** und **password2** am häufigsten verwendet.

Wer wählt die besten Passwörter? *

Verblüffend! Wir Deutschen sind auch in der digitalen Welt relativ sicherheitsbewusst. Laut Studie gehören deutsche Computernutzer eher zu den sorgsameren Vertretern bei der Passwortwahl. Besonders positiv fallen wir etwas Älteren auf. Die angeblich sich so sicher auf dem digitalen Parkett bewegenden Digital Natives sind deutlich argloser.

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

Völlig klar! Auch Prominenz schützt vor unsicheren Passwörtern nicht. Bashar al-Assad, der syrische Diktator, musste Anfang Januar zusehen, wie sich seine politischen Gegner seinen E-Mail Verkehr etwas näher ansahen. Assad, nicht dumm, hielt sich an den **internationalen Standard für miserable Passwörter** und wägte sich mit **123456** in Sicherheit.

Ein wunderbares Beispiel für Erfolg bringende Recherche im sozialen Umfeld einer Person, lieferte einst Paris Hilton. Die junge Dame besaß einen Chihuahua mit Namen „**Tinkerbell**„. Es leuchtet ein, dass sich mit dem Namen des kleinen Felligen auch prima Daten schützen lassen. Gut merkbar, kurz und schnell eingegeben. Dumm nur, wenn andere auch auf diese abwegige Idee kommen und sich so Zugang zu sensiblen Daten verschaffen.

Im Beitrag „Der fiese Wörterbuchangriff“ im Abschnitt „Heute ist der Müller dran!“ kann man sich genau das durchlesen, was der Wissenschaftler Joseph Bonneau empfiehlt, um zum Beispiel den **Account der Queen** zu hacken. Vielleicht liest die nette alte Dame ja den Artikel und überdenkt die Passwortwahl nochmals. Das Thema „Tinkerbell“ hatten wir im Artikel Die Waldi-Absicherung ebenfalls schon. Sie sehen, worauf es wieder einmal hinausläuft. Ähnlich einem Übergewichtigen, der im Prinzip den Kaloriengehalt eines jeden Lebensmittels kennt und dennoch nicht vor Eiscreme, Kuchen und Pizze halt machen kann, begehen wir bei der Passwortwahl immer wieder die gleichen Fehler.

> Wir wählen das Passwort zu kurz und zu leicht zu erraten!

So wählen Sie ein sicheres Passwort *

Bedenken Sie immer die Folgen, die drohen, wenn sich jemand durch Ihre Nachlässigkeit bei der Passwortwahl Zugang zu den Daten verschafft, die Sie eigentlich schützen wollen. Vielleicht motiviert Sie das künftig so, dass Sie Passwörter mit etwas mehr Hingabe erzeugen?!

Was **Tipps zur Passwortkonstruktion** angeht, möchte ich hier nichts Neues schreiben. Bereits im Waldi Artikel konnten Sie Ähnliches nachlesen:

> 1. Ein Passwort muss eine bestimmte Länge haben
> Es besteht ein Konflikt zwischen der Länge eines Passwortes, welches der Nutzer noch bereitwillig lernt und der Länge eines Passwortes, welches ausreichend Sicherheit bietet.
>
> **Ergebnis**: *Ein Passwort sollte aus mindestens 10 Zeichen (besser 12 und mehr) bestehen. Das Passwort sollte sich aus Ziffern, Groß-/Kleinbuchstaben und Sonderzeichen zusammensetzen.*
>
> 2. Keine lexikalischen Begriffe verwenden
> Keine Begriffe/Zeichenfolgen verwenden, die aus einem (Wörter)Buch stammen. Dazu zählen auch Namen, Daten und Fakten.
>
> **Ergebnis**: *Nutzen Sie zur Erzeugung des Passwortes den kompletten Zeichenvorrat – Groß-/Kleinbuchstaben, Ziffern und Sonderzeichen*
>
> 3. Einmalige Verwendung
> Nutzen Sie ein bestimmtes Passwort ausschließlich zur Absicherung eines einzigen Zugangs oder Kontos etc.
>
> **Ergebnis**: *Erzeugen Sie sich für jeden neuen Fall in dem Sie ein Passwort benötigen ein eigenes sicheres Passwort.*
>
> Beispiel für ein solches Passwort:
> Zh8(Dx23_%k6s

Mir ist bewusst, dass man sich solche Passwörter kaum merken kann. Zumindest nicht in der Menge, in der man sie inzwischen im digitalen Zeitalter benötigt.

Verwenden Sie daher einen Passwort Safe!

Es wäre zwar schön, wenn es sich um ArchiCrypt Passwort Safe handeln würde, aber wichtiger ist, dass Sie überhaupt ein sicheres Verwaltungsprogramm für Ihre Zugangsdaten nutzen. Sie müssen sich dann nur noch ein einziges Masterpasswort merken. Die Verwaltung der vielen anderen Passwörter übernimmt dann das Programm. Vielleicht bietet es auch noch so viel Komfort, dass es selbs sichere Passwörter erzeugen kann und Sie nach Eingabe des Masterpasswortes automatisch beim Besuch einer Internetseite einloggt?

Eine Übersicht der Eigenschaften, die **ein guter Passwort Manager** haben sollte, finden Sie im Artikel „Der fiese Wörterbuchangriff„.

