Teil 1: Unknackbar, aber einfach zu merken! - Passwörter einfach erklärt

1. Aus den am Anfang erwähnten mindestens 8 Zeichen für akzeptabel sichere Passwörter sind mittlerweile 16 geworden. Hier ist es wie bei Segelschiffen: Länge läuft…
2. Zum Thema Rechenzeiten für das Knacken per *Brute Force* hilft folgende Seite und birgt auch noch mehr Informationen zur Passwortsicherheit: https://www.1pw.de/brute-force.php
3. Die Empfehlung, einen Passsatz zu verwenden ist in Ordnung, erfordert aber auch Phantasie und Kreativität. Bekannte Zitate aus Büchern oder „Alltagssprüche“, ob Prosa oder Lyrik, verbieten sich, denn die sind auch Teil der genannten Wörterbücher (in allen gängigen Sprachen).
4. Was auch geht: Vier zufällige Substantive aus unterschiedlichen Bereichen (Beruf, Pflanze, Tier, Mobilität, Werkzeug, was auch immer mehr) die keinen inneren Zusammenhang ergeben, sich aber im Kopf zu einem sinnvollen Satz oder einer kurzen Merkgeschichte verbinden lassen. Hintereinander geschrieben, mit oder ohne Sonderzeichen oder Zahlen.

Wer diesen Film auf YouTube ansieht findet in den Anmerkungen (unter „MEHR ANSEHEN“) nicht nur, was Edward Snowden (ja der!) zu Passwörtern anmerkt (https://www.youtube.com/watch?v=yzGzB-yYKcc). Es gibt auch den Hinweis auf den Passwortmanager „Passwort Safe“. Ich selbst ziehe seit längerer Zeit den ebenfalls kostenlosen und quelloffenen „**KeePass**“ vor. **Ich rate sogar zur portablen Version**, die läuft auch auf einem USB-Stick. Dieser Passworttresor hat sich erfolgreich einem *Bug Bounty* der Europäischen Union auf potentielle Sicherheitsprobleme unterzogen. Das ist ein öffentlicher Test mit einem Preisgeld für die Aufdeckung schwerwiegender Mängel. KeePass ist auch die Empfehlung des BSI (Bundesamt für Sicherheit in der Informationstechnik).

Ich kann in dieser verschlüsselte Datenbank manuell oder automatisch generierte Passwörter eintragen. Für letzteres setzte ich die Passwortlänge und das Format, der Rest folgt Algorithmen, die bisher als sicher gelten dürfen. Es gibt eine Fülle von Funktionen, die ich hier nicht aufzählen möchte. Probieren kostet nichts, die Zeit ist ja momentan vorhanden. Das Programm ist (nebst deutschem Sprachpaket) hier zu haben: https://www.heise.de/download/product/keepass-15712/download. Wer Englisch kann, nutzt die Quelle https://keepass.info/download.html.

Ein guter Passworttresor braucht nur ein Passwort. Ist das lang und nach den auch im Video diskutierten Kriterien sicher – warum dann häufig wechseln???

Alternativen?
Ach ja, das Notieren auf Papier geht auch. Dann muss die Aufbewahrung aber an sicherer Stelle erfolgen, in irgendeinem Ordner mittendrin. Niemals am Rechner oder auf dem Schreibtisch (nein, kein Scherz – das gab es mehr als einmal) und möglichst auch nicht dort, wo alle paar Jahre in großem Stil ausgemistet wird (Steuerordner, Rechnungen). Ein Blatt zwischendrin könnte dabei schnell mit verschwinden. Unterwegs bitte kein Papier! Nichts was ich tragen kann ist vor Verlust sicher. Der Passworttresor in fremden Händen – ja und? Ein Papier mit allen Zugängen die mich finanziell am Leben halten – oh je!

Abschließend: Es gibt keine absolute Sicherheit, nur Wahrscheinlichkeiten. Was theoretisch tausende Jahre Rechenzeit dauert, kann auch in Millisekunden vorbei sein. Aber, wer hat

schon im Lotto den Volltreffer gelandet? Der technische Fortschritt kann natürlich auch hier alles beschleunigen. Bis dahin, schlaft beruhigt (das ist ernst gemeint).