Computersicherheit

Inhalt:

- Das sichere Passwort
- Der Adblocker
- Virenscanner
- Backups von Daten

Das Sichere Passwort:

- Wie werden Passwörter geknackt?
  - Die wenigsten Passwörter werden wirklich geklaut…
  - Weitaus die meisten werden einfach erraten.
- Ein Computer kann mehrere tausend Vergleiche pro Sekunde durchführen, somit sind alle kurzen Passwörter, selbst wenn sie aus zufälligen Zeichen bestehen **NICHT SICHER!**
- Passwörter sollten aus Folgenden Elementen bestehen:
  - Großbuchstaben (ABCDEF…)
  - Kleinbuchstaben (abcdef…)
  - Sonderzeichen (.,!?#§%{[&…)
  - Zahlen (1234567…)
- Passwörter die nicht **mindestens 3** Sorten von Zeichen enthalten **und** kürzer als 8 Zeichen sind, sind in wenigen Minuten, wenn nicht Sekunden geknackt!
- Vergleiche: www.howsecureismypassword.net auf dieser Seite können Sie ihr Passwort prüfen lassen**. Dabei müssen Sie beachten, dass die errechnete Zeit nur auf einem zufallsbasierten Programm beruht. Je mehr echte Wörter (z. B. aus dem Duden) oder persönliche Daten, in Ihrem Passwort enthalten sind, desto einfacher ist es zu knacken!**
- Unsicher sind Passwörter besonders, wenn sie persönliche Informationen enthalten wie:
  - Namen, Geburtsdaten o. Ä., von Freunden, Familie oder Haustieren
- Die Passwörter können dann mit sogenannten Wörterbuchangriffen herausgefunden werden. Dabei wird eine Liste von Wörtern, die der Hacker aus dem persönlichen Umfeld der Zielperson entnommen hat, in eine Liste gepackt und durcheinander oder zusammengesetzt ausprobiert. Dabei kann der Hacker sein Programm so schreiben, dass beliebige Manipulationen an den möglichen Passwörtern vorgenommen werden können.

Erstellen des Sicheren Passwortes:

- Zum erstellen von Passwörtern gibt es viele Methoden, hier die effektivsten:
  - Wortmischungen
  - Satz-zu-Wort
  - Leetspeak

Autor: Daniel Meerwald

Wortmischungen:

- Sie vermischen Wörter Buchstabe für Buchstabe und wiederholen dabei das kürzere.
- Fahrradkette+Besen=FBaehsrernaBdekseetntBe
- Dabei empfiehlt es sich erst das eine Wort zu tippen und danach die Lücken mit dem anderen Wort zu füllen.
- Das Passwort sollte trotzdem mit Zahlen und Sonderzeichen verstärkt werden wie:
- 5FBae?hsre?rnaBd?eksee?tntBe? (Die 5 verweist hier auch zusätzlich auf die Stellen an der sich das Sonderzeichen befindet, alle 5 Zeichen)
- Vorteile: Sehr lange Passwörter können erstellt werden, die trotzdem leicht zu merken sind!
- Nachteile: Passwort muss jedes mal „konstruiert“ werden, das kostet Zeit!

Satz zu Wort:

- Anfangsbuchstaben von Wörtern des Satzes, plus Satzzeichen und Zahlen einem Satz:
- Mein Vater erklärt mir jeden Sonntag unsere 9 Planeten!
- MVemjSu9P!
- Vorteile: Mit nur einem gut gewählten Satz, können alle wichtigen Anforderungen für ein Passwort erfüllt werden. (Großbuchstaben, Kleinbuchstaben, Sonderzeichen, mindestens 8 Zeichen)
- Nachteile: Je bekannter der Satz, desto einfacher können findige Hacker diesen Knacken. Deshalb sollten eigene Sätze verwendet werden, und nicht so bekannte wie im Beispiel!

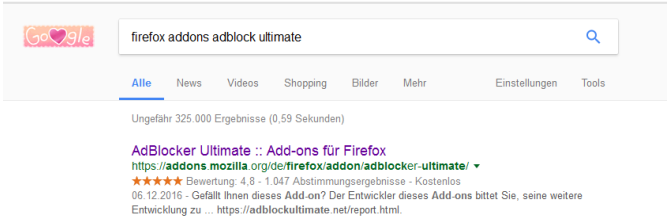
Leetspeak:

- Leetspeak ist eine Methode bei der Buchstaben durch Zahlen und Wörter ausgetauscht werden.
- Damit lassen sich normale Wörter in Sichere Passwörter Verwandeln.
- HundKatzeMaus -> HundK4!z3M4u5
- Es empfiehlt sich, eine eigene Liste mit Buchstaben und Zeichen zu entwerfen um den Hackern möglichst wenig Angriffsfläche zu bieten.
- Vorteile: Einfache und ansonsten schwache Wörter können zu starken Passwörtern aufgewertet werden.
- Nachteil: Mit der richtigen Übersetzungsliste, sind die sicheren Wörter für die Hacker wieder nur normale, schwache Wörter.
- Beispieltabelle Leetspeak: l=1 z=2 e=3 a=4 s=5 o=0 i=! b=& c=(…
- Die sichersten Passwörter erstellt man natürlich durch eine Kombination der Methoden.
- Es gilt, je unkonventioneller ihre Herleitung des Passwortes ist, desto sicherer sind sie.
- Durch das anwenden nur einer dieser Methoden, ist ihre Passwort unten den top 15% der sicheren Passwörter.
- **Top 10 der deutschen Passwörter:** 1. Hallo, 2. Passwort, 3. hallo123, 4. schalke04, 5. passwort1, 6. Qwertz, 7. Arschloch, 8. Schatz, 9. hallo1, 10. Ficken
    - An diesem Beispiel können Sie sehen wie einfallslos die meisten Menschen sind und warum es so einfach ist ihre Passwörter zu knacken.

Der Adblocker:

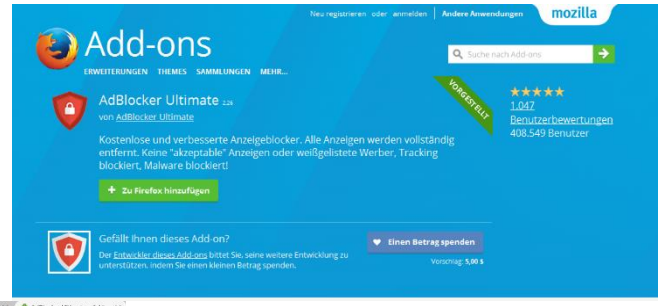
- Blockiert Werbung im Browser, wodurch auch die Potentiell gefährliche und unseriöse Werbung entfernt wird durch die sie sich Viren einfangen können.
- Zusätzlicher Vorteil ist, dass nervige Werbung so gut wie vollständig entfernt wird. Vor Videos oder auf Internetseiten von Magazinen etc. werden keine Anzeigen mehr eingeblendet.

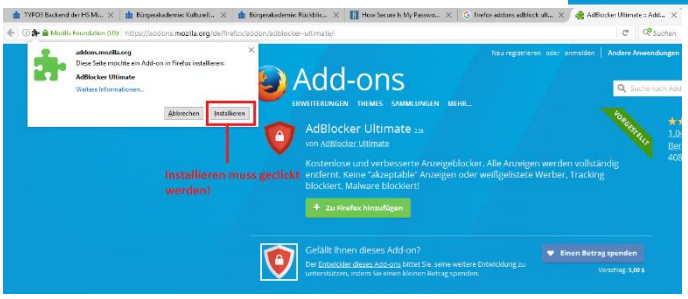
Beispiel Firefox, analog zu Google Chrome:



1. Googlen nach dem Browser (Google Chrome oder Firefox) und dem Addon.
Bei Firefox: **Adblock Ultimate**
Bei Google Chrome: **Adblock Pro**
Es gibt viele Adblocker Addons, die meisten werden aber von Werbefirmen Bezahlt um gewisse Werbung durch zu lassen. Die beiden hier angeführten sind garantiert nicht Bezahlt. Trotzdem kann es sein, das besonders raffinierte Werbung trotzdem ab und an angezeigt wird. Im allgemeinen filtern die Adblocker aber 99% der Werbung.

2. Das Addon zum Browser hinzufügen.





3. Dann muss das Installieren des Addons bestätigt werden.
4. Der Browser muss nach erfolgreicher Installation neu gestartet werden.
5. Der Adblocker sollte nun einwandfrei arbeiten. Zum testen können sie www.bild.de besuchen. Verweigert ihnen die Seite den Besuch, mit einem Hinweis auf ihren Adblocker, haben Sie alles richtig gemacht.

Autor: Daniel Meerwald

Virensanner:

- **Häufig Missverstanden:** Virenscanner schützen Sie nicht vor einer Infektion durch Viren!
- Virenscanner durchsuchen Ihre Festplatte nach einer bereits existierenden Infektion bekannter Viren. Dabei agieren sie ähnlich wie ihr Immunsystem.
- Der Virenscanner kann also nur Effektiv Viren bekämpfen die bereits von anderen Computern erkannt und gemeldet wurden. Selbstgebastelten Viren steht der Computer meist schutzlos gegenüber, weshalb eine Infektion durch überlegtes Handeln bereits vorher vermieden werden sollte.

Virenscanner wie *McAfee* oder *Avira* sollten gemieden werden, Sie aktivieren ungefragt Suchläufe und Updates, die den PC vorrübergehend sehr langsam machen und somit den Arbeitsfluss behindern.

Falls Sie sich für einen kostenpflichtigen Virenscanner entscheiden, empfehle ich ihnen **Kaspersky** oder **Norton**. Diese beiden gehen weit über den Umfang eines herkömmlichen Virenscanners hinaus und arbeiten mit innovativen Techniken um Viren frühzeitig zu erkennen bevor sie schaden anrichten können.

Als Freeware (Kostenlose Software), empfehle ich ihnen den in Windows **integrierten Windows Defender.** Er ist sehr schnell und agiert nicht ohne ihre Zustimmung. Dabei greifen alle Virenscanner bei ihren Suchläufen auf dieselbe Datenbank zurück, weshalb die Erkennungsrate der kostenlosen Virenscanner quasi deckungsgleich ist.
Den Defender aktivieren Sie meist über die Systemsteuerung. Dafür unter Windows Vista-8.1 die Windows-Taste drücken und Systemsteuerung anwählen. Danach clicken Sie auf Sicherheit und können dort den Defender aktivieren.
Unter Windows 10 können Sie einfach die Windows-Taste drücken und dann auf der Tastatur „Defender“ eintippen. Der Windows Defender wird ihnen dann als erster Vorschlag vorgeschlagen. Anclicken und das Programm bietet Ihnen die Option es zu aktiviere.

Backups von Daten:

- Backups sind automatisierte Kopien Ihrer Daten auf einem Externen Medium. Zum Beispiel einer Externen Festplatte oder einem USB Stick oder im Internet.
- Dadurch wird die Redundanz (mehrfach Vorhandensein von Daten) erhöht und Sie sind vor Datenverlust besser geschützt
- Windows bietet seid Windows 7 sehr einfache Wege zum Backup.
- Für eine Schritt für Schritt Anleitung sehen sie bitte in den Folien nach. (Seiten 20-34)
- Im dort angeführten Menü können auch Ordner oder das Laufwerk wieder entfernt werden.
- Ordner sollten ins Besondere bei kleinen Speicher, wie einem USB Stick, aus der Liste der zu Sichernden Ordner entfernt werden. Da alle Ihre persönlichen Ordner bereits Standardmäßig gesichert werden, können damit große Datenmengen anfallen, die einen USB-Stick oft überfordern.
- Es Empfiehlt sich also eine Festplatte für ihre Daten-Backups zu nutzen.