Inhalt

Wir alle sind inzwischen mehr als sensibilisiert. Passwörter müssen bestimmte Anforderungen erfüllen um als sicher zu gelten.

Wir sagen gemeinsam die Regeln auf:

- „Ein Passwort soll mindestens 12 Zeichen lang sein“
- „Verwende keine lexikalischen Begriffe, keine Namen, Orte, Geburtsdaten etc.“
- „Verwende Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen“
- „Verwende niemals dasselbe Passwort an mehreren Stellen“

Uns allen sind auch die damit zusammenhängenden Probleme bekannt. Wer soll sich diese Unzahl an komplizierten Konstrukten merken. Der Gedächtnisweltmeister vielleicht.

Getreu dem Motto „***Geiz ist geil***“ nutzen wir das, was vermeintlich kostenlos ist. Die erste Hilfe, die dem Anwender angeboten wird, ist die in Browser integrierte Passwortverwaltung.

[youtube_video id=“QaXFOD1_R8c“]

Wer ***chrome://settings/passwords*** in die **Adresszeile** des Google Browsers eingibt erhält Zugriff auf alle gespeicherten Passwörter. **Ohne jede Sicherheitsmaßnahme**.

Alle Daten sind offen und ungeschützt. Entdeckt hat diese eklatante Sicherheitslücke der Software-Entwickler **Elliott Kember**.

Unglaublich die Reaktion von Google. Es handle sich nicht um eine Sicherheitslücke, sondern man wolle den Anwendern durch die Verwendung eines Masterpasswortes keine

trügerische Sicherheit vorgaukeln. Wenn jemand Zugang zum Rechner hätte, würde auch kein Passwort mehr schützen.

Die Argumentation ist äußerst aufschlussreich und inakzeptabel!

Warum Autos mit einem Schloss versehen? Das ist doch trügerische Sicherheit.

Warum die EC Karte mit einer PIN schützen? Trügerische Sicherheit!

1. Einem (Passwort)Dieb muss mit allen erdenklichen Maßnahmen das Leben so schwer wie möglich gemacht werden. Dazu gehört im vorliegenden Fall mit Sicherheit die Verwendung eines **Masterpasswortes** zur Verschlüsselung der Passwortdaten. Auch wenn ein Masterpasswort alleine keine 100%ige Sicherheit bieten kann, so stoppt es dennoch eine sehr große Zahl potentieller Angreifer.
2. Die Daten sind auch insbesondere dann nicht geschützt, wenn der Anwender Chrome beendet oder den Rechner herunter fährt. Sofern das eingesetzte Verschlüsselungsverfahren entsprechend leistungsfähig ist und das Masterpasswort unter Beachtung unserer Regeln gewählt wurde, würde das Masterpasswort die Daten zuverlässig auch vor hartnäckigen und ausdauernden Angreifern schützen!

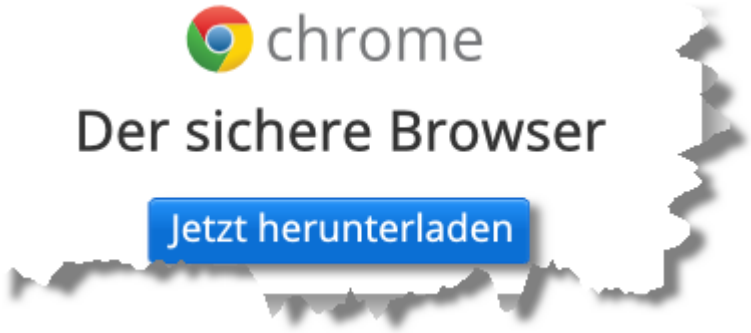
Wie ernst Google sich selbst nimmt, zeigt das jüngste Update von Google Chrome. Die Sicherheitslücke ist weiterhin vorhanden, man denkt nicht im entferntesten daran, die Passwörter der Anwender zu schützen.

Fazit *

Nutzen Sie **niemals** die Funktion zum Speichern von Passwörtern in Google Chrome!

Dann lieber den altmodischen Zettel auf dem Schreibtisch, der landet wenigstens nicht plötzlich in der Cloud!

Die Argumentation von Google lässt indessen Böses erahnen. Wenn man im Zusammenhang mit diesen wirklich sensiblen Daten des Anwenders bereits derart argumentiert, wie sieht es dann mit dem Schutz der Daten anderer Google Dienste aus. Google Drive, Google Mail, …. Warum diese Daten verschlüsseln und absichern? Das wäre doch trügerische Sicherheit? Oder, Herr Google?



Werbung vom 22.08.2013 auf chip.de 2