LinkedIn wurde 2012 Opfer eines breit angelegten Hackerangriffs.

Die Beute der Hacker: **167.370.940** Zugangsdaten. Darunter auch etwa **117 Millionen Passwort-Hashwerte** (*SHA-1*). Soweit so gut, der Diebstahl liegt inzwischen gut 4 Jahr zurück. Wen interessiert das noch?

Das Problem: Zugangsdaten werden jetzt im Darknet (*unter TheRealDeal*) für 2000 EURO angeboten. Darunter anscheinend auch zahlreiche Passwörter. Schuld daran ist die wirklich stümperhafte Pseudoabsicherung der Passwörter. Man verwendete SHA1 und verzichtete zudem noch auf einen s.g. SALT-Wert.

Ohne Salz schmecken nicht nur die meisten Speisen fade, es macht Hackern auch noch das Leben leicht. Man kann vom Hashwert leider auf das Passwort zu schließen.

**siehe dazu**: Schlüssel, Salz und Regenbogen

> Jetzt wird es ernst für alle LinkedIn Anwender!

Auch wenn man sein LinkedIn Passwort geändert hat, sollte man ganz tief in sich gehen und prüfen, ob man das Passwort für LinkedIn entgegen aller Ratschläge, auch für andere Zwecke eingesetzt hat. Falls ja, dann ist es höchste Eisenbahn die entsprechenden Passörter und Zugangsdaten zu ändern und das eigene Konzept zu überdenken!

Denn eine Grundregel lautet: **Verwende ein Passwort nie an mehreren Stellen.**

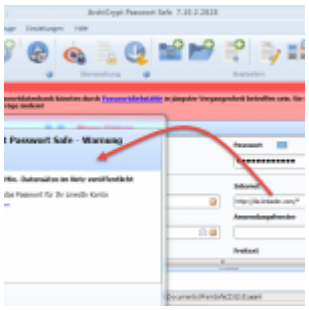
Weitere Tipps und Hinweise zum Umgang mit Passwörtern finden Sie im Artikel Wie sicher ist mein Passwort?

Eine weitere Unannehmlichkeit wartet. Die zum Kauf angebotenen Daten enthalten natürlich E-Mail Adressen. Diese werden anscheinend aktuell in großem Umfang genutzt, um manipulierte und verseuchte E-Mails mit Anhang an die LinkedIn Kunden zu senden. Sehr gefährlich auch für diejenigen, die gar nicht mehr bei LinkedIn sind. In den E-Mails erfolgt eine persönliche Ansprache inkl. Nennung der Position im Unternehmen. Den E-Mails sind Word-Dokumente angehängt, die man keinesfalls öffnen sollte!

Anscheinend wurde auch Mark Zuckerberg Opfer. Eine arabische Hackergruppe knackte kurzerhand Zuckerbergs Twitter und Pinterest Account. Offensichtlich hatte auch Herr Zuckerberg den **Kardinalfehler** begangen und **ein Passwort an mehreren Stellen**

verwendet.



ArchiCrypt Passwort Safe warnt bei Datendiebstahl und Hackerangriffen

Wenn Sie ArchiCrypt Passwort Safe besitzen, wurden Sie frühzeitig gewarnt. Der Passwort Safe warnt nicht nur allgemein, sondern markiert auch potenziell betroffene Einträge und fordert zur Änderung der entsprechenden Passwörter auf.

**Fazit:**

1. Falls Sie LinkeIn Opfer sein könnten!, reagieren Sie und ändern Sie das Passwort.
2. Falls Sie das Passwort tatsächlich auch an anderer Stelle verwendet haben, dann handeln Sie und ändern Sie die Passwörter.
3. Falls 2 zutrifft, überdenken Sie Ihr Konzept!