2012/24 dschungel

https://jungle.world/artikel/2012/24/123456

123456

Von **Elke Wittich und Boris Mayer**

<none>

Am 6. Juni 2012 sollen Hacker die Server des Karrierenetzwerks Linkedin angegriffen und die Passwörter der Mitglieder im Internet veröffentlicht haben. Krise als Chance! Der (angebliche) millionenfache Diebstahl von Linkedin-Passwörtern ist natürlich zunächst einmal nicht gut. Gleichwohl bietet er die Möglichkeit, sich ein echt schickes neues Hobby zuzulegen, nämlich nachzusehen, was Menschen, die in einem Karrierenetzwerk angemeldet sind, eigentlich für Passworte benutzen, beziehungsweise ob sie sich eigentlich für die Sicherheit ihrer Daten interessieren.
Denn kurz nach dem mutmaßlichen Diebstahl boten gleich mehrere Websites einen besonderen Service für potentielle Opfer an. Die entwendeten Zugangswörter wurden nämlich bei Linkedin anscheinend per SHA-1 verschlüsselt und auch als solche von den angeblichen Hackern veröffentlicht. Welche der langen Zeichen- und Buchstabenfolgen nun für das eigene Passwort steht, ist also für eventuelle Opfer gar nicht so leicht herauszufinden. Auf diversen Websites wird nun angeboten, einfach das eigene Passwort in eine Eingabemaske zu schreiben – der ausgegebene SHA1-Wert werde dann automatisch mit der Liste der Hacker verglichen, so dass man sofort erfährt, ob man sich nun Sorgen machen muss oder nicht.
Natürlich sollte man niemals so blöde sein, ein real existierendes Passwort irgendwo einzugeben, aber man kann ja mal prüfen, was für Zugangsbegriffe weltweit so verwendet werden. Der Klassiker »123456« wird zum Beispiel umgehend mit einer roten Warnmeldung versehen – wie übrigens auch »Iamstupid«, »Password« oder »Schalke04«. Wo soll das noch hinführen?
Auch wenn die Linkedin-User viele Unsinnsbegriffe für ein sicheres Passwort hielten, eines ist jedoch klar: »Ihatemypassword« wird als unbedingt sicheres Zugangswort eingestuft.