

POV: Emailzugang gehackt, Passwort geändert, Kontaktadresse geändert

Beitrag von „Volker_D“ vom 17. August 2024 00:04

Ja, knacken kommt immer wieder vor. Bei mir sind die Passwörter bei kickstarter, dropbox und einem anderen Forum geknackt worden. Zeigt auch der schon oben verlinkte Leakchecker von openHPI an.

E-Mail ist übel. Da würde ich bei ALLEN Diensten prüfen bzw. bei ALLEN Diensten neue Passwörter erstellen.

Warum: Wenn ich als Hacker Zugriff auf das E-Mailkonto hätte, dann würde ich mal gucken welche Dienste derjenige so nutzt oder einfach ausprobieren und dann dort ein neues Passwort anfordern (Auf "Ich habe das Passwort" vergessen klicken und mir ein neues zuschicken lassen).

Anschließend würde ich diese Mail löschen (auch im Mülleimer), sodass es nicht so schnell auffällt.

Bezüglich Hash: Korrekt. Passwörter werden normalerweise nicht im Klartext gespeichert, sondern nur ein Hash davon.

Da gibt es verschiedene Hashalgorithmen. Vor Jahren hat man z.B. MD5 benutzt. Wenn sich jemand also z.B. in einem Forum mal vor Jahren angemeldet hat und es dann nie mehr besucht hat, dann wird dort das Passwort immer noch nur mit MD5 gehashed rumliegen. Auf einen neuen Algorithmus kann man es nicht mal so eben ändern, weil der Datenbankbetreiber ja das Passwort selbst nicht kennt.

Dummerweise ist es heute möglich, solche Passwörter dann doch relativ schnell herauszufinden. (Genaugenommen könnte es sogar sein, dass dein Passwort "123" lautet, aber zufälligerweise das Passwort den gleichen Hash erzeugt wie das Passwort "xyz". Dann kann man sich auch mit "xyz" einloggen!)

Damit es schwerer wird, wird das ganze normalerweise mit einem "Salt" erschwert. Das Passwort wird um weitere Buchstaben erweitert, die sich die Datenbank zufällig ausgedacht hat (die sind aber auch in der Datenbank abgespeichert). Es ist aber nur eine Frage der Zeit, bis man das geknackt hat.

Doof ist es für die Leute, die zum Beispiel verschiedene Passwörter bei verschiedenen Diensten haben und sich dadurch sicher fühlen, aber sie es nicht sind. Z.B., wenn ich bei ebay "123ebay" als Passwort habe. Ist der Hash durch ausprobieren geknackt worden, dann ist die Wahrscheinlichkeit sehr groß, dass man bei Amazon mal "123amazon" erfolgreich ausprobieren

kann. Insofern können im schlimmsten Fall alte Passwörte sehr schnell dafür verantwortlich sein, dass auch neue/andere Passwörte unsicher sind.