

Link: <https://www.computerwoche.de/a/nur-jedes-vierte-passwort-ist-sicher,2502205>

Empfehlungen zur Passwort-Security

Nur jedes vierte Passwort ist sicher

Datum: 05.01.2012
Autor(en): Klaus Manhart

Die Sicherheit typischer Passwörter hat sich in den letzten zwei Jahren kaum verbessert. 77 der 100 häufigsten Passwörter aus 100.000 untersuchten Datensätzen ließen sich mit einem einfachen Online-Service innerhalb von zehn Minuten entschlüsseln. Die Folgerung: Passwortsicherheit muss vor allem durch Unternehmensrichtlinien geregelt werden.

Table 1: 15 Most Common Password from FilmRadar.com

Password popularity rank	Password	Number of Occurrences
1	Blink123	1578
2	Greatday1	441
3	Gendut80	436
4	Sample123	420
5	Baobao87	375
6	Matttt24	309
7	Speak2me	261
8	ABcd1234	252
9	[not found]	245
10	abcd1234	215
11	Sara2000	194
12	blueU1234	179
13	Tgold1973	165
14	Hello123	146
15	Timetoget1	144

Verschlüsselung ist gut, nützt aber nichts, wenn die Passwörter einfach zu erraten sind: Die 15 meist verwendeten Passwörter bei Filmradar.com.

Foto: Imperva

Unternehmens-Datenbanken sind durch mangelhafte Passwörter hochgradig gefährdet. Das zeigt der neueste **HII-Report 95**¹ des Datensicherheits-Spezialisten Imperva. Die Studie hat 167 Passwörter untersucht, die durch ein aktuelles Datenleck an die Öffentlichkeit kamen. Betroffen davon waren die Zugangsdaten der Webseite FilmRadar.com.

Die Daten waren durch die SHA1-Hashfunktion - eine übliche Verschlüsselungstechnik für Passwörter - gesichert. Die Verschlüsselung ist allerdings in der Praxis irrelevant, wenn die hinterlegten Informationen einfach zu erraten sind - was bei den untersuchten Passwörtern erstaunlich oft der Fall war: Die meisten der 100 populärsten Passwörter ließen sich mit Hilfe sogenannter Rainbow-Tabellen innerhalb von wenigen Minuten erraten. Zusammen machen sie rund zehn Prozent des gesamten Datenbestandes aus.

Immerhin fünf Prozent der Passwörter hielten einem Wörterbuchangriff nicht einmal zwei Minuten stand - bei einer Datenbasis von 100.000 Benutzer sind dies 2.000 Zugangsdaten, auf die Hacker praktisch frei zugreifen können. Die meisten der 15 populärsten Passwörter ließen sich durch solche Methoden extrem einfach entschlüsseln.

Empfehlungen für Passwortsicherheit

Und so schützen Sie Datenbanken und andere unternehmensrelevante Informationen:

- **Rainbow-Tabellen "versalzen"**: Unternehmen, die sich für den Schutz von Kundenpasswörtern nur auf die SHA-1-Hashfunktion verlassen, machen es Hackern einfach. Die simple Verschlüsselung lässt sich mit Rainbow-Tabellen, die teilweise frei im Internet verfügbar sind, leicht überwinden. Ein effektiver - wenn auch nicht unüberwindbarer - Schutz dagegen ist "Salting". Ein sogenannter Salt-Wert ist eine zufällige Zahl, die dem Passwort vor der Verschlüsselung hinzugefügt wird. Das Ergebnis: Der Entschlüsselungsaufwand steigt exponentiell.
- **Lange Passwörter erlauben**: Die Verwendung längerer Passwörter - im besten Fall sogenannter "Pass-Phrasen" - verbessert die Sicherheit. Gleichzeitig erlauben längere Zugangsdaten leichter zu merkende Kombinationen, so dass die Mitarbeiter sich keine Zettel schreiben und an ihren Bildschirm kleben müssen.
- **Eine starke Passwort-Richtlinie vorgeben**: Diese sollte nicht nur bestimmte Zeichentypen vorgeben, sondern die gewählten Kombinationen auch mit Hacker-Wörterbüchern vergleichen. Hotmail beispielsweise erlaubt seit kurzem keine verbreiteten Passwörter mehr. Auch seitenspezifische Begriffe sollten überprüft und eingeschränkt werden.

"Unternehmen können sich bei der Wahl sicherer Passwörter nicht auf Mitarbeiter und Kunden verlassen", heißt es in der Studie. "Unsichere Passwörter bergen immer das Risiko eines Imageverlustes - daher sollten entsprechende Richtlinien die Endanwender dabei unterstützen, ihre eigenen Daten ausreichend abzusichern. Wir empfehlen Unternehmen, Passwörter als sehr wertvolle Informationen zu betrachten - und diese Einschätzung in ihren Datensicherheitsrichtlinien auch praktisch umzusetzen."

Der vollständige Report ist **hier**² abrufbar.

Links im Artikel:

¹ http://www.imperva.com/docs/HII_Enterprise_Password_Worst_Practices.pdf

² http://www.imperva.com/docs/HII_Enterprise_Password_Worst_Practices.pdf

eingesandte Manuskripte, Fotos und Illustrationen. Für Inhalte externer Seiten, auf die von dieser Webseite aus gelinkt wird, übernimmt die IDG Tech Media GmbH keine Verantwortung.