BearingPoint®

Die 5 goldenen Regeln für einen sicheren Umgang mit Passwörtern

Tipps eines Pentesters zum Thema Passwortmanagement

Einfallstor Passwort

Über 80% der Breaches werden durch unsichere Passwörter verursacht

Vor kurzem habe ich versucht mich bei einer Website anzumelden, die ich schon lange nicht mehr verwendet habe. Leider wusste ich das Passwort nicht mehr, deshalb habe ich die „Passwort vergessen“ Funktion verwendet. In der E-Mail, die ich daraufhin bekommen habe, war kein Link zum Zurücksetzen des Passworts, sondern mein altes Passwort. Im Klartext. Passwörter sollen nie in einer unverschlüsselten E-Mail gesendet werden. Zudem sollte die Seite mein Passwort gar nicht im Klartext haben, sondern nur in gehashter Form. Dieser Vorfall hat mich motiviert hier ein paar Grundsätze für richtiges Passwortmanagement zu schreiben.

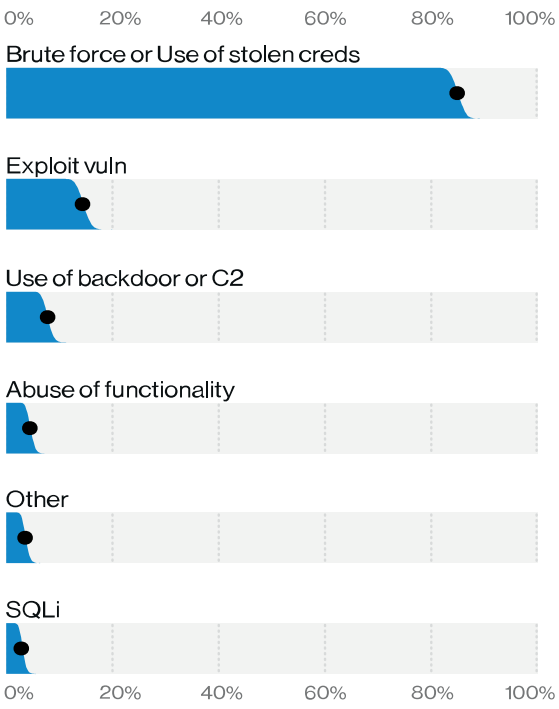

Abbildung 1: Hacking Methoden die zu Breaches geführt haben (Quelle: https://enterprise.verizon.com/resources/reports/dbir/2020/results-and-analysis/)

Der „Data Breach Investigations Report 2020“ von Verizon zeigt, dass in über 80% der Breaches, die durch Hacking verursacht wurden, gestohlene oder erratene Passwörter verwendet wurden.

Diese fünf goldenen Regeln sollten für sicheres Passwortmanagement unbedingt beachtet werden:

1. Starke Passwörter verwenden

Das ist der wohl bekannteste Grundsatz, wenn es um Passwörter geht.

Wichtig ist, dass lange Passwörter verwendet werden. Ein Passwort, dass zwar komplex ist, aber kurz, bietet nicht genügend Sicherheit.

Sicherheitsstandards wie der OWASP ASVS schreiben vor, dass ein Passwort mindestens 12 Zeichen lang sein sollte.

Um für ausreichend Komplexität zu sorgen, kann ein Mix aus Großbuchstaben, Kleinbuchstaben, Zahlen und Symbolen verwendet werden. Desweiteren soll man keine Passwörter verwenden, die häufig verwendet werden (z.B. Passwort1!), da diese durch eine Dictionary-Attack (ein Angriff bei dem ein „Wörterbuch“ an möglichen Passwörtern verwendet wird) erraten werden können. Am besten, man verwendet eine Passphrase, wie z.B. MeinAutoHat120PS. (inklusive des Punkts).

Zusätzlich soll für jede Anwendung ein eigenes Passwort verwendet werden. Da man da schnell den Überblick verlieren kann, empfiehlt es sich einen *Passwort Manager* zu verwenden.

2. Passwörter nicht als Klartext speichern

Um Passwörter bei jedem Login-Vorgang auf ihre Richtigkeit überprüfen zu können, müssen sie irgendwo gespeichert sein.

Wichtig hierbei ist, dass Passwörter nie als Klartext gespeichert werden dürfen. Passwörter müssen durch eine Einweg-Verschlüsselungsfunktion (Hash) unkenntlich gemacht werden.

Der Vorteil einer Hash-Funktion ist, dass man sie nicht rückgängig machen kann. Es ist also keine Verschlüsselung, die man wieder entschlüsseln kann, sondern funktioniert nur in eine Richtung.

Um für zusätzliche Sicherheit zu sorgen, werden die Hashes „gesalzen", also mit einem zusätzlichen, zufälligen Wert versehen. Dadurch können Brute-Force Angriffe verhindert werden.

3. Multifaktor Authentifizierung

Multifaktor Authentifizierung (MFA, auch 2-Faktor Authentifizierung 2FA) bedeutet, dass zum Anmelden mindestens zwei verschiedene Faktoren benötigt werden.

Es gibt Wissensfaktoren (z.B. Passwort, PIN, usw.), Besitzfaktoren (z.B. Smartphone, Token, etc.) und Biometrie-Faktoren (z.B. Fingerabdruck, Gesichtserkennung, ...).

MFA erhöht die Sicherheit enorm. Für Angreifer ist es beinahe unmöglich, MFA zu brechen.

Selbst wenn Zugangsdaten gestohlen oder geleakt wurden können sie nicht verwendet werden, da der zweite Faktor immer noch Schutz bietet.

4. User Experience beachten

Sicherheit und Usability werden oft als Gegensätze gesehen. Das muss und soll aber nicht so sein.

Verschiedenste Sicherheitsmaßnahmen, die in der Vergangenheit als notwendig gegolten haben, führten aufgrund von fehlender Usability zu noch größeren Schwachstellen.

Ein gutes Beispiel dafür ist das häufige Ändern des Passworts.

Früher ging man davon aus, dass dadurch ein gestohlenes Passwort zumindest nicht lange gültig ist. Das häufige Ändern führt aber dazu, dass Passwörter mit bestimmtem Muster angelegt werden (z.B. wird häufig die Monatszahl am Ende des Passworts angehängt). Hat ein Angreifer ein Passwort, ist es ein leichtes das nächste zu erraten.

Zudem führt das häufige Ändern dazu, dass Benutzer sich Passwörter aufschreiben.

Heutzutage ist die Empfehlung, das Passwort nicht zu häufig zu ändern. Einmal pro Jahr ist ausreichend.
Zusätzlich muss ein Passwort immer geändert werden, wenn Verdacht besteht, dass es gestohlen wurde. Hierzu können Dienste hilfreich sein, die Datenleaks nach E-Mail Adressen durchsuchen (wie zum Beispiel haveibeenpwned.com).

Weitere Maßnahmen, die die User Experience und Sicherheit verbessern sind:

- Copy/Paste erlauben: manche Seiten erlauben es nicht, einen Wert in das Passwort-Feld zu kopieren. Da generell Passwortmanager verwendet werden sollten, soll auch das Kopieren des Passworts vom Passwortmanager zum Passwortfeld ermöglicht werden.

- Passwort anzeigen Funktion: Dadurch kann ein Benutzer sein eingegebenes Passwort kurz sehen, um mögliche Tippfehler auszubessern. Dadurch wird es Benutzern einfacher gemacht, lange Passwörter fehlerfrei einzugeben. Muss man jedes Mal von vorne zu Tippen beginnen, wenn man einen Fehler macht, ermutigt das nur dazu kürzere Passwörter zu verwenden.

5. Benachrichtigungen

Bei jeder „auffälligen“ Tätigkeit soll der Benutzer benachrichtigt werden.

Wird z.B. ein Passwort geändert oder zurückgesetzt, soll der Benutzer entsprechend darüber informiert werden.
Wurden vermehrt Login-Fehlversuche registriert, soll der Benutzer informiert werden.
Ist ein Login aus einem anderen Land erfolgt, soll der Benutzer informiert werden.

Dadurch gibt man dem Benutzer die Möglichkeit, bei Auffälligkeiten einzugreifen, und z.B. sein Passwort zu wechseln.

Abschließend gilt zu sagen:

Befolgt man diese Grundregeln, ist man schon auf einem guten Weg für mehr Passwortsicherheit.

Für weitere bzw. genauere Richtlinien gibt es Standards wie z.B. den OWASP ASVS.

Wir helfen gerne beim Umsetzen und Testen davon.

https://pentest.at/

Österreichs größtes Management- und Technologieberatungsunternehmen

Mit mehr als 500 Mitarbeitern in Österreich entwickeln wir innovative Strategien für neue und bestehende Geschäftsmodelle und konzipieren und implementieren digitale Lösungen und Services für führende Unternehmen und öffentliche Institutionen.

Mit unseren Kompetenzen in den Bereichen Managementberatung, agile Transformation, technologiebasierte Business Services und smarte BearingPoint Softwarelösungen entwickeln wir gemeinsam mit unseren Kunden und Partnern innovative Geschäftsmodelle.

Zu den Kunden von BearingPoint zählen die führenden Unternehmen und Organisationen Österreichs. Das globale BearingPoint-Netzwerk mit mehr als 10.000 Mitarbeitern unterstützt Kunden in mehr als 75 Ländern und engagiert sich aktiv für messbare und nachhaltige Geschäftserfolge.

Für mehr Informationen besuchen Sie unsere Website: bearingpoint.services oder www.bearingpoint.com

BearingPoint®