Benutzernamen und Passwörter – ein leidiges Thema

Man sollte glauben, die Zeiten der in gelben Zetteln am Bildschirmrand angebrachten Benutzernamen und dazugehöriger Passwörter sei vorbei. Doch die Zahl der zu verwaltenden Login-Daten nimmt immer weiter zu. In diesem Fachartikel werden Dos and Dont´s, Tipps und Tricks bei der Verwaltung dieser wichtigen Daten beschrieben. Sie lassen ja auch nicht absichtlich die Haustüre offen, oder?

Einleitung

Die Verwendung von Login-Daten ist eine absolut notwendige, aber lästig gewordene Pflicht zum Schutz vor unbefugtem Zugriff auf IT-Systeme. Während vor 10-15 Jahren maximal ein bis zwei Kennwörter zu merken waren, so hat der durchschnittliche Benutzer mittlerweile leicht den Zugang zu zwei Dutzend verschiedenen Diensten zu verwalten.

Regelmäßige Meldungen über Millionen von gehackten Benutzeraccounts und entwendeten Kennwörtern bei Facebook, Yahoo oder Ebay etc. sollten zu denken geben. Mittlerweile existieren im Netz Tabellen mit über 500 Millionen Einträgen (sog. Rainbow-Tables). Mit diesen Tabellen und heutigen leistungsfähigen Grafikkarten können so mehrere Millionen Passwörter pro Sekunde gesucht und in kurzer Zeit geknackt werden.

Sicherheitscheck

Um zu prüfen, ob ein verwendeter Benutzeraccount kompromittiert oder das Passwort geknackt wurde, werden folgende Dienste empfohlen. Für Benutzernamen verwenden Sie:

https://haveibeenpwned.com/

Passwörter prüfen Sie unter

https://haveibeenpwned.com/Passwords.

Die genannten Dienste sind sicher, ihr zu prüfenden Daten werden verwürfelt und verschlüsselt übertragen und gegen vorliegende Tabellen (einer Art Blacklist) geprüft. Werden Ihr Passwort oder die verwendete Benutzerkennung gefunden, so sind sie bei einer Attacke in unberechtigte Hände gefallen. Für alle betroffenen Benutzerkennungen ist es dann an der Zeit, sich ein neues Passwort zu suchen. Kompromittierte, schon bekannte Passwörter müssen gewechselt werden und sind keinesfalls wieder zu verwenden.

Prinzipien

Welche Grundprinzipien sicherer Verwaltung von Benutzernamen und Passwörtern sollten beachtet werden:

1. *Ausreichend lange Kennwörter*

Kennwörter müssen mindestens eine Länge von 10 Zeichen oder mehr haben. 10 Zeichen ist dzt. ein Grenzwert, bei der das Errechnen (= Brute-Force Attacken) eines Kennwortes mit handelsüblichen Rechnern noch Jahre dauert.

2. *Keine gleichen Kennwörter*

Verwenden Sie keine gleichen Kennwörter für verschiedene Dienste. Wurde dieses Passwort kompromittiert, so ist ein Einbruch bei anderen Diensten ein Leichtes.

3. *Keine Speicherung von Kennwörtern in Browsern*

Speichern Sie niemals Benutzerkennungen und Passwörter in von Internet-Browsern angebotenen Kennwortmanagern. Das ist sehr unsicher. Und speichern sie schon gar nicht auf Mobiltelefonen oder Tablets, da deren Betriebssysteme kein ausreichendes Sicherheitsniveau bieten.

4. *Zwei-Faktor-Authentifizierung verwenden*

Bei allen Anwendungen mit hohem finanziellem Risiko (Online-Banking, Zahlungsdienstleistungen,

Kreditkartentransaktionen, digitale Signaturen) muss der Zugriff mit einer Zwei-Faktor-Authentifizierung erfolgen.

Hier wird über einen unabhängigen Kanal eine SMS mit einer TAN gesendet, es muss eine Chipkarte in einen Leser gesteckt werden, der Fingerabdruck, ein Gesichts- oder Irisscan ist notwendig oder die Präsenz eines Tokens bzw. Mobiltelefons mit NFC/RFID-Chip wird nachgewiesen. Erst dann ist ein Login oder eine Zahlung in Verbindung mit einem Passwort möglich. Single-Sign-On-Systeme in Unternehmen, bei denen eine Anmeldung Zugriff auf alle Applikationen gewährt, sollten zwingend mit einer Zwei-Faktor Authentifizierung ausgestattet werden, da hier gleichzeitig auf mehrere Systeme zugegriffen werden kann.

5. *Keine Banking Apps und nur absolut notwendige Apps auf Mobilgeräten*

Die Software auf Mobiltelefonen und Tablets gleicht einem fragilen Flickwerk, da Hersteller Sicherheitsupdates nur verzögert oder gar nicht liefern. Der Support wird nach längstens 2 Jahren meist eingestellt. Je günstiger das Mobilgerät desto schlechter die Versorgung.

Wurde ihr Mobiltelefon gehackt, so hat der Angreifer meist Kontrolle über alle Apps und die damit verbunden automatischen Logins. Eine eingestellte Zwei-Faktor-Authentifizierung über SMS ist wirkungslos, denn der Angreifer liest gleich alle benötigten Informationen für zB eine Überweisung direkt mit. Das ist der Grund, warum Applikationen für Internetbanking nicht auf dem Mobiltelefon laufen sollten.

6. *Keine Verwendung von Facebook oder Google Logins für andere Dienste*

Diverse Dienste bieten den Nutzern an, ihre Facebook- oder Google-Accounts als Login-Daten zu verwenden. Das ist nicht empfehlenswert, denn diese ermöglichen den riesigen Datenkraken unerwünschte Trackingmöglichkeiten.

Erfolgt der Zugriff auf viele Dienste über einen dieser Anbieter, so bedeutet die Kompromittierung eines Systems Zugriff auf alle damit geschützten Systeme, außer eine Zwei-Faktor-Authentifizierung wird verwendet.

7. *Keine Verwendung von Sicherheitsfragen und Hinweisen auf das Kennwort*

Die Verwendung von Sicherheitsfragen oder Kennworthinweisen stellt nur eine weitere Angriffsmöglichkeit für geschickte Hacker dar. Bei Social Engineering oder Pentesting-Angriffen gelingt es beauftragten Sicherheitsfirmen oft, Zugriff über diesen Weg zu erhalten, nachdem vorher über Social Media zur Person recherchiert wurde.

Risikominimierung - Passwortmanager

Wie kann man die vorgenannten Prinzipien bequem umsetzen, ohne sich das Leben schwer zu machen oder auf der anderen Seite ein zu hohes Risiko einzugehen?

Die Empfehlung lautet, einen Passwortmanager zu verwenden.

Unlängst habe ich in meinem Kennwortmanager nachgezählt und bin auf über 70 gespeicherte Einträge mit Benutzernamen, Kennwörtern und PINs gekommen.

Früher hatte ich für viele dieser Anmeldungen die gleiche oder ähnliche Benutzernamen oder Kennwörter. Nachdem dies aber eine risikoreiche Vorgehensweise darstellt, erstellt die og. Software perfekt zufällige, lange Kennwörter automatisch. Das Eintippen dieser komplizierten Zeichenfolgen erfolgt durch das Programm bei einer Anmeldung. Hierzu gibt der Benutzer im Programm die Anweisung und wie von Geisterhand werden Benutzername und das Passwort eingetippt.

Ein weit verbreitetes Programm ist die freie Software KeePass, (https://keepass.info/). Als Open Source-Software ist sie gut gegen Fehler geprüft

und sehr flexibel mit Plugins zu vielen Anwendungen erweiterbar.

Es existieren etwa 15 weitere Anbieter die Kennwörter Offline oder in der Cloud speichern. Eine reine Speicherung in der Cloud wird nicht empfohlen. Die robusteste Variante ist eine Mischung aus einer in der Cloud und einer lokal gespeicherten Datenbank. Bei nur lokaler Speicherung achten Sie bitte auf ein gutes Backup.

Zusammenfassung / Conclusio

Die vorgenannten Maßnahmen stellen eine gute Praxis im Umgang mit Login-Daten dar, die Risiken sehr stark vermindert. Im privaten Bereich und auch im Unternehmensumfeld sind Sie leicht umsetzbar.

Für weitergehende Betrachtungen wird auf die Publikation „Digital Identity Guidelines" des US National Institute of Standards and Technology unter **https://doi.org/10.6028/NIST.SP.800-63-3** verwiesen.

Das Um und Auf stellen Awareness-Trainings und Schulungen aller Mitarbeiter dar. Die Faktoren Unwissen, Zeitmangel, Gewohnheit und Unachtsamkeit sind die größten Risikofaktoren im Bereich der Informationssicherheit.

Mag. Markus Lenotti, Dezember 2018
Geschäftsführer
Lenotti Advisors GmbH