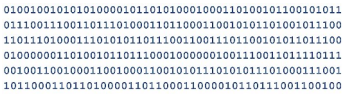
JENS BERGGREN IT-Dienste
Hugo-Klemm-Str. 61 • 21075 Hamburg
+49 40 3280 9983 https://jbdv.de



jens berggren

Passworte sind lästig aber immer noch notwendig. Es gibt zwar Lösungen wie Smartcards oder sogenannte Token, wir werden aber wohl nie für alle Zwecke derartige Techniken verwenden können.

Die meisten Menschen verfügen nicht über ein fotografisches Gedächtnis, was viele veranlasst, immer dasselbe Passwort für alle Systeme, Dienste und Anwendungen zu verwenden.

In Zeiten, in denen es nahezu in jeder Woche eine Meldung über geknackte oder kompromittierte Foren, Shops und sonstige Webanwendungen gibt oder plötzlich Datenbanken mit Millionen Benutzerkonten im Internet auftauchen, ist die Verwendung von nur einem Passwort für alle Anmeldungen hochriskant.

Im Folgenden möchte ich Sie für den Umgang mit Passworten sensibilisieren und Tipps geben.

Recycling von Zugangsdaten?

Beispiel:

Herr Merkmirnichts hat ein Benutzerkonto bei kochdenbrei.de [1)], wo er seine Nudelsuppenrezepte ins Netz stellt. Bei der Registrierung hat er als Benutzernamen sein E-Mail-Konto beim Freemail-Provider kostnixmailmitspamweb.de [1)] merkmirnichts@kostnixmailmitspamweb.de und als Passwort 123456 angegeben.

Seine Anmeldedaten merkmirnichts@kostnixmailmitspamweb.de mit dem Passwort 123456 nutzt er auch bei einem großen Onlinehandel, der auch seine Kreditkartendaten gespeichert hat.

Nun wird kochdenbrei.de [1)], die wenig Geld für Administratoren ausgeben und sich nicht um Sicherheitsupdates und andere technische Pflege ihrer Website kümmern, von Kriminellen geknackt. Die erhalten durch ihre Aktion 25.000 Zugangskonten. Diese Konten probieren sie nun bei den großen Anbietern von Webshops und Onlinehandel durch. Wenige Tage später erhält Herr Merkmirnichts seine Kreditkartenabrechnung und wundert sich …

[1)] Die verwendeten Domänennamen waren bei Erstellung dieses Beitrages nicht registriert.

JENS BERGGREN IT-Dienste
Hugo-Klemm-Str. 61 • 21075 Hamburg
+49 40 3280 9983 https://jbdv.de

Was kann ich tun?

1) Für jeden Anwendungsfall muss ein eigenes Kennwort angelegt werden.

2) Das Kennwort muss "stark" sein, d. h. es sollte mindestens 10, besser 14 oder mehr Stellen haben und eine Zusammensetzung aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen sein. Hier ist die Länge wichtiger, als die Komplexität, wobei 25 Nullen hintereinander nicht sehr sicher sind, der leicht geänderte Anfang eines Gedichtes / Liedes mit eingestreuten Zahlen und Sonderzeichen schon. **Beispiel:** "Der Mond ist untergeg8ngen, d!e gruenen Sternle!n sangen777.

3) Passworte gehören nicht auf einen Zettel, der irgendwo unter der Schreibtischablage oder in der Schublade liegt oder auf einem Backezettel am Monitor prangt. Passworte gehören sicher verwahrt. Und wie merke ich mir das?

Und wie merke ich mir das?

Es gibt Empfehlungen von öffentlichen Stellen, dass man sich einen Zettel mit Passworten / Zugangsdaten in die Brieftasche legen soll. Das ist äußerst fragwürdig. Dann landet auch die PIN für die EC-Karte in der Brieftasche, wovor dieselben öffentlichen Stellen immer warnen.

Benutzen Sie sogenannte Passwortdatenbanken; die speichern alle Zugangsdaten in einer verschlüsselten Datei. Diese Datei ist nur zu öffnen, wenn ein vorher festgelegtes starkes Passwort eingegeben wird. Wenn Sie dieses Passwort vergessen, kommen Sie auch selbst nicht mehr an die Daten. Sollten Sie hier Befürchtungen haben, schreiben Sie dieses starke Passwort auf und bewahren die Aufzeichnung an einem sicheren Ort auf.

Meine Empfehlung lautet hier "KeePass© Password Safe" von Dominik Reichl. Das ist eine freie, quelloffene Software, die Ihre Passworte sicher verschlüsselt, vorausgesetzt, Sie haben ein starkes Passwort für Ihre Datenbank verwendet. Je nach Situation macht es evtl. Sinn, die Datenbank auf einem USB-Stick mit zu speichern und nicht auf dem PC, aber denken Sie an ein Backup!

JENS BERGGREN IT-Dienste
Hugo-Klemm-Str. 61 • 21075 Hamburg
+49 40 3280 9983 https://jbdv.de

Passworte weitergeben?

Sofern personengebundene Nutzerkonten im Betrieb verwendet werden, ist eine Weitergabe von Passworten nicht OK. Auch wenn es in der aktuellen Situation scheinbar nicht anders geht!

Ich möchte hier nur einmal das Stichwort Mobbing nennen, oder auf die Vorgänge in hessischen Polizeirevieren in vergangenen Jahren hinweisen[2)].

Was kann man tun?

In den meisten Fällen der Passwortweitergabe geht es um Krankheitsausfälle oder Urlaubssituationen. Dem kann durch Vertretungen und entsprechende Freigaben begegnet werden, es ist nur eine Frage der Organisation. Sprechen Sie Ihre IT dazu an.

Im betrieblichen Ablauf ist die Passwortweitergabe nicht in Ordnung!

Windows® Passwort ändern

Viele wissen offenbar nicht, wie das Windows® Passwort geändert werden kann.

Deshalb an dieser Stelle die einfachste Möglichkeit:

Drücken Sie gleichzeitig die Tasten STRG + ALT + ENTF, dann erhalten Sie eine Auswahl, die u. a. den Punkt "Kennwort ändern" enthält. Diese wählen Sie aus, anschließend müssen Sie einmal das aktuelle Kennwort und zweimal das neue Kennwort eingeben. Das war es schon.

Terminalserverbenutzer müssen die Tastenkombination STRG + ALT + ENDE verwenden.

2) Frankfurter Rundschau vom 08.07.2022: „NSU 2.0“: Polizei im Zwielicht
2) FragDenStaat vom 06.10.2023: Der NSU 2.0 war nicht allein