01.02.2019 | Julian Pawlowski | 10 min Lesezeit

State of the Union zum “Ändere-Dein-Passwort-Tag”

Weshalb Passwörter ein Auslaufmodel sind und warum sie uns trotzdem noch lange begleiten werden.

Alle Jahre wieder: Auch 2019 wird am 1. Februar dazu aufgerufen sein Passwort zu ändern. Der „Ändere-Dein-Passwort-Tag“ wirkt jedoch aktuell deplatzierter denn je. Schließlich begegnen uns Leaks über Millionen von Passwörtern in fast schon vorhersagbaren Abständen über das ganze Jahr verteilt.[1] **(https://www.heise.de/security/meldung/Neue-Passwort-Leaks-Insgesamt-2-2-Milliarden-Accounts-betroffen-4287538.html)** [2] **(https://www.heise.de/security/meldung/Passwort-Sammlung-mit-773-Millionen-Online-Konten-im-Netz-aufgetaucht-4279375.html)** So wird auch bei der Berichterstattung zu jedem dieser Vorfälle dazu aufgerufen nicht nur auf unterschiedlichen Webseiten zu **überprüfen (https://haveibeenpwned.com/)**, ob der eigene Account betroffen ist, sondern auch vorsichtshalber das Passwort zu ändern.

Das Thema ist also nunmehr ständig präsent und wird wahrscheinlich von der überwiegenden Mehrheit von Personen nur noch beiläufig beachtet – wenn überhaupt. Nicht zuletzt auch, weil es nicht „das eine“ Passwort gibt. Der Bequemlichkeit geschuldet, wird dasselbe Passwort – trotz aller Warnungen – auch heute noch für mehrere Accounts verwendet. Man müsste also ständig sein Passwort bei einer Vielzahl von Accounts ändern und sich diese auch merken. Daher werden Passwörter dann oft nur leicht modifiziert: Hier und da wird aus einem Kleinbuchstaben ein Großbuchstabe und es wird eine Zahl hoch oder runter gezählt. Wirklich schlau ist das nicht, denn solche Änderungen sind leicht vorhersehbar. Natürlich unter der Voraussetzung, dass man sich zuvor bereits ein halbwegs sicheres Passwort ausgedacht hat und nicht eine Variante der meist verwendeten Passwörter benutzt.

Ein erster Schritt: Die Nutzung von Passwort Managern

Die Lösung für dieses Dilemma dürfte sich schon länger herumgesprochen haben und ist deshalb kein Geheimtipp mehr: Die Verwendung von Passwort Manager Programmen wie beispielsweise **1Password (https://1password.com/)**, **LastPass (https://lastpass.com/)** oder dem kostenfreien **KeePass (https://keepass.info/)** hilft dabei, zufällige Passwörter in komplexer Länge zu generieren und zu speichern. Ein (hoffentlich) ebenso komplexes Passwort, welches dann auswendig gelernt wird, schützt den Zugang zur Passwort Datenbank.

Eine tatsächliche Verbesserung des Schutzes kann ein solches Programm jedoch nur bieten, wenn wirklich *jeder* Zugang dort gespeichert und mit einem solch zufälligen Passwort versehen wird. Aus Bequemlichkeit die Zugänge auszusparen, die man täglich mehrfach verwendet, wäre ein großer Fehler. Insbesondere die E-Mail-Postfächer sind von enormer Bedeutung, da mit Zugriff darauf in der Regel das Passwort für jeden anderen Dienst zurückgesetzt werden kann.

Die Alltagstauglichkeit steht und fällt also damit, wie einfach und bequem sich der Passwort Manager in meinen Alltag integriert. Das bedeutet insbesondere auch, dass die Passwort Datenbank mir auf allen meinen Geräten zur Verfügung stehen muss. Eine Synchronisierung zwischen Geräten ist deshalb essentiell. Idealerweise besteht auch Zugriff über einen Webbrowser. Gleichzeitig erhalte ich dabei auch ein Backup, um zu verhindern, dass mir die gespeicherten Passwörter verloren gehen. Diese redundante und ortsunabhängige Speicherung gilt dann sogar als sogenanntes „Offsite Backup“. Klingt gut!

Dieser flexible Zugang zu meinen Passwörtern stellt an sich natürlich ebenfalls ein Risiko dar. Eine möglichst hohe Stufe der Verschlüsselung richtig (!) umzusetzen ist nicht leicht. Diese zudem mit einer einfach einzustellenden, verlässlichen, schnellen und auch sicheren Synchronisierung zu koppeln, die tatsächlich unabhängig von Geräteherstellern funktioniert, beherrschen nur wenige Passwort Manager. Dabei spielt auch die Art, wie die Daten in der Passwort Datenbank strukturiert und abgespeichert sind, eine zentrale Rolle: Ein Fehler in der Datenbank, beispielsweise durch Fehler in der Synchronisierung, sollte nicht dazu führen können, dass ich gänzlich den Zugriff auf alle darin gespeicherten Passwörter verliere. Eine gewisse Robustheit oder auch Reparaturfunktion ist deshalb hilfreich. Auch sollte genau darauf geachtet werden, welche Daten noch unverschlüsselt einsehbar sind: Metadaten wie die dazugehörige Website sind oftmals trotzdem im Klartext gespeichert. Das muss nicht grundsätzlich ein Problem sein, jedoch sollte einem bewusst sein, dass man trotz Verschlüsselung nicht leichtfertig mit der Passwort Datenbank umgehen sollte.

Ein weiterer, unerlässlicher Punkt ist die Einfachheit bei der Verwendung der gespeicherten Passwörter. Hier trennt sich endgültig die Spreu vom Weizen: Ein guter Passwort Manager unterstützt mich beim Auffinden und der Eingabe des Passwortes auf Webseiten und auch in Applikationen. Macht er das richtig, dann funktioniert die Anmeldung sogar schneller als wenn ich selbst den Benutzernamen und das Passwort eintippen muss. Genau diese geräteübergreifende Bequemlichkeit ist es, die die Akzeptanz eines Passwort Managers ganz enorm definiert.
Die Integration in alle populären Desktop Browser ist quasi bereits Standard. Eine mobile App für Smartphone und Tablet anzubieten trifft ebenfalls die Erwartungshaltung des digitalen Nomaden. Die nahezu nahtlose Integration in mobile Browser und Apps ist jedoch erst seit kurzem tatsächlich überhaupt möglich geworden.
Wer ein iOS Gerät verwendet, kann sich seit Version 12 letzten Jahres über eine direkte Betriebssystem Unterstützung für Passwort Manager freuen. Dies ermöglicht, dass das zentral gespeicherte Passwort bei Passwort Abfragen auf Webseiten und auch in Apps über einen einfachen Tapp zugänglich ist – ein großer Komfort Gewinn, der für mich persönlich noch viel mehr wiegt als die beiläufig verbesserte Sicherheit.

Wer nun bei allen genannten Anforderungen nach einem geeigneten Passwort Manager sucht, dem empfehle ich einmal **1Password (https://1password.com/)** auszuprobieren.

Private und geschäftliche Passwörter

Man sieht schon, die Anforderungen an einen Passwort Manager sind komplexer als sie auf den ersten Blick erscheinen. Kostenfreie Lösungen können diese nur schwer erfüllen. Nimmt man dazu noch an, dass man Passwörter sowohl aus dem privaten wie auch dem beruflichen Bereich hat und diese zusammen verwalten möchte, so wird die Luft tatsächlich dünn.

Unternehmen haben natürlich ein starkes Interesse daran, dass ich meine beruflichen Zugänge von den privaten bestmöglich separiere. Unterschiedliche Passwort Datenbanken zu pflegen ist dabei für viele Anwender schon eine ziemliche Hürde. Aus Unternehmenssicht ist es deshalb ratsam, den Mitarbeiter dabei zu unterstützen, dass er im täglichen Umgang private und auch geschäftliche Zugänge auf dieselbe Weise verwenden kann. Nicht zuletzt profitiert das Unternehmen wie auch die Privatperson von einmal erlerntem Wissen. Anstatt sich unterschiedliche Vorgehensweisen immer wieder erneut erarbeiten zu müssen, lässt sich das Gelernte auch auf andere Bereiche übertragen.
So erreiche ich eine möglichst breite Akzeptanz und verbessere letztlich nicht nur in der Theorie die Sicherheit meines Unternehmens.

Das ist jedoch keine leichte Aufgabe, denn wenn geschäftliche Passwörter auch auf privaten Geräten und private Passwörter auf Firmengeräten gespeichert sind, wirft das eine ganze Reihe Fragen auf, sowohl technologischer als auch rechtlicher und betrieblicher Natur.
Man wird konfrontiert mit komplexen Themen wie Datenschutz, Mobile Device Management und Bring your own device (BYOD), verbunden mit der Erkenntnis, dass Geräte und Daten nicht mehr innerhalb der eigenen und kontrollierten Firmenumgebung genutzt werden und zentrale Schutzmechanismen deshalb nicht mehr greifen. Die Grenzen zwischen Identity Management und Device Management verschwimmen deshalb und es ist absehbar, dass diese untrennbar miteinander verschmelzen werden.

Der zweite Faktor

„Etwas, das ich habe“ plus „etwas, das ich weiß“ – so die etwas vereinfachte Erklärung zum Trend der 2-Faktor-Authentifizierung, oft auch bezeichnet als Multi-Faktor-Authentifizierung oder abgekürzt mit 2FA bzw. MFA.

Während man in vielen Unternehmen bereits seit geraumer Zeit zusätzlich zum Passwort einen Zahlencode eingeben muss, der auf einem kleinen Gerät wie einem **RSA SecurID Token (https://www.rsa.com/en-us/products/rsa-securid-suite/rsa-securid-access/securid-hardware-tokens)** angezeigt wird, so ist diese Grundsatzidee inzwischen auch im Privatbereich fast allgegenwärtig. Sogar die Anmeldung mittels einer Schlüsselkarte, die bei größeren Unternehmen auf dem Firmenausweis bereits mit integriert ist, wird in Form von **Yubi Keys (https://www.yubico.com/why-yubico/for-individuals/)** für engagierte Privatleute erschwinglich. Selbst der wenig erfolgreiche **elektronische Personalausweis (https://de.wikipedia.org/wiki/Personalausweis_(Deutschland)#Der_elektronische_Personalausweis_** schlägt in dieselbe Kerbe (einige Gründe für das Scheitern erkläre ich hier beiläufig gleich mit).

Keine Frage, die Verwendung von spezialisierter Hardware bleibt auch auf absehbare Zeit die beste Methode zur Absicherung. Außerhalb der Unternehmens-IT ist der Einsatz aufgrund der beschränkten Unterstützung bei Dienstanbietern eher rar. Einzig Google lässt inzwischen auch die Registrierung eines Yubi Key als zweiten Faktor zu.

Getrieben von den eingangs erwähnten Passwort Leaks haben die großen **FAMGA (https://www.investopedia.com/news/famga-clever-acronym-faux-diversification/)**'s dieser Welt (auch bekannt als Facebook, Apple, Microsoft, Google und Amazon) erkannt, dass private Daten mindestens genauso schützenswert sind wie Unternehmensdaten. Hatte man bei Unternehmen bisher jedoch definiert, dass ein zweiter Faktor nur dann wirklich als solcher gilt, wenn dieser nicht dupliziert werden kann und unbedingt separat vom ersten Faktor – dem Passwort – aufzubewahren ist, so wich man hier bewusst von diesem Detail ab.

Um es vorweg zu nehmen: Die bedingungslose Empfehlung lautet, diesen zusätzlichen Schutz bei jedem Account zu aktivieren, bei dem es möglich ist. Gute Passwort Manager unterstützen auch hier plattformübergreifend und speichern den Geheimschlüssel zum Generieren des PIN Codes. Außerdem unterstützen sie bei der Eingabe des PIN Codes und reduzieren somit den zusätzlichen Aufwand bestmöglich.
Die gemeinsame Speicherung von Passwort und PIN Code Generator widerspricht streng genommen dem Sinn eines zweiten Faktors, hier gilt es abzuwägen. Die alternative Speicherung in einer eigens dafür vorgesehenen App auf dem Smartphone, meist allgemein als „Authenticator App“ bezeichnet, ist besser, mindert allerdings die Nutzererfahrung auch nennenswert.
Daher gilt das Motto: Besser überhaupt einen zweiten Faktor als gar keinen zweiten Faktor. Für ausgewählte Accounts, insbesondere der Firmenzugänge, verwendet man die App, für alle nicht so kritischen Zugänge darf sich auch der Passwort Manager darum kümmern.

Zudem liegt die Hürde, um eine 2-Faktor-Authentifizierung für jeden einzelnen Account zu aktivieren, ohnehin schon enorm hoch. Nicht immer lässt sich derselbe PIN Generator für mehrere Accounts verwenden. Wer möchte schon einen physischen Schlüsselbund, bestehend aus dutzenden unterschiedlichen PIN-Generatoren, mit sich herumtragen und noch dazu für diese eigens bezahlen? Man sieht schnell, dass diese Lösung in der Masse gar nicht skaliert und die allseits bekannte Lieschen Müller bei allem Misstrauen erst gar kein Interesse hätte diesen zusätzlichen Aufwand zu betreiben. Jedoch gilt auch hier wie bei der Grippeimpfung: Der Herdenschutz ist von entscheidender Bedeutung – je mehr mitmachen, desto besser. Legt man die Hürde also so niedrig und macht die Nutzung so komfortabel wie möglich, erreicht man letztendlich einen viel besseren – da weiter verbreiteteren – Schutz.

Erwähnenswert bleibt außerdem, dass Dienstanbieter die 2-Faktor-Authentifzierung unterschiedlich umsetzen. Teilweise kann der Benutzer aus unterschiedlichen Methoden wählen.

Hier eine Übersicht der Software Verfahren, die einem in der Praxis häufig begegnen:

- PIN Code als SMS an das Mobiltelefon
- PIN Code als E-Mail
- Anruf auf das Mobil- oder Festnetztelefon
    - ohne PIN Code Eingabe, nur mit Tastenbestätigung
    - Eingabe eines zuvor festgelegten PIN Codes
    - Eingabe eines PIN Codes, der auf dem Anmeldebildschirm angezeigt wird
- Authenticator App auf dem Smartphone
    - PIN Code nach dem **TOTP Standard (https://de.wikipedia.org/wiki/Time-based_One-time_Password_Algorithmus)**
    - PIN Code, eingebaut in das Betriebssystem (Apple)
    - Bestätigung über Push Nachricht mit PIN Code als Backup Methode

Nicht aufgeführt ist hier das **CAPTCHA Verfahren (https://de.wikipedia.org/wiki/Captcha)**, bei dem während der Anmeldung ein Bild- oder Buchstabenrätsel gelöst werden muss. Dabei handelt es sich jedoch nicht um eine zusätzliche Absicherung des Benutzerkontos, sondern lediglich um einen Schutz vor sogenannten **Brute-Force-Attacken (https://de.wikipedia.org/wiki/Brute-Force-Methode)**, bei denen das Passwort

erraten werden soll. Die Wirksamkeit solcher Maßnahmen ist eher fragwürdig und sie sind gar kontraproduktiv für die Nutzerakzeptanz von wirklichen Sicherheitsmaßnahmen, weshalb ich generell von dem Einsatz von CAPTCHA abraten und Dienstanbieter ermutigen möchte, stattdessen eine 2-Faktor-Authentifizierung anzubieten.

Bei den genannten 2-Faktor-Methoden gibt es eine klare Empfehlung, welche verwendet werden sollten. So gilt SMS bereits **seit längerer Zeit als verwundbar (https://www.schneier.com/blog/archives/2015/08/ss7_phone-switc.html)**. Leider ist es jedoch auch heute noch oftmals die einzig verfügbare Methode. Auch mit der Zusendung eines PIN Codes per E-Mail sollte man sich nicht zufriedengeben, zumal diese Methode naturgemäß nicht für den E-Mail Zugang an sich verwendet werden kann.
Der Rückruf auf eine zuvor hinterlegte Telefonnummer kann je nach Ausprägung durchaus recht sicher sein, ist jedoch so oder so sehr umständlich. Als Backup Methode ist die Variante mit PIN Code Generierung am Anmeldebildschirm jedoch tatsächlich recht universell einsetzbar, insbesondere für Benutzer ohne (funktionierendes) Smartphone.

Als bevorzugte Methode empfiehlt sich der Einsatz einer Authenticator App. Setzt man auf einen PIN Code über den TOTP Standard, so hat man – neben der Nutzung in einem Passwort Manager – die Qual der Wahl zwischen unterschiedlichen mobilen Apps. Man sollte seine Wahl jedoch auf bekannte Anbieter wie zum Beispiel den **Microsoft Authenticator (https://support.microsoft.com/de-de/help/4026727/microsoft-account-how-to-use-the-microsoft-authenticator-app)** oder **Google Authenticator (https://support.google.com/accounts/answer/1066447?co=GENIE.Platform%3DAndroid&hl=de)** eingrenzen. Bei unbekannten Anbietern besteht eine höhere Gefahr von unentdeckter Malware, welche es zu vermeiden gilt.
Weiterhin existiert eine Reihe von Apps, die nur mit bestimmter Hardware funktionieren und deshalb oftmals auch als sogenannte „Soft Token“ gehandelt werden – eine Software Version der Hardware Token. Der Unterschied dieser Apps gegenüber denen, die Standardverfahren verwenden, liegt jedoch zumeist in technischen Details. Nicht selten beschränkt er sich darauf zu verhindern, dass eine andere App als die des Herstellers genutzt werden kann. Gut für den Geldbeutel des Herstellers, die erhöhte Sicherheit besteht jedoch dann meistens lediglich daraus, dass die aktivierte App nicht auf andere Geräte übertragen oder ein Backup gemacht werden kann.

Für die Authenticator Apps von Microsoft und Google spricht noch etwas: Beide unterstützen neben der PIN Code Generierung auch die Anmeldung über eine Push Nachricht. Dabei muss man nach dem Entsperren des Smartphones lediglich eine Popup Nachricht bestätigen – das Abtippen eines PIN Codes entfällt. Selbst mit einer Smartwatch am Handgelenk lässt sich dies erledigen. Allerdings gibt es für die Push Nachricht keinen gemeinsamen Standard, so dass man die Push Benachrichtigung nur bei den jeweiligen Accounts der beiden Anbieter aktivieren kann. Zweifellos trägt diese Technologie dazu bei, die Akzeptanz von 2-Faktor-Authentifizierung bei Nutzern bedeutend zu erhöhen: Nach der Passwort Eingabe noch wenige Sekunden auf eine Push Benachrichtigung zu warten und diese mit einem einfachen Fingertipp zu bestätigen, darauf kann Otto Normalverbraucher sich einlassen.

Wohin geht die Reise für Unternehmen?

Mein kleiner Mann im Ohr sagt mir gerade, dass wir jetzt in die Werbung gehen müssen. Ich bitte deshalb um Verzeihung, dass ich den plakativ gewählten Titel über das Auslaufmodell „Passwort“ noch nicht auflösen kann.

Im zweiten Teil dieses Artikels (https://www.digatus.de/modernes-passwort-management-in-unternehmen-und-warum-passwoerter-weniger-wichtig-werden/) wird es dann darum gehen, wie Passwörter in Unternehmen verschwinden.

„Regie, wie lang ist dieser Werbeblock eigentlich?“ – „Endet Dienstag morgen!“.

Also, bis dahin auf diesem Kanal.

Julian Pawlowski

Als digatus Mitarbeiter erster Stunde führt er Kunden durch den Dschungel der Digitalisierung. Seine Begeisterung für neue Technologien ist seit 25 Jahren ungebrochen. Wenn er nicht gerade den Weg aus dem digitalen Dschungel heraus absteckt, dann beschäftigt er sich mit der Programmierung seines Smarthomes – ganz zum Erstaunen seines Jack-Russel Terriers „Eddie“. Auch als Hobby Programmierer für die Open Source und Smarthome Community verfolgt er stets das Ziel, die Welt durch Technologie ein Stück weit besser zu machen.