05.02.2019 | Julian Pawlowski | 8 min Lesezeit

State of the Union zum “Ändere-Dein-Passwort-Tag” – Teil 2

Modernes Passwort Management in Unternehmen und warum Passwörter weniger wichtig werden.

Willkommen zurück aus der Werbepause (https://www.digatus.de/weshalb-passwoerter-ein-auslaufmodel-sind-und-warum-sie-uns-trotzdem-noch-lange-begleiten-werden/). Ich freue mich, dass Sie drangeblieben sind. Wo waren wir doch gleich?

Ach ja: Alle von mir im vorigen Artikel erwähnten Prinzipien lassen sich sowohl auf den privaten als auch beruflichen Bereich anwenden. Für Unternehmen gibt es jedoch einige interessante weitere Entwicklungen um das Thema Passwort, welche ich an dieser Stelle gerne weiter ausführen möchte.

Der Mythos von regelmäßig geänderten Passwörtern

Seit Jahrzehnten hat sich die Praxis etabliert, dass Mitarbeiter in Unternehmen ihr Passwort regelmäßig ändern müssen. Nicht nur einmal jährlich, um die Brücke zum Eingangsthema zu schlagen. Im Laufe der Zeit kamen Richtlinien zur Komplexität des Passwortes hinzu, um zu verhindern, dass zu einfache Passwörter verwendet werden.
Dieser Zwang führte schnell zu den berühmten gelben Post-It Zetteln unter Tastaturen oder an Monitoren, auch auf und in zugeklappten Laptops sind sie zu finden. Spätestens seitdem Geräte mobil geworden sind, hat sich diese Passwort Richtlinie überlebt. Theoretisch sind komplizierte Passwörter und eine regelmäßige Änderung eine gute Idee. In der Praxis suchen Mitarbeiter aber nach allen Regeln der Kunst nach Wegen, diese lästige Richtlinie möglichst zu umgehen. Leider kann hier ein Passwort Manager nicht helfen, da sich ansonsten ein Henne-Ei-Problem bei der Anmeldung am Firmengerät ergibt.

Allerdings erlaubt uns die Einführung von zusätzlichen Faktoren, wie im vorigen Teil beschrieben, auch eine Überarbeitung der Passwort Richtlinie. Das regelmäßige Ändern eines Passwortes zu erzwingen kann abgeschaltet werden, verbunden mit der Schulung der Mitarbeiter, wie sie ihr dann unbegrenzt gültiges Passwort einmalig sicher anlegen ohne es anschließend aufzuschreiben. Richtig erklärt werden Mitarbeiter begeistert sein, endlich von dieser Bürde befreit zu sein. Auch der Eindruck eines Kuhhandels, bei dem man sich dann im Austausch auf die Nutzung von 2-Faktor-Authentifizierung einlassen muss, kann sehr leicht ausgeräumt werden, wenn man die richtigen Methoden dafür wie beschrieben anwendet.

Umfragen in Unternehmen haben ergeben, dass diese Änderung allein die Zufriedenheit mit der Unternehmens-IT signifikant gesteigert hat: Die Alltagsprobleme von Mitarbeitern sichtbar und nachhaltig zu lösen bringt Pluspunkte. Auch bei der Auswertung von Service Desk Statistiken ist dann festzustellen, dass bedeutend weniger Anrufe für die Rücksetzung eines Passwortes beantwortet werden müssen. Positives Feedback von den KollegInnen der IT Operations ist somit auch gewiss.

Die Schattenseite bei einem nicht mehr regelmäßig geänderten Passwort wird dann oft recht schnell von Beauftragten der Informationssicherheit im Unternehmen beziffert: Ist ein Account trotz 2-Faktor-Authentifizierung erst einmal kompromittiert, so bleibt er dies womöglich bis in alle Ewigkeit, weil das Passwort nicht geändert wird.
Naheliegend ist es daher einen Mechanismus zu installieren, der erkennt, wenn ein Benutzer sein Passwort ändern sollte, weil der Account womöglich einem konkreten Angriff ausgesetzt ist oder dieser gar bereits kompromittiert wurde. „Risk-driven password change" nennt sich diese Methode, bei der alle Aktivitäten eines Benutzers von einer KI auf ihr Risiko analysiert wird. In der heutigen Cloud Welt funktioniert das selbstverständlich in Echtzeit, so dass man hier ebenfalls sogar eine erhöhte Sicherheit erreicht, als zuvor. Der Benutzer kann aktiv dazu aufgefordert werden, sein Passwort zu ändern und alle Zugriffe auf Programme und Daten können bis dahin blockiert werden. „Bedingter Zugriff" oder neudeutsch **Conditional Access (https://docs.microsoft.com/azure/active-directory/conditional-access/conditions#sign-in-risk)** arbeitet hier Hand in Hand mit der **Benutzerkonto-Absicherung (https://docs.microsoft.com/azure/active-directory/identity-protection/vulnerabilities)** zusammen.

Diese neuen Funktionen werden möglich, weil über eine breite Datenbasis und Machine Learning Algorithmen (oft im Volksmund mit „KI" bezeichnet) Vorhersagen getroffen werden können, die mit sehr hoher Wahrscheinlichkeit zutreffen. Sogenannte „false positives", also fälschlicherweise ausgelöste Alarme, sind bei dieser Technologie nicht sehr wahrscheinlich, zumal sie sich stetig selbst verbessert.
Die für solche Funktionen notwendige, breite Datenbasis ist natürlich ausschlaggebend für die Sicherheit und Zuverlässigkeit solcher Technologien. Die Speicherung von Daten direkt in der Cloud anstatt im eigenen Netzwerk ermöglicht eine schnelle und einfache Nutzung. Aber auch Daten, die sich (noch) im eigenen Unternehmensnetz befinden, können hier angeschlossen werden, um eine 360 Grad Sicht über alle Ebenen zu erhalten und somit tatsächlich einen bestmöglichen Schutz des Mitarbeiters zu ermöglichen. Durch die Standort-unabhängige Verfügbarkeit dieser Technologien können letztendlich sogar Unternehmensnetze so zurückgebaut werden, dass sie sich nur noch wenig von einem Homeoffice Arbeitsplatz unterscheiden müssen.

Auch dieser Teilbereich des „Modern Identity & Access Management" ist gewiss eine eigene Kolumne wert, denn hier wird es tatsächlich interdisziplinär. Beispielsweise spielt dann auch der Schutz vor unbeabsichtigten Daten-Leaks eine zentrale Rolle.

Bringing it all together: Multiple Faktoren gemeinsam

Alle bereits beschriebenen 2-Faktor-Methoden lassen sich sowohl im Unternehmen als auch privat bei unterschiedlichen Diensten aktivieren. Beide Welten befruchten sich hier seit geraumer Zeit gegenseitig in ihrer Entwicklung. Insbesondere bei Microsoft wird deutlich, dass neue Konzepte wie die passwortlose Anmeldung (siehe nächster Abschnitt unten) zunächst für die persönliche Microsoft ID verfügbar werden, um sie anschließend auch für die Unternehmenskonten in Office 365 zu adaptieren.

Die Absicherung von Unternehmens-Accounts geht inzwischen noch einen Schritt weiter: Weitere Faktoren können für die Bestätigung der Identität genutzt werden. Naheliegend, dass die Geräte, die ein Unternehmen seinen Mitarbeitern bereitstellt, ebenfalls als ein Faktor gelten. Diese Geräte sind in der Regel von der hauseigenen IT gemanagt und können deshalb direkt als vertrauenswürdig gelten. Greift ein Mitarbeiter von einem solchen Gerät aus zu, ist es nicht notwendig eine Bestätigung über eine 2-Faktor-Authentifizierung einzufordern, da dieser sich bereits bei der Anmeldung am Rechner authentifiziert hat.

Was passiert nun aber bei der Anmeldung am Rechner?

In Windows 10 lassen sich hierzu seit einiger Zeit ebenfalls weitere Faktoren zusätzlich zum Passwort einschalten. **Windows Hello for Business (https://docs.microsoft.com/windows/security/identity-protection/hello-for-business/hello-videos)** ermöglicht hier, dass beispielsweise ein Mobiltelefon in Bluetooth Reichweite sein muss oder eine Gesichtserkennung über die Kamera die Identität bestätigt. Dass hier aber auch ein Fallback auf die Browser gestützte 2-Faktor-Authentifizierung möglich ist, wirkt dann schon fast wieder etwas altbacken.

Im Falle eines mobilen Endgerätes verhält es sich **ganz ähnlich (https://docs.microsoft.com/intune/conditional-access-intune-common-ways-use#device-based-conditional-access)**: Das Entsperren von Geräten kann inzwischen anstelle der Eingabe eines PIN Codes auch mit biometrischen Verfahren erfolgen. Ein von der Unternehmens-IT gemanagtes Smartphone kann somit ebenfalls als Ersatz für einen der anderen Faktoren zur Identitätsbestätigung dienen, wenn man davon ausgeht, dass das Entsperren des Gerätes nur durch die berechtigte Person erfolgen kann.

Anmeldung ohne Passwort

Um vor allem dem plakativen Titel des ersten Artikels gerecht zu werden, wie genau soll man sich nun ganz ohne die Eingabe eines Passwortes anmelden? Wir kommen nun also endlich zur Auflösung. Um es gleich zu sagen: Ein Passwort wird man vorerst mal noch weiterhin vergeben müssen. Allerdings wird man es deutlich seltener eingeben müssen, was tatsächlich eine signifikante Verbesserung für die Sicherheit darstellt: Ein Passwort, welches ich gar nicht mehr eingebe, kann auch nicht übertragen und ausgespäht werden.

Der letzte Bereich, wo ein Mitarbeiter normalerweise nun noch sein Passwort eingeben muss, ist bei der Anmeldung am PC. Im Falle von Windows 10 kann auch hier „Windows Hello for Business“ so verwendet werden, dass bei der ersten Anmeldung am PC eine **lokale PIN (https://docs.microsoft.com/windows/security/identity-protection/hello-for-business/hello-why-pin-is-better-than-password)** vergeben werden muss, mit der sich der Benutzer dann anschließend statt seines eigentlichen Passworts anmeldet. Das Prinzip dahinter ist dann dasselbe wie bei einem Smartphone auch und daher leicht verständlich. Die PIN kann tatsächlich nur aus Ziffern bestehen, sollte jedoch mindestens 6-stellig sein, besser 8-stellig. Gekoppelt mit einem biometrischen Verfahren wie der Gesichtserkennung, einem Fingerabdruck oder aber auch dem Bluetooth Signal des Smartphones ergibt sich eine tatsächlich sehr sichere Anmeldung bei hohem Komfort für den Benutzer. Dieses Level an Sicherheit stand früher nur großen Konzernen mit entsprechenden Firmenausweisen zur Verfügung. Ein durchaus vergleichbares Level ist mit moderatem, finanziellem Aufwand nun auch bereits für KMU’s verfügbar und macht das mobile Arbeiten sorgenfreier und einfacher.

Angesichts dessen, dass wir dem Benutzer oben zwar die Freiheit gegeben haben, dass sein Passwort nicht mehr ausläuft, dieses jedoch nun tatsächlich möglichst nicht mehr zu erraten sein und es auch nicht mehr aufgeschrieben werden soll, ergibt sich hier noch ein kleines Dilemma: Das Vergessen von Passwörtern.
Eine Möglichkeit, die man tatsächlich in Erwägung ziehen kann, ist das Kennwort für den Firmenaccount nun ebenfalls in einem Passwort Manager zu speichern. Solange der zweite Faktor hier weiterhin getrennt bleibt, ist dagegen nicht viel einzuwenden, schließlich soll ja auch der Passwort Manager mit einem komplexen Passwort abgesichert sein.

Die andere Möglichkeit ist, dem Benutzer einen möglichst einfachen, aber auch sicheren Weg zu bieten, sein vergessenes Passwort selbst zurückzusetzen. Eine generelle Möglichkeit hierfür haben viele Firmen schon seit geraumer Zeit implementiert, um der Numero Uno bei den Tickets am IT Service Desk entgegen zu wirken. Selten sind diese Prozesse jedoch absolut perfekt und nicht selten scheitern Mitarbeiter trotzdem noch häufig genug an einem Self-Service Passwort Reset. Der Grund liegt auf der Hand: Ist man aus dem eigenen Rechner bereits ausgesperrt, ergibt sich oft ein Henne-Ei-Problem für den Zugriff auf die Portalseite für den Reset. Die Unterstützung von Kollegen hilft manchmal, ist aber nicht die Art von Prozess, die sich Mitarbeiter wünschen.

Die naheliegende Überlegung zur Auflösung: Kann der Mitarbeiter nicht noch irgendwie doch mit seinem eigenen Rechner das Passwort zurücksetzen, ohne sich anmelden zu müssen? Er kann: Windows 10 Enterprise erlaubt in den neueren Versionen den Zugriff auf den **Self-Service-Password-Reset von Office 365 (https://docs.microsoft.com/azure/active-directory/user-help/user-help-reset-password)** (bzw. genauer Azure Active Directory) **direkt vom gesperrten Bildschirm (https://docs.microsoft.com/azure/active-directory/authentication/tutorial-sspr-windows#what-do-users-see)** aus. Das funktioniert dann tatsächlich auch von überall, nicht nur vom Büroarbeitsplatz aus. Als ich das das erste Mal gesehen habe dachte ich: Wow, das klingt so einfach und naheliegend, warum erst jetzt? Aus meiner ausführlichen Beschreibung dürfte jedoch deutlich werden: Es war ein sehr langer Weg für Microsoft all diese Puzzlesteine zusammenzulegen. Chapeau!

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.