RESOURCE CENTER

Fünf bewährte Verfahren für die Passwortverwaltung in Unternehmen

Lernen Sie in diesem Whitepaper die besten Methoden für die Passwortverwaltung in Unternehmen kennen.

Get the full interactive view at
https://bitwarden.com/de-de/resources/five-best-practices-for-password-management-white-paper/

bitwarden

Während Unternehmen der Sicherheit weiterhin Priorität einräumen, ist ein wichtiger Teil dieser Bemühungen die Aufklärung normaler Benutzer über bewährte Verfahren. Bedenken Sie einige der folgenden Statistiken aus dem "Yubico 2019 State of Password and Security Authentication Security Behaviors Report":

- 2 von 3 Befragten teilen Passwörter mit Kollegen
- 51 Prozent gaben an, dass sie Passwörter für private und geschäftliche Konten wiederverwenden
- 57 Prozent gaben an, dass sie ihre Passwörter nach einem Phishing-Versuch nicht geändert haben

Um einen Wandel in einem Unternehmen herbeizuführen, müssen Sicherheits- und IT-Teams die Mitarbeiter über bewährte Verfahren aufklären. In Bezug auf die Passwortverwaltung ist eine der einfachsten Möglichkeiten, eine gute Passworthygiene zu fördern, der Einsatz einer Lösung zur Passwortverwaltung am Arbeitsplatz. Es folgen einige weitere bewährte Verfahren, die Sie umsetzen sollten.

1. Nutzen Sie eine Lösung zur Passwortverwaltung.

Im Laufe des Tages besuchen die meisten Menschen viele verschiedene Internetseiten, die Passwörter erfordern. Es ist praktisch unmöglich, sich Dutzende von individuellen und ausreichend starken Passwörtern (oder Passphrasen) zu merken. Ein Passwort-Manager vereinfacht die Verwendung von Passwörtern auf verschiedenen Webseiten, um die Sicherheit der Benutzer zu erhöhen. Es gibt eine Reihe solider Passwort-Manager. Bevorzugen Sie solche, die plattformübergreifend funktionieren und die Dienste für Privatanwender kostenlos oder zumindest zu einem sehr niedrigen Preis anbieten. Der Funktionsumfang der meisten Passwort-Manager hat sich im Laufe der Jahre übrigens erweitert.

2. Wählen Sie ein Tool, das Sie problemlos in Ihrem Unternehmen einsetzen können.

Passwort-Manager müssen für jede Benutzerebene – vom Anfänger bis zum Fortgeschrittenen – einfach zu bedienen sein. Wenn Sie einen großen oder breit gestreuten Mitarbeiterstamm haben, sollten die Anwendungen intuitiv zu bedienen und leicht zu implementieren sein. Egal, ob Sie sich für die Bitwarden Cloud entscheiden oder Ihre eigene, selbst gehostete Infrastruktur nutzen: Bitwarden ist einfach zu installieren und in Betrieb zu nehmen. Und der Bitwarden Directory Connector arbeitet mit den heute am weitesten verbreiteten Verzeichnisdiensten wie Azure, Active Directory, Google, Okta und anderen, um Ihre Bitwarden-Benutzer mit Ihren Teams und Mitarbeitern zu synchronisieren.

3. Ändern Sie Passwörter nur, wenn Sie möglicherweise kompromittiert wurden.

Die Zeiten, in denen Sie Ihr Passwort alle drei Monate ändern sollten, sind vorbei. Sie sollten sie nur noch ändern, wenn Sie glauben, dass Sie kompromittiert worden sind. Das National Institute of Standards and Technology (NIST) in den USA empfiehlt Benutzern nicht, Passwörter häufig zu ändern. Dies führe nämlich zu einem Verhalten, das im Laufe der Zeit zu schwächeren Passwörtern beitragen könnte. Sie können feststellen, ob Sie kompromittiert wurden, indem Sie sich auf handfeste Anhaltspunkte beziehen, z. B. Kreditkartenbetrug, oder indem Sie ein Tool wie Ihren Passwort-Manager verwenden, das feststellen kann, ob Ihr Passwort bei einem Sicherheitsverstoß enthüllt wurde.

4. Verwenden Sie sichere, eindeutige Passwörter.

Die Verwendung sicherer, eindeutiger Passwörter für jeden Dienst, den Sie online nutzen, trägt dazu bei, die Auswirkungen von Datenmissbrauch zu minimieren. Ein sicheres Passwort bedeutet nicht unbedingt, dass man einfach Sonderzeichen oder Zahlen zu einem gewöhnlichen Wort oder Namen hinzufügt, sondern dass man die Entropie oder die Zufälligkeit des Passworts erhöht. Eine einfache Taktik zur Erstellung eines sicheren Passworts ist die Verwendung einer Passphrase. Eine Passphrase kombiniert scheinbar nicht zusammenhängende Wörter oder Phrasen, die sich der Benutzer leicht merken kann, die aber ansonsten für einen Angreifer schwer zu erraten sind. Passphrasen haben ein hohes Maß an Entropie und sind gleichzeitig leicht zu merken.

5. Aktivieren Sie, wann immer möglich, die Zwei-Faktor-Authentifizierung.

Da die Zwei-Faktor-Authentifizierung (2FA) auf Internetseiten für Verbraucher und Unternehmen immer üblicher wird, sollten gute Passwort-Manager Möglichkeiten zur Ausweitung dieser Funktion anbieten. Die Verwendung von 2FA erhöht die Sicherheit Ihres Kontos, da Sie neben Ihrem Master-Passwort ein weiteres Token eingeben müssen. Selbst wenn jemand Ihr Master-Passwort herausfindet, kann er sich ohne das zusätzliche Token nicht bei Ihrem Passwort-Manager anmelden. Wenn Sie anfangen möchten, mit einem Passwort-Manager zu arbeiten, können Sie sich hier für ein kostenloses Bitwarden-Konto anmelden.