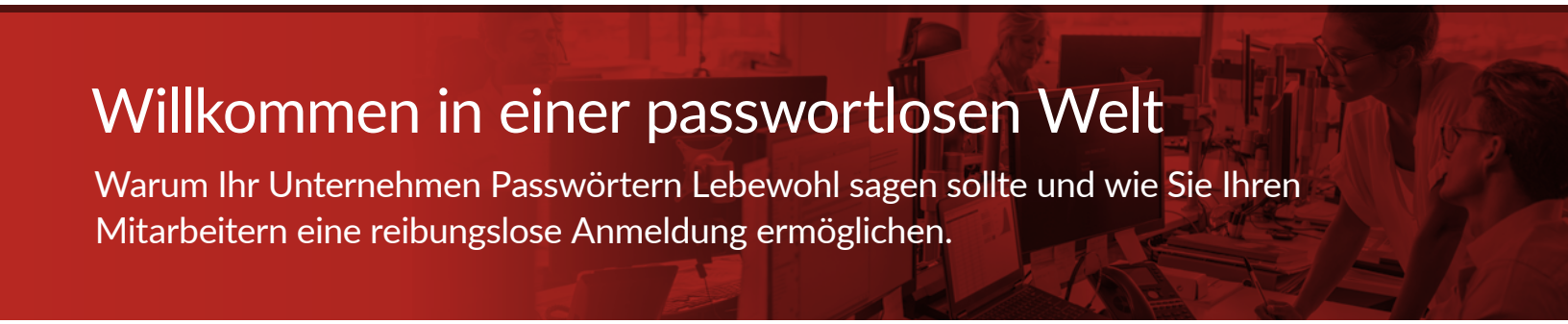

Willkommen in einer passwortlosen Welt

Warum Ihr Unternehmen Passwörtern Lebewohl sagen sollte und wie Sie Ihren Mitarbeitern eine reibungslose Anmeldung ermöglichen.

80 Prozent der Sicherheitsverletzungen sind nach wie vor auf schwache oder mehrmals verwendete Passwörter zurückzuführen, und 76 Prozent der Mitarbeiter haben regelmäßig Probleme mit ihren Passwörtern. Was sollen IT-Teams angesichts des damit verbundenen Ressourcenaufwands und der Sicherheitsrisiken tun?

Warum Ihr Unternehmen Passwörtern den Rücken kehren sollte.

Keine Passwörter mehr? Das mag utopisch klingen, aber mit der richtigen Kombination aus technologischen Lösungen lassen sich passwortbezogene Hürden aus dem Weg räumen. Aber warum sollte Ihr Unternehmen überhaupt in Betracht ziehen, auf das passwortlose Arbeiten umzusteigen? Es bietet eine Reihe von Vorteilen:

Höhere Sicherheit

Die mit Passwörtern verbundenen Sicherheitsrisiken – insbesondere mit schwachen, mehrmals verwendeten der schlecht verwalteten – sind bestens bekannt. Nahezu 80 Prozent aller Datenlecks aufgrund von Hackerangriffen sind auf gestohlene Zugangsdaten zurückzuführen. Wenn Sie Passwörter in Ihrem Unternehmen eliminieren, können Sie die Gefahr einer durch Passwörter verursachten Sicherheitsverletzung beträchtlich reduzieren.

Verbessertes Nutzungserlebnis

Ein durchschnittlicher Mitarbeiter muss sich mit mehr als 100 Passwörtern herumschlagen. Kein Wunder, dass 59 Prozent der Benutzer meistens oder immer dasselbe Passwort verwenden. Mitarbeiter wünschen sich einfach nur effiziente und benutzerfreundliche Technologien. Passwortlos zu arbeiten bedeutet, dass sie schneller auf ihre beruflich genutzten Tools zugreifen können, während „Zeitfresser“ wie Kontosperren, Zurücksetzen und häufige Passwortaktualisierungen der Vergangenheit angehören.

Mehr Kontrolle

77 Prozent der Mitarbeiter verwenden ohne Genehmigung oder Wissen der IT-Abteilung Cloud-Apps von Drittanbietern, und die meisten IT-Experten (83 Prozent) geben an, dass Mitarbeiter Firmendaten in nicht autorisierten Cloud-Diensten speichern. Kurz gesagt: IT-Abteilungen haben nicht genug Einblick in den unternehmensweiten Mitarbeiterzugriff und zu wenig Kontrolle über die sogenannte Schatten-IT. Technologien, die Passwörter ersetzen oder eliminieren, machen es IT-Teams möglich, für diese Art von Transparenz und Kontrolle zu sorgen.

Geringere Kosten

IT-Sicherheitsteams verbringen durchschnittlich vier Stunden pro Woche mit passwortbezogenen Problemen und erhalten 96 passwortbezogene Anfragen pro Monat. Intern betriebene und verwaltete Legacy-Technologien sind oft mit großen Overheads verbunden. Passwortlose Softwarelösungen senken diese Kosten und den benötigten Personalaufwand, sodass sich IT-Abteilungen auf rentablere Aktivitäten konzentrieren können.

So machen Sie das passwortlose Arbeiten zur Realität.

Erfassen Sie zunächst alle Passwörter an einem Ort.

Einer der Gründe, warum Passwörter nach wie vor so viele Probleme bereiten, ist, dass die Mitarbeiter selbst für ihre Zugangsdaten verantwortlich sind. Führen Sie einen Enterprise-Passwort-Manager (EPM) ein, der jedes verwendete Passwort erfasst und speichert.

Nun müssen sich die Mitarbeiter ihre Passwörter nicht mehr merken, da sie der Passwort-Manager für sie eingibt, und die IT-Abteilung erhält Einblick in die Passwortgewohnheiten jedes Benutzers.

Sie arbeiten zwar immer noch mit Passwörtern, aber immerhin müssen sich die Mitarbeiter nur mehr ein Master-Passwort merken – ein großer Schritt in die richtige Richtung.

Ersetzen Sie Passwörter nach Möglichkeit durch andere sichere Protokolle.

Ersetzen Sie Passwörter als Nächstes durch Single Sign-On (SSO), auch Einmalanmeldung genannt. Dann können Ihre Mitarbeiter über das sichere Protokoll SAML 2.0 auf ihre Apps zugreifen – ob Cloud- oder mobile Apps, Legacy- oder lokal installierte Anwendungen –, ohne ihre Passwörter speichern oder Anmeldeformulare ausfüllen zu müssen.

SSO in Verbindung mit einem Enterprise-Passwort-Manager sorgt dafür, dass sich die Benutzer nach wie vor nur ein Passwort merken müssen und passwortlos auf zahlreiche Dienste zugreifen können. Gleichzeitig werden Zugangsdaten bei formularbasierten Anmeldungen automatisch für sie eingegeben.

Eliminieren Sie Passwörter mit einer stärkeren Authentifizierung.

Der letzte Schritt auf dem Weg zum passwortlosen Arbeiten ist die Einführung der Multifaktor-Authentifizierung (MFA). Generell wird die Multifaktor-Authentifizierung als zusätzlicher Anmeldeschritt gesehen – was auch stimmt, da eines der Hauptziele eine höhere Sicherheit ist, indem man seine Identität mit Hilfe zusätzlicher Informationen („Faktoren“) nachweisen muss.

Moderne Authentifizierungslösungen können jedoch biometrische (menschliche) Faktoren wie Fingerabdrücke und die Gesichtserkennung mit kontextuellen (versteckten) Faktoren wie der Gerätekennung, dem Standort oder der IP-Adresse kombinieren. Anhand dieser Datenpunkte lässt sich die Identität eines Benutzers präziser nachweisen. Darüber hinaus können diese Faktoren Passwörter ersetzen, da keine Zugangsdaten mehr eingegeben werden müssen, bevor der Benutzer Zugriff auf ein SSO- oder EPM-Portal oder einen anderen Dienst erhält.

Eine Komplettlösung für die Identitätsverwaltung macht eine passwortlose Welt möglich.

Eine Identitätslösung, die EPM, SSO und MFA umfasst, bietet Unternehmen eine effektive Methode für den passwortlosen Zugriff. Passwortlose Authentifizierung bedeutet ein besseres Nutzungserlebnis für die Mitarbeiter, mehr Transparenz und Kontrolle für IT-Teams, höhere Sicherheit im gesamten Unternehmen und geringere IT-Kosten. Kurzum, davon profitieren sowohl Benutzer als auch Administratoren.

Unternehmen, die auf der Suche nach einfacher Kontrolle und einheitlicher Transparenz für jeden Einstiegspunkt zu ihren Daten sind, sollten LastPass Identity ausprobieren. Der intuitive Zugriff und die Multifaktor-Authentifizierung mit LastPass Identity funktionieren sowohl für Cloud- und mobile Apps als auch für ältere, vor Ort installierte Tools.

Erfahren Sie mehr über LastPass Identity, das Zugriff und Authentifizierung in einer Lösung vereint: www.lastpass.com/products/identity