SecurID

Passwortlose Authentifizierung Die Zeit ist gekommen - Hilfe steht bereit

Passwörter sind schwer zu merken und leicht zu knacken und stellen für Unternehmen seit jeher ein Sicherheitsproblem dar. Aber das Problem hat sich verschärft, da immer mehr Menschen auf Anwendungen und Daten jenseits der traditionellen Sicherheitsperimeter zugreifen. Um Anwendungen und Daten in der digitalen Welt erfolgreich abzusichern, benötigen Unternehmen einen sicheren Zugriff, der nicht auf Passwörter angewiesen ist. Aber wie gelangt man von einem Passwort-für-alles-Ansatz zu einer passwortlosen Zukunft? Indem Sie einen Schritt nach dem anderen gehen auf einem Weg, der mit diesen Best Practices gepflastert ist:

Wenden Sie einen schrittweisen benutzerfreundlichen Ansatz an

Passwörter können mühsam sein, aber wir haben uns im Laufe der Zeit an sie gewöhnt. Die schrittweise Abkehr von Passwörtern erleichtert den Nutzern den erfolgreichen Übergang zu einer neuen Authentifizierungsmethode. Beginnen Sie mit der Einführung moderner Authentifizierungsmethoden – biometrische Verfahren, FIDO, OTP usw. – in Verbindung mit und nicht anstelle von Passwörtern. Dieser Ansatz vermeidet Unterbrechungen und trägt dazu bei, dass Nutzer produktiv bleiben, während sie sich der Veränderung anpassen.

Authentifizierung wird sicherer und bequemer

Die Abkehr von Passwörtern soll natürlich Ihre Sicherheitslage verbessern, aber Sie dürfen dabei keine Abstriche bei der Benutzerfreundlichkeit machen. Ein wichtiger Faktor zur Erreichung dieses Gleichgewichts ist die Implementierung von Risikoinformationen, um zu bestimmen, wie und wann eine verschärfte Authentifizierung erforderlich ist. Dies kann ein schrittweiser Prozess sein, der sich von statischen Richtlinien über bedingten Zugang hin zu dynamischen Risikobewertungen in Echtzeit entwickelt.

Wenden Sie eine starke Authentifizierung an Schwachstellen an

Das Risiko kompromittierter Anmeldedaten ist an den schwächsten Punkten im Lebenszyklus der Anmeldedaten am größten, z. B. bei der Registrierung, dem Zurücksetzen von Passwörtern und dem Notfallzugang. Bei der Umstellung auf passwortlose Authentifizierung sollten diese Punkte als erste durch biometrische Daten, FIDO-Geräte und andere starke Authentifizierungsmethoden geschützt werden, die nicht auf herkömmlichen Passwörtern basieren.

Um Anwendungen und Daten in der digitalen Welt erfolgreich abzusichern, benötigen Unternehmen einen sicheren Zugriff, der nicht auf Passwörter angewiesen ist.

Verlieren Sie nicht das Ziel aus den Augen

Sie werden Passwörter nicht über Nacht los und möglicherweise werden einige Systeme und Anwendungen – sowohl Legacy- als auch SaaS – weiterhin Passwörter erfordern, wenn auch nur für eine kleine Untergruppe von Nutzern. Letztendlich lohnt es sich jedoch, eine passwortlose Zukunft anzustreben, die dem kostspieligen umfangreichen Passwortmanagement ein Ende setzt, das Risiko einer Verletzung von Zugangsdaten verringert, das Nutzererlebnis verbessert und viele andere Vorteile bietet.

SecurID: Ein reibungsloser Weg in Ihre passwortlose Zukunft

Die weltweit am weitesten verbreitete Multi-Faktor-Authentifizierungslösung ist SecurID, eine Identitätsmanagementplattform, der sicherheitskritische Organisationen vor Ort und in der Cloud vertrauen. Sie bietet:

Ein breites Angebot an Authentifikatoren zur passwortlosen Authentifizierung, einschließlich FIDO, Push-to-Approve, biometrischer Verfahren (Fingerabdruck und Gesichtserkennung), „Bring your own Authenticator“ und Hardware-Token, die den Goldstandard für die Authentifizierung darstellen

RSA Ready-Partnerbeziehungen mit führenden FIDO-Authentifizierungsunternehmen, um eine **sofort funktionierende Interoperabilität** mit FIDO-basierten, passwortlosen Lösungen zu gewährleisten

Risikobewertung durch fortschrittliches maschinelles Lernen und KI-Funktionen, die das Zugriffsrisiko basierend auf Unternehmenskontext, Geräteattributen und Verhaltensmerkmalen berechnen und die Authentifizierung entsprechend verstärken

Geschützte Self-Service-Optionen für das Management von Anmeldeinformationen, die passwortabhängige Workflows eliminieren, um die Sicherheit an Schwachstellen beim Onboarding, der Wiederherstellung von Anmeldeinformationen und dem Notfallzugriff zu gewährleisten

Permanente starke Authentifizierung mit 99,95% iger Verfügbarkeit und eine einzigartige „No-Fail“-Funktion für Windows und macOS, die einen sicheren und bequemen Zugriff auch bei unterbrochener Netzwerkverbindung gewährleistet

Erfahren Sie mehr über die SecurID-Funktionen, mit denen Sie den Weg Ihres Unternehmens weg von passwortzentrierter Datensicherheit und hin zu einer passwortlosen Zukunft planen können.

Informationen über SecurID

SecurID, ein RSA-Unternehmen, ist eine Identitätsplattform, der bereits 13.000 Unternehmen auf der ganzen Welt vertrauen. Sie verwaltet 50 Millionen Identitäten und bietet 30 Millionen Benutzern einen sicheren und bequemen Zugriff. Mit SecurID können Unternehmen in einer digitalen Welt erfolgreich sein und verfügen über umfassende Funktionen für moderne Authentifizierung, Lebenszyklusmanagement und Identity Governance. Ob in der Cloud oder On-Premise – SecurID verbindet Menschen mit den digitalen Ressourcen, von denen sie abhängig sind, wo immer sie leben, arbeiten und spielen. Weitere Informationen finden Sie unter **securid.com**.

SecurID
An RSA Business