yubico

Passwortlos 1x1: **Wie Sie Ihr Unternehmen noch heute vor Phishing schützen**

Die Umstellung auf passwortlose Anmeldung ist eine der besten Maßnahmen, um die IT-Sicherheit in ihrem Unternehmen zu steigern. Sie bietet die dreifache Chance, die Sicherheit drastisch zu verbessern, die Benutzerfreundlichkeit zu steigern und den Aufwand zu reduzieren. Passwortbasierte Umgebungen sind immer anfälliger für Phishing. Jeder Schritt weg von Passwörtern wird Ihre Sicherheit nachhaltig verbessern.

Der Weg zur passwortlosen Umgebung kann jedoch lang und steinig sein, wenn Sie sich nicht auf eine erfolgreiche Implementierung vorbereiten. In diesem Dokument erklären wir, was passwortlose Authentifizierung ist und wie Sie am besten vorgehen, um Ihr Unternehmen heute und in Zukunft vor Phishing und dem Diebstahl von Anmeldedaten zu schützen.

Was ist passwortlose Authentifizierung?

Grundsätzlich versteht man unter passwortloser Authentifizierung jede Form der Authentifizierung, bei der der Benutzer kein Passwort eingeben muss, um sich anzumelden.

Die Umstellung auf passwortlose Authentifizierung ist eine Reise und kein Ziel, das über Nacht erreicht wird. Um dorthin zu gelangen, werden die meisten Unternehmen zunächst ihre alte Multifaktor-Authentifizierung (MFA) auf eine moderne MFA-Lösung umstellen, die einen starken Phishing-Schutz bietet. Der Weg von veralteter MFA hin zu moderner MFA bereitet ein Unternehmen dann auf den Übergang zu einer passwortlosen Authentifizierung vor.

Es gibt zwar viele Beispiele für die heute verwendete MFA, jedoch sind nicht alle MFA gleich stark in Bezug auf Sicherheit und Schutz vor Phishing. Werfen wir zunächst einen Blick auf die heute verfügbaren Optionen.

Alte MFA

SMS

Bei der SMS-Verifizierung wird dem Benutzer in der Regel ein Einmalpasswort (OTP) gesendet, oftmals in Form eines 6-stelligen Codes.

Link per E-Mail

Bei dieser Methode wird ein eindeutiger Link mit einem eingebetteten Token erstellt und an eine E-Mail-Adresse gesendet. Durch Anklicken des Links wird der Benutzer für diesen bestimmten Dienst verifiziert.

Was SMS-Verifizierung und Links per E-Mail an Benutzerfreundlichkeit gewinnen, verlieren sie an Sicherheit: Beide Methoden sind sehr anfällig für Phishing. Benutzer können leicht dazu verleitet werden, ein gefälschtes OTP einzugeben oder auf einen „Phishing-Köder“-Link zu klicken.

Moderne MFA

Smartcards

Bei dieser Lösung führt ein Benutzer seine Smartcard in ein Lesegerät ein und validiert sie mit einer eindeutigen PIN. Diese Methode ist eine der wirksamsten Methoden zum Schutz vor Phishing-Angriffen aus der Ferne, aber herkömmliche Smartcards sind für Administratoren unter Umständen nur schwer zu implementieren und in großem Umfang zu verwalten.

Biometrische Lesegeräte

Biometrische Lesegeräte verwenden ein eindeutiges biologisches Merkmal (ein Gesicht, einen Fingerabdruck, eine Iris oder ein anderes Merkmal) als Berechtigungsnachweis. Da immer mehr moderne Geräte mit integrierten Plattform Authentifikatoren wie TouchID, FaceID und anderen verfügbar sind, nimmt die Verwendung biometrischer Merkmale rasch zu.

PINs

PINs werden häufig mit lokalen Geräten wie biometrischen Lesegeräten oder Smartcards gekoppelt. Da eine PIN immer an ein physisches Gerät gebunden ist, gilt sie als sicherer als herkömmliche MFA, da sie sich weder auf einem Server befindet, der geknackt werden kann, noch über ein Netzwerk gesendet werden muss.

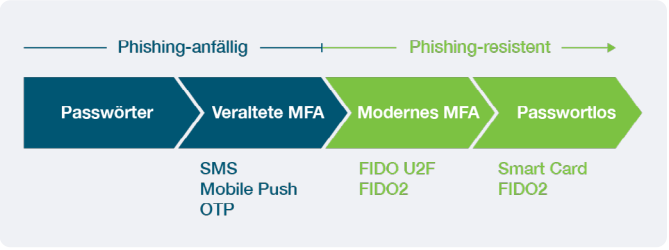

Abbildung 1: Passwortlos werden ist eine Reise, und sie hat bereits begonnen

Wie entwickelt man eine passwortlose Strategie?

Der erste Schritt zur Entwicklung einer passwortlosen Strategie besteht darin, die vorhandene Umgebung, die Investitionen und die Ressourcen zu bewerten.

Dabei sollten Sie sich zwei Fragen stellen:

- Arbeiten Sie in der Cloud, vor Ort oder in einer hybriden Umgebung?
- Welche Prioritäten setzen Sie bei Sicherheitsniveau, Benutzerfreundlichkeit und Kosten?
- Diese Elemente stehen manchmal in Widerspruch zueinander, daher ist es wichtig zu wissen, welche Kompromisse Sie eingehen werden, wenn Sie schwierige Entscheidungen treffen müssen.

Auf diese Weise können sie herausfinden, welcher Weg zum passwortlosen Arbeiten für Ihr Unternehmen und Ihre Benutzer am besten und effizientesten ist.

Wege zur passwortlosen Anmeldung

Passwortloser Ansatz mit Smartcard

Unternehmen mit einer lokalen Infrastruktur sollten die Implementierung eines Smartcard-basierten passwortlosen Ansatzes in Betracht ziehen. Dies bietet sowohl die Vorteile einer hohen Sicherheit als auch einer passwortlosen Benutzererfahrung.

Smartcards sind deutlich weniger Phishing-anfällig als passwortbasierte Systeme und werden in sehr vielen Unternehmen der Welt, die besonderen Wert auf IT-Sicherheit legen, bereits erfolgreich eingesetzt. Wie bereits erwähnt, sind herkömmliche Smartcard-Implementierungen komplex und zeitaufwendig. Unternehmen sollten eine Vereinfachung der Smartcard-Implementierung mit einer starken Authentifizierungslösung in Betracht ziehen, die sowohl für die IT-Abteilung einfach zu übernehmen ist als auch die Benutzer nicht mit zusätzlicher Hardware wie Smartcard-Lesegeräten belastet.

FIDO2/WebAuthn passwortloser Ansatz

FIDO2 ist die neueste Spezifikation der FIDO Alliance für Authentifizierungs Standards, und WebAuthn ist eine webbasierte API, mit der Websites ihre Anmeldeseiten aktualisieren können, um FIDO-basierte Authentifizierung auf unterstützten Browsern und Plattformen hinzuzufügen. Dies ist ein sich entwickelndes Sicherheits-Ökosystem, dass Cloud-First-Unternehmen dabei helfen kann, passwortlos zu werden. Für Cloud-First-Umgebungen kann FIDO2/WebAuthn eine effektive passwortlose Strategie sein.

Wenn Sie über cloudbasierte Anwendungen wie Office 365 oder andere SaaS-Anwendungen wie Salesforce verfügen, die mit Azure AD (AAD) verbunden sind und unter AAD oder einer hybriden AD-AAD-Backend-Umgebung arbeiten, dann ist FIDO2 (passwortlos) wahrscheinlich Ihr bester erster Schritt. Wenn Sie mit anderen IAM-Anbietern wie Okta, Duo oder Ping arbeiten, können Sie auch von einem FIDO2/WebAuthn-basierten passwortlosen Ansatz profitieren.

Hybrider passwortloser Ansatz

Unternehmen entscheiden sich zunehmend dafür, verschiedene Arten von passwortlosen Ansätzen zu kombinieren, um eine Lösung zu schaffen, die ihren Anforderungen gerecht wird. Ein Unternehmen könnte FIDO2/WebAuthn (passwortlos) für die Computeranmeldung und verbundene Webanwendungen verwenden und einen passwortlosen Smartcard-Ansatz für sicheren Fernzugriff (RDP, VPN, VDI).

Zukunftssicherheit für Ihre Strategie zur passwortlosen Anmeldung

Es gibt viele Möglichkeiten, eine Phishing-resistente passwortlose Authentifizierung zu erreichen. Alle Strategien führen zu höherer Sicherheit, einer besseren Benutzererfahrung und einem beruhigenden Gefühl für Ihr gesamtes Unternehmen.

Egal, welche Richtung Sie einschlagen, Sie können Ihre Investition mit Hardware-basierten Sicherheitsschlüsseln wie der YubiKey 5-Serie zukunftssicher machen. Die YubiKey 5-Serie arbeitet nahtlos mit einer Smartcard, FIDO2/WebAuthn und einem hybriden passwortlosen Ansatz. Sie ist auch mit einer Reihe von technischen Umgebungen kompatibel, von veralteten Anwendungen bis hin zu einer modernen Cloud-Umgebung.

Sie müssen keine neuen Investitionen in Software oder Peripheriegeräte tätigen, bevor Sie die YubiKey 5-Serie als Teil Ihres Systems integrieren. YubiKeys sind der Startschuss für Ihre Reise zur passwortlosen Anmeldung.

Des Weiteren verbessern YubiKeys Ihre allgemeine Sicherheitslage, vereinfachen die Bereitstellung und machen Ihre Sicherheitsinvestitionen zukunftssicher, wenn sich Ihre Anforderungen weiterentwickeln und die Compliance-Vorschriften strenger werden.

Und während Sie die beste passwortlose Strategie für Ihr Unternehmen festlegen, können Sie Phishing sofort ein Ende setzen, indem Sie YubiKeys als zweiten Faktor zusätzlich zu einem Passwort verwenden.

Yubico: Passwortlos möglich machen

Seit unserer Gründung setzt sich Yubico für offene Sicherheitsstandards ein, um Sicherheit und Benutzerfreundlichkeit in großem Umfang zu erreichen. Yubico hat den Weg geebnet, indem es Pionierarbeit für die offenen Standards WebAuthn und FIDO geleistet und mit Tech-Giganten wie Google, Microsoft und Apple zusammengearbeitet hat, um diese Standards in die Betriebssysteme und Browser zu integrieren, die wir jeden Tag nutzen. Diese Standards ermöglichen in Verbindung mit einem YubiKey eine starke passwortlose Authentifizierung über Geräte, Apps und Dienste hinweg, ohne zusätzliche proprietäre Software.

Yubico AB
Kungsgatan 44
2nd floor
SE-111 35 Stockholm
Schweden

Yubico Inc.
530 Lytton Avenue, Suite 301
Palo Alto, CA 94301 USA
844-205-6787 (gebührenfrei)
650-285-0088