ForgeRock®

INTELLIGENT ACCESS-SERIE

Go Passwordless

Mehr Sicherheit durch passwortlose Authentifizierung

Das Passwort-Problem

Als Experte für Identity und Access Management wissen Sie, dass Passwörter ein Problem darstellen. Konten mit Passwörtern anlegen zu müssen, ist nicht gerade eine Lieblingsbeschäftigung Ihrer Benutzer. Ihre Sicherheitsteams machen sich Sorgen wegen E-Mail-Phishing, Zugangsdaten-Diebstahl und Datenschutzverletzungen.

Durchschnittlich verfügt jede Person über mehr als 90 verschiedene Konten. Da ist es nicht so einfach, sich alle Passwörter zu merken. Deshalb verwenden über 50 % der Benutzer die gleichen Passwörter auf mehreren Websites.[1] Wenn Passwörter auf persönlichen Informationen beruhen, sind sie außerdem anfällig für Wörterbuchangriffe. Eine Möglichkeit, mit dem Passwort-Problem umzugehen, ist der Einsatz eines Passwort-Management-Systems. Doch einige dieser Dienste sind selbst anfällig für Angriffe.[2]

Laut „Data Breach Investigations Report (DBIR) 2021“ von Verizon entfielen 61 % aller Datenschutzverletzungen auf gestohlene Zugangsdaten.[3]

Der **ForgeRock Consumer Identity Breach Report 2020** hat gezeigt, dass unbefugte Zugriffe als häufigste Methode bei 43 % der Angriffe durch Cyberkriminelle zum Einsatz kamen ein. Der Bericht, in dem verschiedene Branchen betrachtet wurden, kam zu dem Ergebnis, dass 34 % der Datenschutzverletzungen auf das Gesundheitswesen und 12 % auf den Finanzdienstleistungssektor entfielen.[4]

Das geschäftliche E-Mail-System des Gesundheitsnetzwerks UnityPoint Health im US-amerikanischen Iowa wurde 2018 Opfer einer Reihe von E-Mail-Phishing-Angriffen, bei denen es die Angreifer auf die Zugangsdaten von Mitarbeitern abgesehen hatten. Ziel war es wahrscheinlich, den Unternehmen Geld zu stehlen, doch die Angriffe führten auch dazu, dass geschützte Patientendaten und/oder persönliche Finanzdaten kompromittiert wurden.[5]

Datenschutzverletzungen aufgrund von Zugangsdatendiebstahl werden nicht aufhören. Unternehmen können zwar versuchen, sich und ihre Mitarbeitenden und Kunden durch Sicherheitsschulungen, E-Mail-Sicherheitsmaßnahmen und eine stärkere Authentifizierung zu schützen. Solange jedoch die Authentifizierung mit Benutzernamen und Passwörtern nicht durch sicherere Methoden ersetzt wird, bleibt der Zugangsdaten-Diebstahl die bevorzugte Taktik von Angreifern.

In diesem Whitepaper empfehlen wir, die auf Industriestandards basierende passwortlose Authentifizierung von ForgeRock zu verwenden, um die Authentifizierung mittels Benutzernamen und Passwörtern zu reduzieren oder gleich ganz vermeiden und die Sicherheit in Ihrem Unternehmen zu erhöhen.

Sehen wir uns jedoch zunächst an, welche Alternativen zurzeit zum Einsatz kommen.

Starke Authentifizierung

Viele Anwendungen und Services bieten heute eine „starke Authentifizierung“ mittels Zwei-Faktor-Authentifizierung (2FA) oder Multi-Faktor-Authentifizierung (MFA).

Bei der 2FA muss sich der Benutzer zuerst mit einem Benutzernamen und Passwort und danach mit einem zweiten Faktor authentifizieren, der auf einem Einmal-Passwort (One-Time Passcode, OTP) basiert. Der Benutzer erhält dieses Passwort üblicherweise über eine Authenticator-Anwendung, eine Push-Benachrichtigung in einer mobilen App oder – und das ist der unsicherste Weg – über das SMS-Textnachrichtenprotokoll. Bei der 2FA muss für jeden Authentifizierungsversuch der zweite Authentifizierungsfaktor angegeben werden.

Die MFA beinhaltet mehr kontextabhängige Attribute – zusätzliche Authenticator-Arten und Kontextinformationen – wie etwa das Benutzergerät, den Browser, die IP, den Standort oder die Tageszeit. Bei einigen MFA-Lösungen muss sich der Benutzer je nach Sitzungskontext mehr oder weniger authentifizieren.

Durch die Verwendung von zwei oder mehr Faktorarten steigt die Sicherheit. Die Kombination aus zwei oder mehr nicht eindeutigen Faktoren kann hingegen mehr schaden als nützen.

Das Prinzip, das beiden Methoden zugrunde liegt, ist, dass sich ein Benutzer bei einer starken Authentifizierung mit einer Kombination aus mindestens zwei eindeutigen Faktoren authentifizieren muss. Der Benutzername und das Passwort sind „Wissensfaktoren“ (etwas, das die Benutzer wissen). Mobile Geräte, Hardware-Token oder Smartcards sind „Besitzfaktoren“ (etwas, das sie besitzen). Biometrische Eigenschaften wie Fingerabdrücke oder Gesichtserkennungsmerkmale sind Beispiele für „inhärente Faktoren“ (etwas, das ihnen eigen ist).

Wenn sich Benutzer auf Websites erst mit Benutzernamen und Passwort anmelden und dann andere Wissensfaktoren wie etwa die Antworten auf „Sicherheitsfragen“ eingeben müssen, die sie vielleicht im Laufe der Zeit vergessen haben, ist der zweite Authentifizierungsfaktor nutzlos. Antworten auf gängige Sicherheitsfragen (zum Beispiel nach dem Mädchennamen der Mutter) können in Behördendaten, sozialen Netzwerken oder über Social Engineering ermittelt werden.

2FA und MFA sind sicherer als die Authentifizierung mit Benutzername und Passwort, aber sie haben auch ihre Grenzen. Die 2FA kann den Benutzern schnell lästig werden, wenn sie sich immer doppelt authentifizieren müssen, besonders wenn sie dafür erst eine Authenticator-App oder eine SMS aufrufen müssen, um das Einmalpasswort zu finden und einzugeben. Die MFA ist zudem oft schwierig zu implementieren und basiert teils auf der Konfiguration von Richtlinien, was den Sicherheitsteams nicht die nötige Agilität und Präzision beim Zugangsmanagement bietet. Eine erfolgreiche MFA- oder 2FA-Implementierung hängt zudem in weiten Teilen von der Qualität und Flexibilität der Identity und Access Management-Lösung eines Unternehmens ab.

Ein standardbasierter Authentifizierungsansatz

Die bessere Option für eine starke Authentifizierung ist ein standardbasierter Ansatz, der die Verwendung von Benutzername und Passwort reduziert oder ganz vermeidet. Die Analysten von Gartner empfehlen, Passwörter durch eine biometrische Authentifizierung zu ersetzen. Sie prognostizieren, dass 60 % der großen und globalen Unternehmen sowie 90 % der mittleren Unternehmen bis 2022 in mehr als 50 % der Anwendungsfälle im Bereich Authentifizierung Passwörter durch andere Methoden ersetzen werden.[6]

Anbieter von Browsern, Betriebssystemen und Hardware treten der FIDO-Allianz bei und werden in Zukunft FIDO2 unterstützen.[7]

Das World Wide Web Consortium (W3C) ratifizierte 2019 den Web Authentication-Standard (WebAuthn) Fast Identity Online 2 (FIDO2), der eine Authentifizierung ohne Benutzernamen und Passwörter ermöglicht.

Der ursprüngliche FIDO-Standard, auch als „Universal 2 Factor“ (U2F) bekannt, nutzt ein skalierbares Modell mit öffentlichem/privatem Schlüssel, bei dem für jeden Dienst ein neues Schlüsselpaar generiert wird. Dabei werden die Schlüsselpaare getrennt, um so die Aufrechterhaltung des Datenschutzes sicherzustellen.[8] Der Standard ermöglicht die „passwortlose“ Authentifizierung bei Online-Diensten mit einem Hardware-Sicherheitsschlüssel.

Der neuere FIDO2-Standard ist die FIDO-Weiterentwicklung ohne Benutzername und Passwort und beruht auf Zugangsdaten, die lokal auf einem Benutzergerät gespeichert sind. FIDO2 besteht aus zwei Spezifikationen:

- Einer webbasierten API namens **Web Authentication (WebAuthn)**, die bei Web-Anwendungen eine „passwortlose“ Authentifizierung mit öffentlichem Schlüssel und Authenticator ermöglicht. WebAuthn unterstützt Zugangsdaten auf Basis des ursprünglichen FIDO U2F-Standards und FIDO2-Zugangsdaten.

- Dem FIDO2 **Client to Authenticator Protocol (CTAP2)**, das die Kommunikation zwischen Client-Anwendungen und FIDO2-fähigen Authenticators über FIDO2-fähige Browser und Betriebssysteme ermöglicht.

Authenticator-Arten

FIDO2 nutzt ein Schlüsselpaar bestehend aus einem öffentlichen und einem privaten Schlüssel. Diese sind sicher auf lokaler Hardware bzw. in FIDO2-konformen Browsern gespeichert, die mit Diensten interagieren, um mithilfe des öffentlichen/privaten Schlüssels sichere Zugangsdaten für den jeweiligen Dienst zu erstellen. Die privaten Schlüssel der Schlüsselpaare werden lokal gespeichert und verlassen den Authenticator des Benutzers nicht. Die öffentlichen Schlüssel werden vom Authentifizierungsserver zum Verschlüsseln und Signieren der Kommunikation mit dem Endgerät des Benutzers verwendet.

Die Speicherfähigkeit des lokalen Authenticators des Benutzers bestimmt, ob die Authentifizierung sowohl ohne Benutzernamen als auch ohne Passwörter erfolgen kann.

Plattform-Authenticators auf Basis des Trusted Platform Module (TPM) oder einer sicheren Enklave, die auf vielen Laptops und Smartphones installiert ist, werden normalerweise mit einem biometrischen Sensor entsperrt, so zum Beispiel bei Microsoft Windows Hello oder der Apple TouchID.

Plattformübergreifende oder „wandernde" Hardware-Authenticators präsentieren einem anderen Dienst oder Gerät die Zugangsanforderung des Benutzers. Beispiele hierfür sind Google Titan-Sicherheitsschlüssel, YubiKeys oder Duo-Authenticators, die USB, Near-Field Communication (NFC) und Bluetooth verwenden. Der Authenticator wird durch Verbinden mit einem USB-Anschluss, Drücken einer Taste oder Tippen aktiviert und sendet eine signierte Antwort, die die Benutzeranmeldung bestätigt. Auch Smartphones können als Authenticators dienen.

Durch die sicheren Zugangsdaten, die auf der eigenen vertrauenswürdigen Hardware gespeichert sind, ermöglicht FIDO2 WebAuthN die Authentifizierung ohne Benutzernamen und Passwörter und schließt damit potenzielle Datenschutzverletzungen durch Zugangsdaten-Diebstahl praktisch aus.

Passwortlose Authentifizierung von ForgeRock

Die passwortlose Authentifizierung von ForgeRock implementiert den FIDO2 WebAuthn-Standards in ForgeRock Intelligent Access. Damit können Sie sichere und nahtlose Benutzererlebnisse für die Authentifizierung ohne Passwörter und teilweise sogar ohne Benutzernamen entwickeln.

Die passwortlose Authentifizierung von ForgeRock macht den Zugangsdaten-Diebstahl durch Phishing-Angriffe, die Mehrfachverwendung von Passwörtern, Credential Stuffing, Keylogger usw. praktisch unmöglich und verkleinert so die Angriffsfläche des Unternehmens.

Vorteile einer passwortlosen Authentifizierung

- **Sicherheit:** Die Anmeldedaten sind für jede Website eindeutig und verlassen niemals das Gerät des Benutzers. Im Gegensatz zum Benutzernamen und Passwort werden die Zugangsdaten nie über eine Verbindung übertragen, wodurch Person-in-the-Middle-Angriffe vermieden werden.
- **Komfort:** Die Lösung nutzt einfache integrierte Methoden wie Fingerabdruckleser oder Kameras oder verwendet die benutzerfreundlichen FIDO-Sicherheitsschlüssel. Die Benutzer können das Gerät auswählen, das ihren Anforderungen am besten entspricht.
- **Datenschutz:** Die Schlüssel sind eindeutig und können nicht verwendet werden, um Benutzer über Websites hinweg zu verfolgen. Biometrische Daten verlassen niemals das Gerät des Benutzers.

„Ohne Benutzernamen und Passwörter können wir jetzt allen unseren Benutzern ein sehr viel besseres Benutzererlebnis bieten und zudem die Zahl der Service-Desk-Anrufe wegen vergessener Passwörter reduzieren.“

– Doug Neumann, IT-Manager bei der Nationalen Behörde für nukleare Sicherheit (NNSA) der USA

So funktioniert die passwortlose Authentifizierung

ForgeRock nutzt für die passwortlose Authentifizierung die Baumstrukturen in ForgeRock Intelligent Access sowie WebAuthn-spezifische Knoten für die Registrierung und Authentifizierung. Um eine passwortlose Authentifizierung verwenden zu können, müssen sich Benutzer zunächst mit ihrem Benutzernamen und ihrem Passwort beim Identitätsverzeichnis authentifizieren und sich so registrieren, damit ForgeRock die Benutzer und ihre jeweiligen Geräte identifizieren kann.

Wenn ein Benutzer erstmals versucht, sein Gerät zu registrieren, erkennt ForgeRock Intelligent Access, ob das Gerät den WebAuthn-Standard unterstützt. Ist die Geräteregistrierung erfolgt, weist ForgeRock das Gerät des Benutzers an, ein eindeutiges Paar aus öffentlichem/privatem Schlüssel für die Kommunikation mit ForgeRock zu erstellen. Wenn sich der Benutzer anschließend über den integrierten biometrischen Sensor bei seinem Gerät authentifiziert, wird der private Schlüssel des Benutzers – der sicher im persistenten Speicher gespeichert ist und das Gerät nie verlässt – für das Signieren von Authentifizierungsaufforderungen verfügbar.

ForgeRock gibt eine Aufforderung an das Gerät des Benutzers aus und verschlüsselt sie mit dem öffentlichen Schlüssel des Benutzers. Der private Schlüssel auf dem Benutzergerät signiert die Aufforderung, die ForgeRock mit dem öffentlichen Schlüssel des Benutzers verifiziert. Dieser Prozess stellt eine sichere Verbindung zwischen dem Hardware-Gerät des Benutzers und ForgeRock her und ermöglicht anschließend die Anmeldung ohne Passwort.

Die herkömmlichen Benutzererlebnisse mit Benutzernamen und Passwörtern in Verbindung mit starker Authentifizierung sollten als alternative Authentifizierungsmethode erhalten bleiben für den Fall, dass der Benutzer sich nicht über sein registriertes, vertrauenswürdiges Gerät bei ForgeRock authentifizieren kann. (Beispiel: Sein vertrauenswürdiges Gerät ist nicht verfügbar, verlorengegangen oder wurde gestohlen.)

Passwortlose Authentifizierung ohne biometrische Daten

Einige Menschen können Biometrie nicht nutzen, oder sie wird von ihrem Unternehmen nicht unterstützt. Sie können in dem Fall die passwortlose Authentifizierung mit einem beliebigen externen PIN-geschützten Authenticator (etwas, das Sie wissen, und etwas, das Sie besitzen) nutzen. Das können FIDO2-fähige Smartcards, FIDO2- oder Universal 2 Factor-fähige Hardware-Sicherheitsschlüssel oder Smart Watches sein. ForgeRock unterstützt die passwortlosen FIDO2 Web Authentication-Funktionen für zahlreiche Authenticators sowie Nachweisformate und -arten. Weitere Informationen hierzu lesen Sie im **Lösungsüberblick**.

Konfiguration der passwortlosen Authentifizierung

Die passwortlose Authentifizierung umfasst eine Reihe von Funktionen in ForgeRock Intelligent Access, die speziell für die Unterstützung des FIDO2/WebAuthn-Standards konzipiert wurden. Benutzer können so vertrauenswürdige Geräte registrieren und die darin integrierten Funktionen für die lokale Speicherung von Zugangsdaten nutzen. In den Baumstrukturen von Intelligent Access existieren drei vorkonfigurierte Knoten. Diese Knoten können einfach per Drag & Drop in die Intelligent Access-Benutzeroberfläche gezogen werden, um Benutzererlebnisse zu erstellen. Weitere Informationen zu den Baumstrukturen und Knoten von Intelligent Access finden Sie im Whitepaper „**Wir stellen vor: ForgeRock Intelligent Access**“.

Registrierung von Geräten

Um die passwortlose Authentifizierung verwenden zu können, müssen sich Benutzer zunächst mit ihrem Benutzernamen und ihrem Passwort authentifizieren und ihr Gerät registrieren. Erstellen Sie dazu ein entsprechendes Benutzererlebnis und fügen Sie einen WebAuthn-Registrierungsknoten nach dem Erfassungsknoten für Benutzername/Passwort sowie dem Data-Store-Entscheidungsknoten hinzu. Nachdem der Benutzer einen Authenticator, der die Vorgaben des Knotens erfüllt, erfolgreich registriert hat, wird die Evaluierung innerhalb der Baumstruktur fortgeführt und erfolgreich abgeschlossen. Die passwortlose Authentifizierung schlägt fehl, wenn der Client WebAuthn nicht unterstützt. Das kann der Fall sein, wenn ein nicht unterstützter Browser verwendet wird oder die Registrierung mit der falschen Art von Authenticator erfolgt ist. Kommt es bei der Client-Registrierung zu einer Zeitüberschreitung, wird ein Client-Fehler ausgegeben.

Validierung der Benutzeridentität

Jeder Authenticator, der für die passwortlose Authentifizierung verwendet wird, muss mit der Benutzeridentität abgeglichen werden, um als sicher eingestuft zu werden. Unternehmen müssen Benutzer entweder persönlich oder mithilfe eines vertrauenswürdigen digitalen Identitätsnachweisverfahrens überprüfen, wenn sie Authenticators registrieren. Weitere Informationen zu Identitätssicherheitsstufen und digitalen Identitätsnachweisverfahren in ForgeRock Intelligent Access finden Sie im Whitepaper **Reduce Government Services Fraud – Incorporate Identity Proofing Into Citizen Registration and Authentication**.[9] Weitere Informationen zur Integration kreditbasierter Identitätsprüfungen finden Sie im Whitepaper **Reduce the Total Cost of Fraud**.

Authentifizierung ohne Benutzername

Damit Benutzer sich künftig ohne Eingabe des Benutzernamens authentifizieren können, aktivieren Sie die Option „Username to device“ rechts neben dem Registrierungsknoten.

Für die Authentifizierung ohne Benutzername ist es erforderlich, dass die Authenticators des Benutzers die Speicherung von Resident Keys unterstützen.

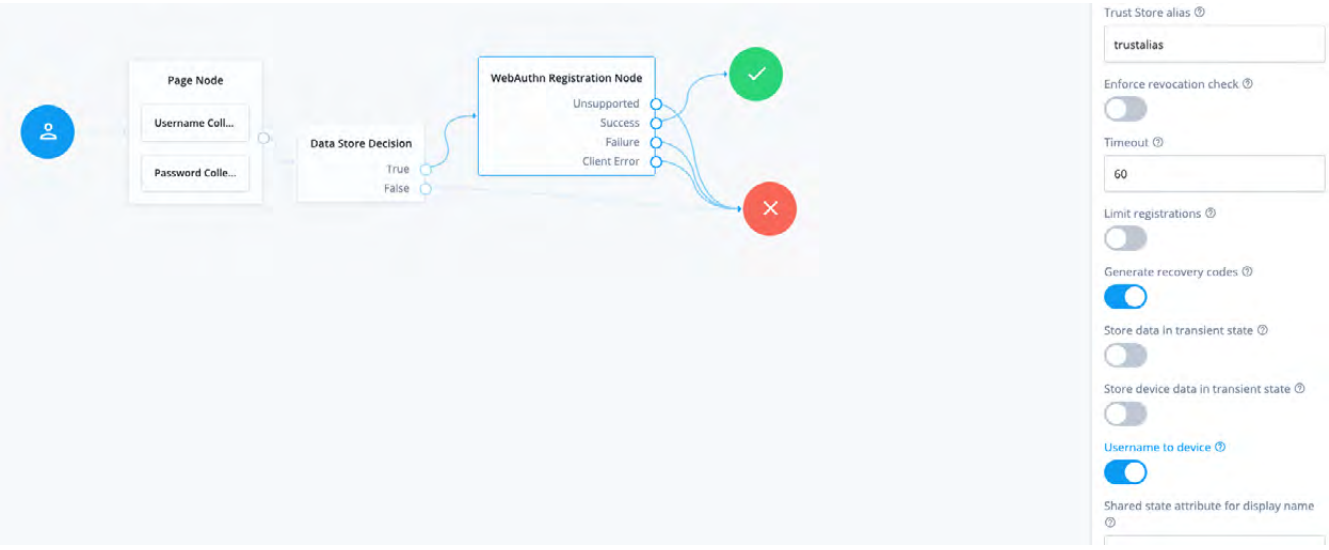

Abbildung 1: Passwortlose Authentifizierung ohne Benutzername

Wenn sich der Benutzer registriert hat und anmelden will, wird der WebAuthn Authentication Node ausgeführt und bietet dem Benutzer nun eine Anmeldung ohne Benutzernamen.

Analyse von Geräten

Wenn Sie eine zusätzliche Analyse auf einem Benutzergerät durchführen möchten und die Registrierung so lange verzögert werden soll, bis das Ergebnis der Analyse vorliegt, können Sie den WebAuthn Device Storage Node (Gerätespeicherknoten) in die Baumstruktur Ihrer WebAuthn-Registrierung aufnehmen. Dieser Knoten ist optional.

Hier ein Beispiel dafür, wie Sie ihn nutzen können: Angenommen Sie wollen die Authentifizierung ohne Benutzername und Passwort aktivieren, dies soll jedoch nur für Mitarbeitende möglich sein, die vom Unternehmen ausgegebene Laptops eines bestimmten Herstellers nutzen, auf denen ein biometrisches TPM installiert ist. Sie können den WebAuthn Device Storage Node in die Baumstruktur der Registrierung aufnehmen und einen benutzerdefinierten skriptbasierten Decision Node (Entscheidungsknoten) einfügen, um gerätespezifische Nachweisdaten zu erfassen (z. B. Seriennummer und für mehr Sicherheit eine Zertifikatskette zur Bestätigung der Echtheit des Geräts). Dies verhindert, dass sich rechtmäßige Benutzer über nicht verwaltete Geräte authentifizieren, und stärkt die Sicherheit Ihres Unternehmens.

Zur Aktivierung des WebAuthn Device Storage Node aktivieren Sie rechts auf dem Bildschirm die Option „Store data in transient state“. „Transient state“ (Übergangszustand) bedeutet hierbei, dass die Gerätedaten nur im temporären Speicher gespeichert werden, damit ForgeRock sie für die Analyse nutzen kann.

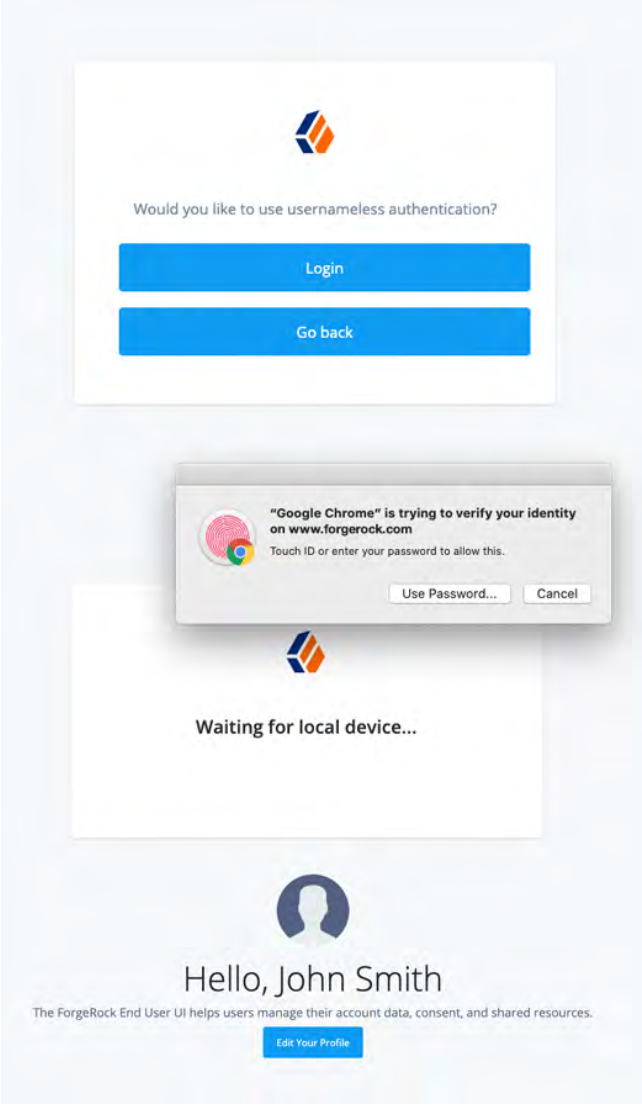

Abbildung 2: Authentifizierung ohne Benutzername

Abbildung 3: WebAuthn Device Storage Node in der Registrierung

Alternativen zur passwortlosen Authentifizierung

Benutzer sollten stets eine Alternative zur passwortlosen Authentifizierung haben für den Fall, dass ihr registriertes Gerät verlorengeht oder gestohlen wird oder sie Browser bzw. Geräte nutzen, die FIDO2-Zugangsdaten und WebAuthn noch nicht unterstützen. Sie können Benutzererlebnisse entwickeln, die Zugangsdaten bestehend aus Benutzername und Passwort erfassen und MFA durch TMP (Trusted Platform Module), mobile Push-Benachrichtigungen oder Drittanbieter-Authenticators ergänzen.

Einsatzmöglichkeiten für die passwortlose Authentifizierung

Die passwortlose Authentifizierung von ForgeRock eignet sich ideal für Mitarbeitende, die sich bei Cloud- oder On-Premises-Anwendungen authentifizieren müssen. Die passwortlose Authentifizierung von ForgeRock kann sowohl für die Authentifizierung bei der Erstanmeldung als auch für die starke Authentifizierung, einschließlich der Transaktionsautorisierung, verwendet werden. Weitere Informationen zur starken Authentifizierung und zur Transaktionsautorisierung finden Sie im Whitepaper „**Wir stellen vor: ForgeRock Intelligent Access**“.

Da immer mehr Browser und verbraucherorientierte Anwendungen FIDO2 und den WebAuthn-Standard unterstützen, können Sie auch Benutzererlebnisse

Die passwortlose Authentifizierung von ForgeRock kann sowohl für die Authentifizierung bei der Erstanmeldung als auch für die starke Authentifizierung, einschließlich der Transaktionsautorisierung, verwendet werden.

ohne Passwort für verschiedene Anwendungsfälle Ihrer Kunden entwickeln. Der WebAuthn-Standard wird derzeit in sozialen Medien, im Finanzdienstleistungssektor, im Gaming-Bereich und in Cloud-Speicheranwendungen genutzt.

Fazit

Mit ForgeRock Intelligent Access können Sie schnell und einfach eine sichere Authentifizierung ohne Benutzernamen und Passwörter für Mitarbeitende und Kunden entwickeln. Diese Erlebnisse lassen sich innerhalb von Minuten erstellen und unterstützen mehrere Authenticators gleichzeitig, wodurch Sie im Vergleich zu älteren starken Authentifizierungslösung erhebliche Kosten sparen. Die passwortlose Authentifizierung von ForgeRock verbessert die Sicherheit, den Komfort und den Datenschutz für Ihre Benutzer.

[1]https://fidoalliance.org/what-is-fido/
[2]https://www.welivesecurity.com/2020/03/19/security-flaws-found-in-popular-password-managers/
[3]https://enterprise.verizon.com/resources/reports/dbir/
[4]https://www.forgerock.com/resources/2020-consumer-identity-breach-report
[5]https://www.unitypoint.org/filesimages/About/Security%20Substitute%20Notification.pdf
[6]https://www.gartner.com/smarterwithgartner/embrace-a-passwordless-approach-to-improve-security/
[7]https://www.theverge.com/2020/6/24/21301509/apple-safari-14-browser-face-touch-id-logins-webauthn-fido2
[8]https://www.yubico.com/blog/what-is-fido2/
[9]https://www.forgerock.com/resources/whitepaper/reduce-government-services-fraud

Über ForgeRock

ForgeRock® (NYSE: FORG) ist ein weltweit führender Anbieter im Bereich digitale Identität. Das Unternehmen liefert moderne und umfassende Identity und Access Management-Lösungen für Verbraucher*innen, Mitarbeiter*innen und Dinge und bietet so einen einfachen und sicheren Zugang zur vernetzten Welt. Mit ForgeRock orchestrieren, verwalten und sichern mehr als 1.300 globale Unternehmen den gesamten Lebenszyklus von Identitäten, angefangen bei dynamischen Zugriffskontrollen, Governance und APIs bis hin zur Speicherung autoritativer Daten – verwendbar in jeder Cloud- oder Hybridumgebung. Das Unternehmen mit Hauptsitz in San Francisco, Kalifornien, unterhält Niederlassungen auf der ganzen Welt. Für weiterführende Informationen und kostenlose Downloads besuchen Sie gerne unsere Website **www.forgerock.com**.

Folgen Sie uns

ForgeRock