thalesgroup.com

THALES

Authentifizierung ohne Passwort:

Wie der Verzicht auf Passwörter mehr Sicherheit schaffen könnte

White Paper

Warum Passwörter schlecht sind

Passwörter gehören zu den ältesten Sicherheitstools in der Welt der Software und des Internets. Heutzutage können sie Unternehmen jedoch aus verschiedenen Gründen nicht genug Sicherheit bieten.

Passwortermüdung fördert Nachlässigkeit

Richtlinienbasierte Passwortstärken und -rotation führen zu Passwortermüdung und tragen so zu einer schlechten Passwortverwaltung bei. Der Data Breach Investigation Report[1] von Verizon zeigt, dass **mehr als 70 Prozent der Mitarbeiter** Passwörter für berufliche und private Konten wiederverwenden. Kriminelle Akteure können also die Anmeldedaten eines Mitarbeiters missbrauchen, um Zugriff auf andere Anwendungen und sensible Kundeninformationen zu erhalten.

81%

der Sicherheitsverletzungen sind auf schwache oder gestohlene Anmeldedaten zurückzuführen

~40

Durchschnittlich hat jeder ca. 40 Online-Konten

4 von 5

Die Benutzer verwenden dieselben Passwörter für verschiedene Konten

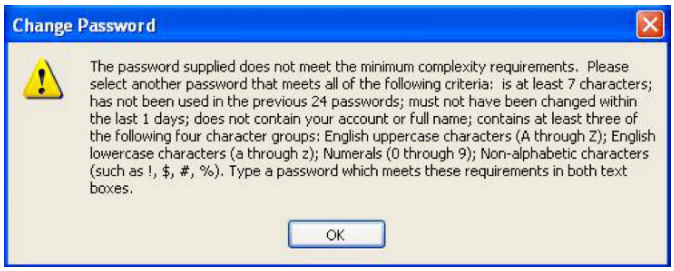
„123456“
„Passwort“

2018 noch immer unter den beliebtesten Passwörtern

Viele Nutzer neigen dazu, einfach zu knackende Passwörter zu nutzen, um sie nicht zu vergessen. Eine Analyse von mehr als 5 Millionen geknackten Passwörtern ergab, dass 10 Prozent der Betroffenen eines der 25 schlechtesten Passwörter verwendeten[2]. 7 Prozent der Unternehmensanwender nutzen extrem schwache Passwörter.

Passwörter beeinträchtigen die Benutzererfahrung

Recherchen der Carnegie Mellon University ergaben, dass eine auf die richtige Weise verfasste Passwortrichtlinie für ein Unternehmen eine erhöhte Sicherheit bedeuten kann. Dennoch besteht weniger Einigkeit darüber, was in eine effiziente Richtlinie aufgenommen werden sollte. Zur Verdeutlichung: Wenn eine Richtlinie vorschreibt, dass das Passwort eine Zahl enthalten soll, wählen Benutzer in der Regel stets dieselbe Zahl aus oder verwenden die Zahl in ihren Passwörtern an der gleichen Stelle[3].



Einige Passwortrichtlinien führen dazu, dass Passwörter schwer zu merken oder einzugeben sind. Das hat zur Folge, dass sich die Benutzer ihre Passwörter notieren, für verschiedene Konten wiederverwenden oder sie an Freunde weitergeben und so deren Sicherheit untergraben. Außerdem vergessen sie die Passwörter regelmäßig und der Helpdesk versinkt in Arbeit, um sie wiederherzustellen.

Passwörter können die Benutzersicherheit einschränken

Ironischerweise können Passwörter die Sicherheit beeinträchtigen, indem sie als Angriffsvektor dienen. Laut dem Data Breach Investigations Report von Verizon aus dem Jahr 2018 sind **81 % der Sicherheitsverletzungen** auf schwache, gestohlene oder wiederverwendete Passwörter zurückzuführen[4]. Bedrohungen wie Man-in-the-Middle- und Man-in-the-Browser-Angriffe täuschen die Benutzer, indem sie ihnen einen vermeintlichen Anmeldebildschirm präsentieren und sie dazu auffordern, ihre Passwörter einzugeben. Die Cloud ist noch unsicherer. Anmeldeseiten, die in der Cloud gehostet werden, liegen komplett offen und ermöglichen kriminellen Akteuren Phishing- oder Brute-Force-Angriffe auf öffentlich bekannte Anmeldeseiten wie outlook.com.

1 https://enterprise.verizon.com/resources/reports/dbir/
2 https://www.vice.com/en_us/article/paqd4m/too-many-people-are-still-using-password-as-a-password
3 https://cups.cs.cmu.edu/passwords.html
4 https://enterprise.verizon.com/resources/reports/DBIR_2018_Report_execsummary.pdf

Die Konzentration auf Passwortregeln ist nur eine Ablenkung. Um zu verstehen, warum das so ist, ist es wichtig, sich die verschiedenen Angriffe auf Passwörter genauer anzusehen und zu prüfen, wie das Passwort den Angreifern in die Karten spielt. Im Folgenden wird beschrieben, wie Passwörter heutzutage für gewöhnlich geknackt werden[5]:

Angriff	Auch bekannt als	Häufigkeit	Schwierigkeit
Credential Stuffing	Breach Replay, List Cleaning	Sehr hoch – mehr als 20 Millionen Konten täglich	Sehr einfach: Es werden Annmeldedaten von gehackten Websites mit schlechten Data-at-Rest-Richtlinien gekauft und auf Übereinstimmungen in anderen Systemen geprüft. Einsatzbereite List Cleaning-Tools sind verfügbar.
Phishing	Abfangen von Anmeldedaten	Sehr hoch. 0,5 % aller eingehenden E-Mails.	Einfach: Es werden E-Mails versendet, in denen der Adressat entweder mit Unterhaltung geködert oder bedroht wird. Er wird gebeten, über einen Link die Doppelgänger-Webseite zu öffnen, um sich anzumelden. Erfassen von Anmeldedaten Ganz einfach mit Tools wie Modlishka oder ähnlichen.
Password Spraying	Guessing, Hammering, Low-and-slow	Sehr hoch – wird bei mindestens 16 % aller Angriffe genutzt. Manchmal bis zu hunderttausende Sicherheitsverletzungen täglich. Millionen	Banale Methode: Verwendung einfach zugänglicher Benutzerlisten, dasselbe Passwort wird für eine große Menge an Benutzernamen ausprobiert. Steuert Geschwindigkeit und wird auf viele IPs verteilt, um nicht entdeckt zu werden Die Tools dafür sind einsatzbereit und zu niedrigen Preisen erhältlich.

Sicherheitsverletzungen können katastrophale Folgen haben. Ein gestohlener Datenträger verursacht im Durchschnitt Kosten von 148 USD, dagegen liegen die **Gesamtkosten einer Datensicherheitsverletzung durchschnittlich bei 3,86 Millionen USD**[6].

Wenig Fortschritt in Sachen Passwortproblem

Bisher haben die Unternehmen versucht, diese Probleme anzugehen, indem sie eine Reihe weiterer Authentifizierungsmethoden zusätzlich zu alten Passwörtern implementieren oder diese ersetzen. Die vorherrschende Methode ist die Zweifaktor-Authentifizierung (2FA), auch bekannt als Multifaktor-Authentifizierung (MFA).

Es gibt unzählige Authentifizierungsfaktoren, die als Teil eines Multifaktor-Systems verwendet werden können und sich dennoch in der Regel in drei größere Gruppen einteilen lassen:

- **Wissensfaktor** („etwas, das Ihnen bekannt ist"): Das System akzeptiert Sie, weil Sie eine bestimmte Information kennen. Dazu gehören PINs, die Beantwortung von Sicherheitsfragen, Steuererklärungsdaten usw.
- **Besitzfaktor** („etwas, das Sie besitzen"): Sie werden vom System akzeptiert, wenn Sie beweisen können, dass Sie ein bestimmtes physisches Gerät besitzen. Beispiele dafür sind SMS-Codes, Authentifizierungs-Apps, USB-Schlüssel, Wireless-Tags, Kartenlesegeräte usw.
- **Inhärenzfaktor** („das, was Sie sind"): Das System akzeptiert Sie anhand von biometrischem Vergleichen. Dazu gehören Fingerabdruck-Scanner, Netzhaut-Scanner, Stimmerkennung usw.

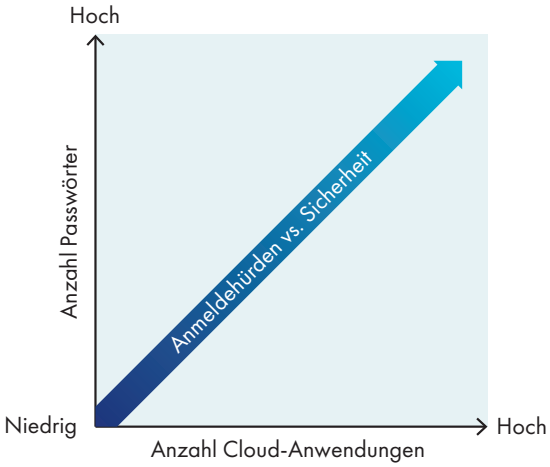
Eine Methode der MFA ist die **SMS-Nachricht**. Dieses MFA-Modell ist äußerst praktisch, birgt jedoch Risiken. Zunächst müssen Sie dem Service ausreichend vertrauen, um Ihre Telefonnummer preiszugeben, denn unseriöse Dienste könnten diese für Werbezwecke missbrauchen oder zu Profitzwecken weiterverkaufen. Da Telefonnummern nicht gerätegebunden sind, können Hacker die SMS-basierte Authentifizierung umgehen, ohne Ihr Telefon überhaupt zu berühren. Dazu müssen sie einfach nur einen SIM-Tausch-Angriff starten, indem sie das Mobilfunkunternehmen der Zielperson anrufen und den Vertreter durch Täuschung dazu bringen, die Zieltelefonnummer auf eine ihrer SIM-Karten zu übertragen.

Einmal-Passwörter sind sicherer, da die Codes kryptographisch und basierend auf einem Geheimschlüssel generiert werden, der bei der Kontoerstellung erzeugt wird. Auf diese Weise erhalten Sie gültige Codes auf Ihrem Gerät, auch wenn Sie keinen Empfang haben und/oder keinen mobilen Service nutzen. Die auf Einmalpasswörter basierende Multifaktor-Authentifizierung kann dem Smartphone des Benutzers in Form von mobilen Token oder als eigenständiges Gerät, zum Beispiel als Schlüsselanhänger, bereitgestellt werden.

Die Zugriffsumgebungen werden zunehmend komplexer und es gibt mehr Zugriffspunkte als je zuvor. Aus diesen Gründen haben Unternehmen allen Grund, eine Multifaktor-Authentifizierung hinzufügen. Die Anwendung der MFA für jeden einzelnen Anmeldeversuch ist jedoch nicht gerade benutzerfreundlich und eher unpraktisch, da die Anzahl der zu schützenden Cloud-Services viel zu hoch ist.

5 https://techcommunity.microsoft.com/t5/Azure-Active-Directory-Identity/Your-Pa-word-doesn-t-matter/ba-p/731984
6 https://www.ibm.com/security/data-breach

Wir befinden uns an einem kritischen Wendepunkt, an dem das Aufkommen cloud-basierter Technologien (und die damit verbundenen Bedrohungen) mit zunehmend mobilen Mitarbeitern kollidiert, die in ihrer Arbeit auf keinen Fall durch unpraktische Authentifizierungsbereitstellungen beeinträchtigt werden möchten. Wir brauchen daher eine passwortlose und benutzerfreundliche Authentifizierung mit einem hohen Sicherheitsniveau. Bislang fehlten dafür aufgrund mangelnder Technologie die Lösungen. Aber wir befinden uns mitten im technologischen Wandel.



Was hat sich geändert und warum sieht es für die Zukunft gut aus?

Das Bewusstsein für die Bedeutung von Online-Sicherheit und Datenschutz hat in den letzten Jahren deutlich zugenommen, besonders bei staatlichen Einrichtungen und Regulierungsbehörden. Datenschutzverletzungen und Sicherheitsvorfälle sind in Unternehmen schon seit geraumer Zeit keine Seltenheit mehr, sie hatten jedoch nur milde rechtliche und finanzielle Konsequenzen zur Folge. Das sieht heute anders aus.

Die Regulierungsbehörden haben reagiert und immer mehr Unternehmen fügen ihren Datenschutzmaßnahmen strengere Authentifizierungen hinzu. Eine der relevantesten Maßnahmen der Aufsichtsbehörden ist die Datenschutz-Grundverordnung (DSGVO), in der Standards für die Zugriffssicherheit festgelegt sind. Unternehmen, die diese Verordnung missachten und die Daten ihrer Kunden nicht schützen, werden mit Geldstrafen belegt. Die DSGVO bezieht sich nur auf das Rechtsgebiet der EU, da aber viele Unternehmen außerhalb der EU ansässig sind und Geschäfte im EU-Raum tätigen, gilt dieses Regelwerk weltweit als Sicherheitsstandard.

In Zeiten, in denen immer mehr Unternehmen strengere Authentifizierungsmöglichkeiten implementieren und Datenschutzverletzungen immer häufiger auf die Kompromittierung von Passwörtern zurückzuführen sind, wird es für ein Unternehmen zunehmend schwerer, einer DSGVO-Aufsichtsbehörde geeignete Argumente zu liefern, dass eine allein auf Passwörter basierende Authentifizierung für angemessene Sicherheit sorgt. Dem Unternehmen drohen unter Umständen Geldstrafen, die weitaus höher ausfallen können als die Investition in den Wechsel von Passwörtern zu starker Authentifizierung.

Weitere branchenspezifische Vorschriften gehen in Bezug auf die Verwendung von Authentifizierungstechnologie noch weiter ins Detail. Ein Beispiel dafür ist die Zahlungsdienstrichtlinie 2 (PSD2) zur Regelung von e-Commerce und Online-Finanzdiensten in Europa, die eine Zweifaktor-Authentifizierung vorschreibt. PSD2 fördert außerdem den Einsatz von Sicherheitskarten, mobilen Geräten und biometrischen Scannern zur Verbesserung der Benutzerfreundlichkeit ohne Sicherheitsverlust.

Abschließend erläutert NIST in den Leitfäden zu digitalen Identitäten, dass Unternehmen den Wechsel von Passwörtern und Einmalpasswörtern hin zu moderner, starker Authentifizierung vollziehen müssen. NIST empfiehlt, dass ein Gerät kryptographische Geheimschlüssel als neue Konto-Anmeldedaten erstellt und nutzt, die anschließend auf dieselbe Art und Weise sicher gespeichert werden, wie es heute schon die meisten Smartphones mit Fingerabdrucksdaten tun.

Technologische Innovationen wie die Verbreitung von mobilen Geräten mit integrierten Funktionen zur Biometrie, Geolokalisierung und anderen Sensoren ermöglichen die Anwendung passwortloser Lösungen, für die keine traditionellen Passwörter mehr erforderlich sind, da eine adaptive und kontextbasierte Authentifizierung möglich ist. Diese Sensoren erfassen im Hintergrund Daten zum Nutzerverhalten, ohne dass dafür eine Aktion des Nutzers notwendig ist. Mithilfe von Sensormetriken wird das Nutzerverhalten laufend und regelmäßig überprüft, um die Benutzerauthentifizierung in einen nahtlosen, fortlaufenden Vorgang zu transformieren.

Eine kontext- und risikobasierte Authentifizierung kann die Identität einer Person, die sich bei einer Anwendung anmeldet, verifizieren, indem sie eine Reihe von Attributen wie IP-Adresse, mobile Parameter, Gerät und Betriebssystem bewertet. Das ist sogar möglich, ohne dass die sich anmeldende Person es bemerkt. Die Unternehmen sind sehr bemüht, entsprechende passwortlose Authentifizierungslösungen einzuführen, die für mehr Sicherheit sorgen und gleichzeitig die Benutzererfahrung verbessern und IAM-Richtlinien anwenden.

Passwortlose Authentifizierung – Ein mehrschichtiger Ansatz

Die passwortlose Authentifizierung ersetzt Passwörter durch andere Methoden der Identitätsvalidierung und verbessert gleichzeitig die Sicherheit und die Benutzerfreundlichkeit. Diese Art der Autentifizierung gewann an Zugkraft, da sie die Anmeldung für die Benutzer signifikant erleichtert und die Sicherheitslücken überwindet, die auf textbasierte Passwörter zurückzuführen sind. Diese Vorteile sorgen für eine reibungslose Anmeldung sowie ein höheres Sicherheitsniveau aller Anwendungen, und – das ist das Beste von allem – sie machen ältere Passwörter überflüssig.

Gartner trifft die Vorhersage, dass bis zum Jahr 2022 60 Prozent der großen und globalen Unternehmen sowie 90 Prozent der mittelständischen Unternehmen in 50 Prozent aller Fälle passwortlose Authentifizierungsmethoden implementieren werden. Dies stellt einen enormen Zuwachs dar, denn heute sind es weniger als fünf Prozent[7].

7 „Embrace a Passwordless Approach to Improve Security" – https://www.gartner.com/smarterwithgartner/embrace-a-passwordless-approach-to-improve-security/

Es gibt verschiedene Schichten der passwortlosen Authentifizierung mit verschiedenen Sicherheitsniveaus. Die Implementierung eines speziellen Modells hängt von den Authentifizierungs- und Föderationsansätzen ab, die ein Unternehmen basierend auf seinen Geschäfts- und Sicherheitsrisiken und der Sensibilität der zu schützenden Daten anwenden möchte.

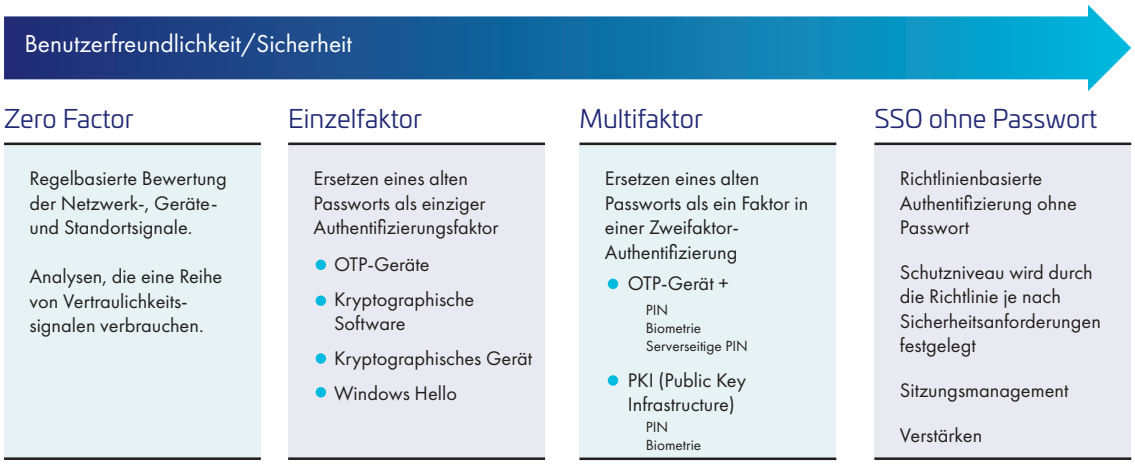
Die passwortlose Zero-Faktor-Authentifizierung kann Regeln, wissensbasierte Authentifizierung (z. B. Sicherheitsfragen) oder Geräte- und Standortindikatoren als Vertraulichkeitssignale berücksichtigen. Der Nachteil einer Zero-Faktor-Authentifizierung ist, dass keine vollständige Identitätsvalidierung sichergestellt werden kann. Sie sollte idealerweise als Backup-Methode oder in Verbindung mit weiteren Authentifizierungsmethoden eingesetzt werden.

Obwohl Passwörter als **Einzelfaktor-Authentifizierung** gelten und den „Etwas, was Sie wissen"-Faktor integrieren, lehnt die Industrie deren Anwendung ab und entscheidet sich für die Anwendung von Einzelfaktor-Authentifizierungslösungen, die den „etwas, was Sie besitzen"-Faktor nutzen. Diese Lösungen beinhalten die Verwendung von Geräten, die OTPs generieren, oder von kryptographischer Software und/oder Hardware. Einzelfaktor-Programme ermöglichen Unternehmen das Ersetzen von alten Passwörtern als einzigen Authentifizierungsfaktor durch andere Methoden. Die passwortlose Einzelfaktor-Authentifizierung ist zwar sicherer als die Zero-Faktor-Methode, dennoch kommt sie nicht an das Sicherheitsniveau der Multifaktor-Authentifizierung heran. Bei ausschließlicher Abhängigkeit von kryptographischen Geheimschlüsseln, die im TPM des Geräts gespeichert werden, ist Windows Hello ein Beispiel für ein Modell der Einzelfaktor-Authentifizierung, da das „Etwas, was Sie besitzen"-Geheimnis im Benutzergerät und nicht separat gespeichert wird.

Passwortlose Multifaktor-Authentifizierungsprogramme ermöglichen den Unternehmen das Ersetzen von Passwörtern als ein Faktor in einer MFA-Bereitstellung, indem sie ein OTP-Gerät oder eine PKI-basierte Lösung mit einem PIN oder biometrischen Daten verbinden. Normalerweise sind PIN und biometrische Daten einem bestimmten Gerät zugehörig. Die Sicherheit kann jedoch noch gesteigert werden, wenn die PIN von einem Authentifizierungsserver festgelegt und validiert wird.

Die Authentifizierungs- und Zugriffsverwaltungsprogramme der nächsten Generation zeigen sich äußerst flexibel, was adaptive und Multifaktor-Methoden betrifft. Diese können innerhalb flexibler Zugriffsrichtlinien miteinander kombiniert werden, um das richtige Niveau passwortloser Sicherheit für verschiedene Zugriffsszenarien zu bieten.

Modelle einer passwortlosen Authentifizierung



Eine passwortlose Authentifizierung bedeutet nicht zwangsläufig ein niedrigeres Sicherheitsniveau

Die Antwort darauf, ob etwas tatsächlich sicher ist, lautet normalerweise: „das ist von Ihrem Bedrohungsmodell abhängig". Diese Antwort verliert auch heute nicht an Bedeutung. Die Sicherheit von passwortlosen Authentifizierungssystemen hängt im Endeffekt von der Fähigkeit des Programms ab, die Identität einer Person mit einem hohen Grad an Gewissheit zu validieren. In einfachen Worten: die passwortlosen Methoden sind genauso sicher wie die zugrundeliegende angewendete Authentifizierung.

Die Verwendung von sicheren Push-Benachrichtigungen, die an das mobile Gerät eines Kontoinhabers gesendet werden, wird als sicherer angesehen als die Verwendung von Passwörtern. SMS-Codes, die an das mobile Gerät des Kontoinhabers gesendet werden, gelten als unsicherer, da SMS ein unsicherer Kommunikationskanal ist und es vermehrte, dokumentierte Angriffe auf SMS-Authentifizierungssysteme gibt.

Ein Passwort ist nicht die Lösung, um gegen bestimmte, kapitalkräftige Angreifer vorzugehen. Die beste Abwehrmethode ist der Verzicht auf die veralten Passwörter und die uneingeschränkte Anwendung passwortloser Lösungen, die Multifaktor-Authentifizierung, adaptiven Sicherheit und Anomalieerkennung verbinden. Solche Bereitstellungen passwortloser Authentifizierungen können verschiedenste Sicherheitsanforderungen erfüllen, je nach dem, wie sie implementiert werden.

Es gibt kein Universalkonzept

Aufgrund der vielfältigen Anwendungsfälle für Identifikations- und Zugriffsverwaltung in einem einzigen Unternehmen, kann es kein Universalkonzept für Authentifizierungslösungen geben. Sicherheitsbeauftragte und Geschäftsführer sollten nach Authentifizierungslösungen suchen, die einem oder mehreren Anwendungsfällen in ihrem Unternehmen entsprechen. Einige Methoden passen auf verschiedene Anwendungsfälle, und viele Anbieter offerieren Tools, die eine Vielzahl unterschiedlicher Methoden unterstützen. Dennoch ist es möglich, dass die Sicherheitsbeauftragten keine einzelne Lösung finden, die auf alle Anwendungsfälle passt.

Vor der Auswahl einer Authentifizierungsmethode müssen die Sicherheitsbeauftragten folgende Kriterien evaluieren:

- **Vertrauen vs. Risiko**. Eine risikogerechte Authentifizierung ist ein Best-Practice-Prinzip. Sie verlangt vom Verantwortlichen, für jeden Anwendungsfall das Mindestniveau an Vertrauen entsprechend dem Risikoniveau zu evaluieren. Anschließend muss er die Authentifizierungsmethoden auswählen, die dem Vertrauensniveau entsprechen.
- **Die Gesamtbetriebskosten im Vergleich zum vertretbaren und verfügbaren Budget** unter Berücksichtigung von Faktoren, die Betriebskosten senken können, z. B. die Effizienz von Cloud-basierten Umgebungen oder Workflows, die eine automatisierte Authentifizierung ermöglichen.
- **Benutzererfahrung/Kundenerfahrung im Vergleich zu den Kundenbedürfnissen**. Die Kundenerfahrung ist ein Auswahlkriterium mit hoher Gewichtung. Mehr als 65 % der IT-Mitarbeiter gaben in der jährlich von Thales durchgeführten Umfrage zu Zugriffsverwaltung und -authentifizierung an, dass sie einen vereinfachten Zugriff für Endbenutzer in Betracht ziehen, da dieser ein wichtiger Beweggrund bei der Entscheidung darüber ist, ob eine Zugriffsverwaltungs- und Authentifizierungslösung implementiert wird oder nicht.
- **Andere technische und betriebliche Bedürfnisse und Zwänge**, z. B. wie eine Zugriffsverwaltungs- und Authentifizierungslösung in die bestehenden IT-Umgebung des Unternehmen integriert werden kann und welche Anwendungen geschützt werden müssen.

Passwortloses SSO (Single Sign-On)

Single Sign-On (SSO) ist die Nutzung eines Sitzungs- und Benutzerauthentifizierungsservices, der Endnutzern erlaubt, einzelne Anmeldedaten für den Zugriff auf mehrere Anwendungen einzugeben. Der Benutzer meldet sich einfach im SSO-Portal oder bei einer Anwendung an und kann anschließend nahtlos auf alle Anwendungen zugreifen, ohne sich erneut authentifizieren zu müssen (während einer einzigen Sitzung, so z. B. für einen Arbeitstag). SSO unterstützt Unternehmen dabei, sich wichtigen Zugriffsherausforderungen zu stellen, und bietet gleichzeitig klare Vorteile in Sachen Produktivität und Benutzerfreundlichkeit.

Die Integration von passwortlosen Lösungen in SSO kann die Benutzerfreundlichkeit weiter stark verbessern, da dies einen weiteren Schritt hin zur passwortlosen Authentifizierung darstellt: der Benutzer authentifiziert sich und hat anschließend Zugriff auf weitere Apps und Services, ohne dass er sich noch einmal authentifizieren muss.

Wie immer gilt, dass mehr Benutzerfreundlichkeit und eine verbesserte Benutzererfahrung ein erhöhtes Sicherheitsrisiko bedeuten. SSO birgt Sicherheitsrisiken, da die Benutzer dieselben Anmeldedaten für den Zugriff auf verschiedene Apps verwenden, sowohl vor Ort als auch in der Cloud. Aus diesem Grund ist es wichtig, dass die SSO-Lösung einen richtlinienbasierten Zugriff unterstützt, der eine verstärkte Authentifizierung und Zugriffskontrolle ermöglicht. Das bedeutet, dass für verschiedene Zugriffsanwendungsfälle unterschiedliche Richtlinien angewendet werden können, je nach Benutzerprofil und Sensibilität der Daten, auf die zugegriffen wird.

Zur Aufrechterhaltung der erforderlichen Balance zwischen Benutzerfreundlichkeit und Sicherheit können Unternehmen zwei Best Practices zur Risikoverwaltung implementieren:

- Sie müssen sicherstellen, dass die anfänglichen passwortlosen Authentifizierungslösungen dem richtigen Schutzniveau entsprechen.
- Sie müssen sicherstellen, dass konditionale Richtlinien zur Zugangskontrolle angewendet werden, sodass das Authentifizierungsniveau bei einem sich ändernden Anmeldeszenario entsprechend verstärkt wird.

Betrachtet man Zugriffsverwaltung und Benutzerauthentifizierung in der Zukunft, lässt sich abschätzen, dass sich die passwortlose Authentifizierung zum fortlaufenden, passwortlosen SSO weiterentwickeln wird, bei dem die Aktionen des Benutzers innerhalb einer fortlaufenden Anmeldesitzung überwacht und eine zusätzliche Identitätsverifizierung gemäß vorab festgelegter Szenario- und Compliance-basierter Richtlinien zur erneuten Authentifizierung ausgelöst werden. Benutzeraktionen, die eine erneute Authentifizierung auslösen könnten, wären zum Beispiel das Herunterladen großer Datenmengen, der Zugriff auf sensible Informationen in einer Datenbank, die Neukonfiguration von Serviceeinstellungen oder ein geänderter Standort.

Passwortlose und fortlaufende Authentifizierung sind miteinander verknüpft

Mit einem Token, einem Passwort oder einem Fingerabdruck – Authentifizierung ist im Grunde eine Ja-Nein-Entscheidung: Das System validiert die Identität eines Benutzers und erlaubt den Zugriff auf eine Anwendung oder lehnt diesen ab. Traditionelle Authentifizierungsmethoden validieren die Authentizität eines Benutzers einmalig bei der ersten Anmeldung. Die einmalige Authentifizierung kann Sicherheitslücken hervorrufen, wenn die Benutzer ihre Arbeitsumgebungen ändern. Daher muss die Identität des Benutzers fortlaufend geprüft werden.

Eine fortlaufende Authentifizierungssitzung stellt über einen bestimmten Zeitraum an jedem Zugangspunkt sicher, dass es sich bei der Person, die von Gerät zu Gerät oder von App zu App wechselt, tatsächlich um die berechtigte Person handelt. Der Zugriffsverwaltungsservice validiert fortlaufend und transparent die Identität der Person jedes Mal neu. Dazu ist nur eine zusätzliche Authentifizierung notwendig, wenn eine Richtlinie ausgerufen oder eine Anomalie erkannt wird.

Der Benutzer muss sich dank transparenter Authentifizierung nicht mehr explizit in allen Situationen authentifizieren, da die adaptiven und kontextbezogenen Attribute die Grundlage für Authentifizierungsentscheidungen schaffen. Sicherheit und Benutzerfreundlichkeit können durch transparente Authentifizierung erhöht werden, da das mobile Gerät eine großartige Quelle für Daten zum Benutzerverhalten [8]darstellt.

Die umfangreichen und potenziell nahtlosen sensorbasierten Daten bieten eine transparente Authentifizierung mit der Möglichkeit der Bereitstellung eines granulareren Ansatzes für den Anwendungs- und Datenzugriff durch Schwellenwertaufgaben. Die Benutzeraktionen innerhalb einer Anwendung werden über einen längeren Zeitraum geprüft, wobei je nach ausgeführter Aktion eine zusätzliche Authentifizierung notwendig ist. Wenn ein Benutzer beispielsweise damit beginnt, große Mengen Daten aus einer Anwendung herunterzuladen, ruft der Zugriffsverwaltungsservice ein Authentifizierungsereignis aus, das ein höheres Niveau der Identitätsvalidierung bietet.

Der Vorteil dieser Systeme ist, dass sie ein hohes Maß an Zugriffssicherheit beibehalten und gleichzeitig die Anmeldung benutzerfreundlich gestalten. Ein weiterer Vorteil liegt in der Flexibilität, mit der je nach Sensibilität der App, Benutzerprofil und weiteren Bedingungen verschiedene Authentifizierungsmethoden für mehrere Zugriffsszenarien angewendet werden können.

So starten Sie in Richtung passwortloses SSO

Wie von Gartner vorhergesagt, wird die Mehrheit der Unternehmen in den nächsten Jahren mit der Migration hin zur passwortlosen Authentifizierung beginnen. Diese Unternehmen können ihre eigenen passwortlosen SSO-Implementierungen einführen, indem sie die Anwendungen und die Daten identifizieren, auf die ein typischer Anwender zugreift. Mit diesem Wissen können Sie die Sensibilität und die damit verbundenen Risiken der Daten bewerten, auf die zugegriffen werden muss, um anschließend für jeden Datensatz das richtige Niveau der Authentifizierungssicherheit festzulegen. Anschließend können die Unternehmen Zugriffsrichtlinien für ihr passwortloses SSO-Programm aufsetzen, um die Sicherheit und die Benutzerfreundlichkeit gleichermaßen zu fördern.

8 Alotaibi, Furnell und Clarke (2015), „Transparent authentication systems for mobile device security: A review", IEEE, verfügbar unter https://ieeexplore.ieee.org/document/7412131

THALES

Americas
Arboretum Plaza II, 9442 Capital of Texas Highway North,
Suite 100, Austin, TX 78759 USA
Tel.: +1 888 343 5773 or +1 512 257 3900
Fax: +1 954 888 6211 | E-Mail: sales@thalesesec.com

Asia Pacific – Thales Transport & Security (HK) Ltd
Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East
Wanchai, Hong Kong | Tel.: +852 2815 8633
Fax: +852 2815 8141 | E-Mail: asia.sales@thales-esecurity.com

Europa, Naher Osten, Afrika
350 Longwater Ave, Green Park,
Reading, Berkshire, UK RG2 6GF
Tel.: +44 (0)1844 201800 | Fax: +44 (0)1844 208550
E-Mail: emea.sales@thales-esecurity.com

> thalesgroup.com <