Was ist passwortlose Authentifizierung?

Tolleiv Nietsch - 2024-11-23 - Fragen zum Produkt

Sind Sie es leid, sich mehrere Passwörter zu merken und sie ständig zurückzusetzen? Die passwortlose Authentifizierung revolutioniert die Art und Weise, wie wir uns bei unseren Konten anmelden und bietet sichere und bequeme Alternativen zu herkömmlichen Passwörtern. In diesem Artikel erfahren Sie mehr über die Vorteile der passwortlosen Authentifizierung und darüber, wie sie unser Verständnis von Sicherheit verändert.

Die Nutzung digitaler Ressourcen ist im beruflichen Umfeld unabdingbar, Geschäftsprozesse und Anwendungen werden teils vollständig und ausschließlich digital abgebildet. Mit der Zunahme der Online-Aktivitäten steigt allerdings auch die Angriffsfläche und die Zahl der Cyberangriffe und Datenschutzverletzungen. Eine der häufigsten Möglichkeiten für Hacker, sich Zugang zu sensiblen Informationen zu verschaffen, ist die Verwendung von Passwörtern.

Klassische Anmeldeverfahren, bei denen sich die Nutzer nur ein einziges Passwort merken und eingeben müssen, weisen mehrere Schwachstellen auf. Eines der Hauptrisiken ist das Potenzial für Phishing-Angriffe, bei denen Hacker gefälschte E-Mails oder Nachrichten versenden, die legitim erscheinen und Mitarbeitende auffordern, ihre Anmeldedaten einzugeben. Dies kann dazu führen, dass nicht nur die Anmeldedaten des Nutzers, sondern auch sensible persönliche oder finanzielle Daten in die Hände von Angreifern gelangen.

Ein weiteres Problem bei klassischen Anmeldeverfahren ist, dass es für Mitarbeitende allzu leicht und bequem ist, schwache und leicht zu erratende Passwörter zu wählen. Studien haben gezeigt, dass ein erheblicher Prozentsatz dasselbe Passwort für mehrere Konten verwendet oder leicht zu erratende Kombinationen wie "123456" oder "password" nutzen. Dadurch wird es für Angreifer noch einfacher, sich Zugang zu sensiblen Informationen zu verschaffen.

Die Entwicklung zur passwortlosen Authentifizierung

Zur Absicherung von Logins wird Mehr-Faktor-Authentifizierung (MFA) eingesetzt, eine Authentifizierungsmethode, die die Verwendung von zwei oder mehr Arten von Authentifizierungsfaktoren erfordert, um die Identität eines Benutzers zu überprüfen. Diese Faktoren können etwas sein, das der Benutzer weiß (z. B. ein Passwort), etwas, das der Benutzer hat (z. B. ein Sicherheitsschlüssel oder ein Telefon), und etwas, das der Benutzer ist (z. B. ein Fingerabdruck oder eine Gesichtserkennung).

Das Ziel von MFA ist es, die Sicherheit zu erhöhen, indem mehrere Formen der Verifizierung

verlangt werden, bevor der Zugriff auf ein Konto oder ein System gewährt wird. Beispielsweise kann ein Benutzer aufgefordert werden, ein Passwort einzugeben und dann seine Identität durch einen Fingerabdruck zu bestätigen oder einen einmaligen Passcode zu erhalten und einzugeben, der an sein Telefon gesendet wird.

MFA gilt als sicherer als die einfache Anmeldung, die sich nur auf eine Form der Verifizierung, z. B. ein Passwort, stützt. Sie erschwert es einem Angreifer, Zugang zu einem Konto zu erhalten, selbst wenn er in der Lage ist, das Passwort eines Benutzers zu erlangen, da er immer noch eine andere Form der Authentifizierung bestehen müsste.

Allerdings differenzieren sich Methoden der Mehr-Faktor-Authentifizierung enorm in ihrer Sicherheit, da einige Verfahren auch auf Passwörtern und Shared Secrets bestehen während andere die passwortlose Authentifizierung ermöglichen. Präferiert werden deshalb Verfahren, die deutlich mehr Sicherheit bieten als die Nutzung eines einzelnen statischen Passworts. Dabei werden für die zweifelsfreie Bestimmung der Identität des Benutzers mehrere Faktoren verwendet. So wird zum Beispiel der Faktor „Wissen“ (Passwort oder PIN) um den Faktor „Besitz“ (Smartphone, Smartcard oder Authentifizierungs-Token) erweitert. Eine immer größere Rolle spielen auch die Faktoren „Eigenschaft“ (Biometrie) oder „Verhalten“.

Die Entwicklung verläuft in Richtung vollständig passwortlose Authentifizierung, diese ist aber nur dann gegeben, wenn auch im Backend keine Kennwörter oder PINs vorhanden sind. Dazu werden Lösungen eingesetzt, die auf einem Public-Key-Verschlüsselungsverfahren basieren und Passwörter meist durch sichere kryptografische, asymmetrische Schlüsselpaare ersetzen. Mit solchen Verfahren sind Hackerangriffe nur noch auf einzelne Personen und Geräte denkbar, nicht aber auf eine ganze Datenbank mit zahlreichen Anmeldeinformationen. Möglich sind hier biometrische Daten, FIDO2-Geräte und andere starke Authentifizierungsmethoden, die nicht auf herkömmlichen Passwörtern basieren.

Fazit

Mehr-Faktor-Authentifizierung ist also ein wichtiger Bestandteil eines ganzheitlichen Sicherheitskonzepts im Unternehmen. Allerdings ist MFA nicht gleich MFA – eine moderne passwortlose MFA, die biometrische Daten und gerätespezifische private Schlüssel nach dem FIDO-Standard verwendet, bietet eine stärkere und besser nutzbare Authentifizierung als herkömmliche MFA-Lösungen, zudem minimiert sie die Angriffsfläche von Unternehmen.

Hinzu kommt die aktuelle globale Tendenz zu mehr Remote Work und bietet somit steigende Marktmöglichkeiten für passwortfreie Lösungen. Da in vielen Unternehmen langfristig eine Kultur des mobilen Arbeitens entsteht, ist es wichtiger denn je, den Mitarbeitern die Mittel und Ressourcen zur Verfügung zu stellen, um sicher im Internet unterwegs zu sein - sowohl im Privatleben als auch im Home-Office.