KAUFLEITFADEN

Potenzielle Fragen an MFA-Anbieter

Die Multifaktor-Authentifizierung (MFA) ist ein zentraler Bestandteil der Sicherheit in modernen Unternehmen. Ganz gleich, ob Sie bestrebt sind, die Compliance-Anforderungen zu erfüllen oder die Sicherheit des Unternehmens zu steigern, kann MFA hilfreich sein. Durch die Umsetzung von MFA können Sie einen Beitrag zum Schutz der Ressourcen, vertraulichen Informationen und Konten in Ihrem Unternehmen leisten. Dies gilt insbesondere bei Remote-Benutzern, privilegierten Benutzern, Cloud-Anwendungen und bei Mitarbeitern, die von ihrem Notebook aus auf Unternehmensressourcen zugreifen. Durch MFA wird auch das Risiko von Sicherheitsverletzungen und den damit verbundenen Konsequenzen wie etwa Rufschädigung und juristischen Kosten reduziert.

Zwischen den einzelnen MFA-Lösungen bestehen jedoch deutliche Unterschiede. Die folgenden Fragen verhelfen bei der Einschätzung, ob eine potenzielle MFA-Lösung die benötigte Sicherheit bietet oder ob eine andere Lösung den Sicherheitsbedarf abdeckt.

1

Wird eine MFA-Lösung mit SMS-basierter Überprüfung als Haupt- bzw. Standardoption für die Authentifizierung eingesetzt?

Eine SMS-basierte Überprüfung ist weniger sicher als andere Methoden, da die Gefahr von Hijacking besteht. Als Alternative ist eine SMS-Lösung ratsam, weil mehrere Authentifizierungsfaktoren immer besser als nur eine Schutzebene sind. Die SMS-basierte Authentifizierung sollte aber nicht die Haupt- bzw. Standard-Authentifizierungsmethode sein, sondern nur ergänzend. Falls doch, wird zur anderen Lösungen geraten.

2

Wie benutzerfreundlich ist die Lösung?

Die MFA-Lösung wird nur dann akzeptiert, wenn sie benutzerfreundlich ist. Wenn Endbenutzer das Gefühl haben, dass die konkrete Lösung die Produktivität hemmt und den Zugriff auf benötigte Ressourcen verhindert, ist die Lösung ungeeignet. Bitten Sie den Anbieter um eine Demonstration der Lösung. Betrachten Sie alle Punkten mit Frustrationspotenzial für die Mitarbeiter (z. B. Hardware-Token, die verlorengehen oder vergessen werden). Erfragen Sie, ob es Funktionen gibt, die die Akzeptanz auf Seiten der Endbenutzer erhöhen, oder ob es Vorschläge gibt, wie sie sich erhöhen lässt.

3

Ist eine Offline-Authentifizierung möglich?

Wenn Mitarbeiter auch unterwegs, zum Beispiel während eines Flugs am Notebook arbeiten und auf das System zugreifen müssen, benötigen Sie eine MFA-Lösung, die die Offline-Authentifizierung unterstützt. Auch in anderen Situationen wie etwa beim Verbindungsaufbau zum Hotel-WLAN, zu einem öffentlichen WLAN oder bei schlechtem Empfang ist eine Offline-Authentifizierung erforderlich. Fragen Sie den Serviceanbieter, welche Optionen es zur Offline-Authentifizierung gibt, und achten Sie darauf, dass die Lösung einfach und sicher ist und möglichst keine Helpdesk-Unterstützung erfordert.

4

Unterstützt die Lösung ein sicheres Web-Single-Sign-On (SSO)?

Web-Single-Sign-On bedeutet nicht nur eine Erleichterung für die Endbenutzer, sondern auch mehr Sicherheit. Eine MFA-Lösung sollte unbedingt Web-SSO für Cloud-Anwendungen unterstützen. Wenn ein Unternehmen mehrere Cloud-Anwendungen nutzt, bei denen sich die Benutzer anmelden und Passwörter festlegen müssen, wird die Nutzung oftmals sehr komplex. Zumal, wenn User Kontakt mit dem Helpdesk aufnehmen müssen, um Passwörter zurücksetzen. Dies gelingt mit einer Single-Sign-On-Lösung leichter, da die Benutzer sich hierbei nur einmal anmelden müssen und dann auf alle Cloud-Anwendungen zugreifen können. Dadurch steigt letztlich die Benutzerfreundlichkeit, die ein wesentlicher Faktor für die Benutzerakzeptanz ist.

5

Welches Geschäftsmodell verfolgt der MFA-Anbieter?

Beim Kauf einer MFA-Lösung muss nicht nur die Lösung zu individuellen Anforderungen passen, sondern auch der Anbieter. Fragen Sie den Anbieter, wie intensiv er Sie nach dem Kauf noch betreuen kann. Kann er in der Bereitstellungsphase den nötigen Support bereitstellen? Können Support-Partner bei Problemen helfen? Kommt das Preismodell Ihren Vorstellungen beim Wie und Wann der Lizenzierung entgegen?

6

Gibt es eine lokalisierte Version der Lösung?

Die Benutzeroberfläche sollte lokalisiert sein. Bei der Managementoberfläche ist eine Lokalisierung verzichtbar, aber die Benutzeroberfläche sollte für alle relevanten Länder in der jeweiligen Sprache verfügbar sein. Dies erhöht die Akzeptanz der MFA-Lösung seitens der Endbenutzer. MFA-Endbenutzer sind in den seltensten Fällen Computerexperten für Cybersicherheit.

7

Lässt sich die Lösung einfach verwalten?

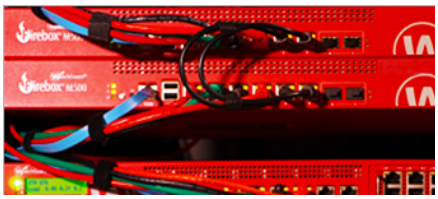
Das Management und die Zuweisung von Tokens muss einfach, schnell, intuitiv und webbasiert erfolgen und darf auch unerfahrene User nicht vor Probleme stellen. Wie einfach lässt sich die Lösung einrichten und starten? Wie schnell kann eine von der MFA-Lösung zu schützende Ressource hinzugefügt werden? Wie schnell und einfach können Authentifikatoren für die Benutzer bereitgestellt werden? Ist die Admin-Oberfläche leicht verständlich und benutzerfreundlich? Ziehen Sie Lösungen in Betracht, die eine umfassende Benutzeroberfläche für die erforderlichen Aufgaben bieten und nicht nur von Computerspezialisten bedient werden können.

8

Wie hoch sind die Kosten für die Lösung?

Bei den Preisen für MFA-Lösungen müssen verschiedene Faktoren betrachtet werden, was einen direkten Vergleich erschwert und versteckte oder unerwartete Kosten anfallen können. Wird die Lösung pro Benutzer, pro Authentifikator oder pro geschützte Anwendung berechnet? Ist der Support im Preis enthalten – sowohl technischer Support als auch Support für die Verwaltung des Abonnements? Gibt es sonstige versteckte Kosten, die berücksichtigt werden müssen, etwa Lizenzkosten für zusätzliche Software? Die Preisgestaltung bei MFA-Lösungen basiert meist auf Preisspannen bzw. -bereichen und Mengenrabatten.

WATCHGUARD-SICHERHEITSPORTFOLIO



Netzwerksicherheit

Secure Wi-Fi

Multifaktor-Authentifizierung

Mehr erfahren

Weitere Details erhalten Sie von Ihrem autorisierten WatchGuard-Vertriebspartner oder unter **https://www.watchguard.com/authpoint**

Über WatchGuard

WatchGuard® Technologies, Inc. gehört zu den führenden Anbietern im Bereich Netzwerksicherheit, sicheres WLAN, Multifaktor-Authentifizierung und Network Intelligence. Beinahe 10.000 Vertriebspartner und Dienstanbieter im Bereich Sicherheit verlassen sich auf die prämierten Produkte und Dienste des Unternehmens, um mehr als 80.000 Kunden zu schützen. Die Philosophie von WatchGuard ist es, Sicherheit auf Enterprise-Niveau für Unternehmen jeder Größenordnung und Art zu realisieren. Das macht WatchGuard insbesondere für kleine und mittlere sowie dezentral aufgestellte Unternehmen zum idealen Anbieter. Neben der Zentrale in Seattle im US-Bundesstaat Washington unterhält das Unternehmen Niederlassungen in ganz Nordamerika, Lateinamerika und Europa sowie im asiatisch-pazifischen Raum. Weitere Informationen finden Sie unter WatchGuard.de.