consol

DIE FÜNF GRÖßTEN HERAUSFORDERUNGEN FÜR MULTI-FAKTOR-AUTHENTIFIZIERUNG

IT SECURITY

Eine Multi-Faktor-Authentifizierung (MFA) spielt beim Zero-Trust-Sicherheitskonzept eine zentrale Rolle. Sie ist eine effektive Methode, um den Zugang zu sensiblen Daten und Systemen abzusichern.

MFA bedeutet, dass man für die Authentifizierung eines Users mehr als einen Nachweis heranzieht. Die Eingabe eines Passworts alleine reicht nicht aus. Häufig wird Multi-Faktor-Authentifizierung in Form einer 2-Faktor-Autorisierung (2FA) umgesetzt. Hier muss z. B. zusätzlich zur Eingabe des Passworts ein Code eingegeben werden, der an ein anderes Gerät gesendet wird. Auch ein biometrisches Merkmal wie ein Fingerabdruck oder ein Hardware-Token können als zweiter Authentifzierungs-Faktor dienen. Damit liegen zwei Belege vor, dass die Person diejenige ist, die sie zu sein vorgibt.

Moderne Multi-Faktor-Authentifizierung ist eine Lösung, um Phishing und andere Angriffe auf Passwörter effektiv abzuwehren. Bei der Implementierung von MFA stehen Unternehmen vor Herausforderungen, die zu beachten sind.

Herausforderung 1: Hohe Kosten und großer Implementierungsaufwand

Die Integration einer MFA-Methode in die Unternehmens-IT kann erhebliche Kosten und Implementierungsaufwand mit sich bringen. Es kommen Investitionen finanzieller als auch personeller Hinsicht auf die Firma zu: Dies können Ausgaben für die Anpassung der IT-Infrastruktur, der Erwerb von Softwarelizenzen oder Schulungsaufwand für die Mitarbeitenden sein. Verschiedene Faktoren können zu hohen Kosten beitragen:

- Je nach Komplexität der verwendeten MFA-Methode kann dies eine aufwendige Integration mit den bestehenden Systemen erfordern.
- Es könnte die Notwendigkeit bestehen, unterschiedliche MFA-Methoden für verschiedene Benutzergruppen je nach Zugriffsrechten implementieren zu müssen.
- Erhöhte Kosten gehen mit dem notwendigen Schulungsaufwand einher, um sicherzustellen, dass Mitarbeitende die neuen MFA-Methoden korrekt nutzen.
- Es müssen gegebenenfalls in der IT-Abteilung zusätzliche Ressourcen für den MFA-Support bereitgestellt werden.

Herausforderung 2: Die Verwaltung von Sicherheit-Tokens ist kompliziert

Die Implementierung von Multi-Faktor-Authentifizierung mit zusätzlichen Hardwarekomponenten wie Smartcards oder Security Keys stellt eine zusätzliche Herausforderung dar. Die physischen Tokens müssen nicht nur bereitgestellt werden. Sie bergen auch das Risiko von Verlust oder Diebstahl, was die IT-Sicherheit gefährdet. Die Verwaltung der Tokens ist zudem zeitaufwendig und verursacht Ausgaben.

Sollten Sie sich im Unternehmen für den Einsatz physischer Token entscheiden, stellen Sie sicher, dass ein effizientes Verwaltungssystem vorliegt. Um die Tokens zu schützen, sollten regelmäßige Überprüfungen der Token-Berechtigungen stattfinden.

Herausforderung 3: Veraltete MFA verursacht Betriebsunterbrechungen

Manchmal kann es bei der Einführung von MFA-Konzepten zu Betriebsstörungen kommen. Dazu gehören:

- Technische Probleme: Die Einführung von MFA kann zu technischen Problemen führen wie beispielsweise Konflikte mit anderen Systemen oder Anwendungen. Das kann zu Ausfällen oder Verzögerungen führen.

- Compliance-Verstöße: Bei der Einführung von MFA müssen womöglich spezifische Compliance-Anforderungen berücksichtigt werden. Eine Nichterfüllung kann zu Verstößen führen, die finanzielle Strafen oder rechtlichen Konsequenzen nach sich ziehen.

- Widerstand innerhalb der Belegschaft: Auch Widerstand bei der Belegschaft im Rahmen der Einführung eines MFA-Konzeptes ist denkbar. MFA-Methoden könnten von den Angestellten als unbequem oder einschränkend empfunden werden.

Herausforderung 4: Nicht alle MFA-Methoden sind gleich

Nicht alle MFA-Methoden bieten den gleichen Schutz. Berücksichtigen Sie bei der Auswahl einer geeigneten MFA-Methode auch deren Schwachstellen.

- SMS-Authentifizierung: SMS-Codes können abgefangen oder durch SIM-Swapping kompromittiert werden.

- Codes via E-Mail: Codes via E-Mail sind ebenfalls anfällig, da Angreifer Zugriff auf E-Mail-Konten erlangen können.

- Authentifizierungs-Apps: Diese Methode ist anfällig für Phishing-Angriffe auf die App selbst und kann durch Malware-Angriffe auf das Gerät kompromittiert werden.

Herausforderung 5: Die Integration von MFA in bestehende Systeme ist schwierig

Die Integration einer Multi-Faktor-Authentifizierung in bestehende Systeme stellt eine technische Herausforderung dar bezüglich:

- **Kompatibilität:** Die neue MFA muss mit den vorhandenen Systemen kompatibel sein, um eine reibungslose Integration zu gewährleisten. Dies hängt von Faktoren wie der verwendeten Technologie oder der Versionen der vorhandenen Systeme ab.

- **Benutzerverwaltung:** Ein MFA-Konzept, das eine umfassende Userverwaltung erfordert, sollte intuitiv gestaltet sein. Neuen Nutzerinnen und Nutzer sollte es ein reibungsloses Off- und Onboarding ermöglichen.

- **Skalierbarkeit:** Die neue MFA sollte skalierbar sein, um eine wachsende Zahl von Anwendern unterstützen zu können.

- **Integration:** Die Integration der MFA-Lösung in bestehende Systeme erfordert die Verwendung von APIs und die Anpassung vorhandener Systeme. Eine sorgfältige Planung der Integration ist unabdingbar.

- **Vorhandene Systeme:** Die neue MFA sollte über eine Möglichkeit verfügen, Altsysteme zu schützen, die keine modernen Authentifizierungsmethoden wie SAML, OIDC oder WS-Fed unterstützen.

- **Verfügbarkeit:** Die Verfügbarkeit der MFA ist der entscheidende Faktor für den Erfolg der Integration. Die MFA muss jederzeit zuverlässig verfügbar sein, um eine reibungslose Authentifizierung der User zu gewährleisten.

Um eine Multi-Faktor-Authentifizierung erfolgreich in ein bestehendes System zu integrieren, bedarf es einer umfassenden Planung, um alle technischen Herausforderungen zu bewältigen. Die Berücksichtigung der oben genannten Faktoren ist entscheidend, um eine erfolgreiche Integration sicher zu stellen und die Sicherheit der Daten und Systeme zu verbessern.

ConSol
Consulting & Solutions Software GmbH

St.-Cajetan-Straße 43
D-81669 München
Tel.: +49-89-45841-100
vertrieb@consol.de
www.consol.de
Folgen Sie uns auf LinkedIn:
@consol-software-gmbh

ConSol
Austria Software GmbH

Maysedergasse 2/25
A-1010 Wien, Österreich
Tel.: +43-1-9971392
info-austria@consol.com
www.consol-software.at
Folgen Sie uns auf LinkedIn:
@consol-austria-software-gmbh