



Workshop: Einführung Entra ID Multi-Faktor Authentication (MFA)

In strukturierten Schritten zur sicheren und benutzerfreundlichen Authentifizierungslösung.

Kompromittierte Zugangsdaten gehören zu den häufigsten Einfallstoren für Cyberangriffe und sind gleichzeitig eines der am einfachsten zu schließenden Sicherheitslücken. Mit unserem Workshop „Einführung Entra ID MFA“ führen Sie Entra ID MFA strukturiert und sicher in Ihr Unternehmen ein – von der Analyse bis zum Rollout, individuell auf Ihre Organisation abgestimmt.

Cyberangriffe werden immer ausgefeilter, und kompromittierte Zugangsdaten gehören nach wie vor zu den häufigsten Einfallstoren für Angreifer. Für Unternehmen jeder Größe ist es daher entscheidend, den Zugang zu ihren digitalen Ressourcen zuverlässig abzusichern, ohne dabei die Produktivität der Mitarbeitenden zu beeinträchtigen. Multi-Faktor Authentication (MFA) ist heute ein effektiver Schutzwall gegen unbefugte Zugriffe und eine unverzichtbare Grundlage jeder modernen IT-Sicherheitsstrategie. Microsoft Entra ID bietet hierfür leistungsstarke MFA-Funktionen, die sich flexibel an die Anforderungen unterschiedlicher Organisationen anpassen lassen.

Damit die Einführung gelingt bedarf es eines strukturierten Vorgehens, das strategische Planung und praktische Umsetzung verbindet. Mit unserem Workshop zur Einführung von Entra ID MFA begleiten wir Sie Schritt für Schritt – von der Analyse Ihres aktuellen IT-Umfelds über die Auswahl geeigneter Authentifizierungsmethoden bis hin zum produktiven Rollout, mit minimaler Belastung für Ihren laufenden Betrieb.

Analyse, Methodenauswahl und Risikobetrachtung

Der Workshop startet mit einer gründlichen Bestandsaufnahme Ihrer bestehenden Identitäts- und Zugriffssituation in Entra ID. Aktuelle Authentifizierungs- und Sicherheitskonzepte werden analysiert, vorhandene Conditional Access Policies geprüft und der Umgang mit privilegierten und regulären Benutzerkonten beleuchtet. So werden Schwachstellen identifiziert und eine solide Grundlage für alle weiteren Schritte geschaffen.

Anschließend stellen wir Ihnen die verfügbaren MFA-Methoden in Microsoft Entra ID vor und erarbeiten gemeinsam die optimale Auswahl für Ihre Organisation – individuell abgestimmt auf Ihre Benutzergruppen, Sicherheitsziele und regulatorischen Anforderungen. Betrachtet werden unter anderem:

- Microsoft Authenticator (Push-Benachrichtigung & passwortlose Anmeldung)
- FIDO2-Security Keys
- SMS, Telefonanruf und Temporary Access Pass

Darüber hinaus werden typische Risiken und Herausforderungen beleuchtet, die bei einer MFA-Einführung auftreten können – von Legacy-Anwendungen und fehleranfälligen Policy-Konfigurationen bis hin zu Break-Glass-Szenarien und der Förderung der Benutzerakzeptanz. Mit bewährten Best Practices helfen wir Ihnen, diese frühzeitig zu adressieren und kostspielige Ausfall- oder Support-Szenarien zu vermeiden.

Planung, Test und Pilotierung

Ein strukturiertes Konzept für MFA-basierte Conditional Access Policies ist das Herzstück einer erfolgreichen Einführung. Zielgruppen, Ausnahmen, Zugriffsbedingungen und Sicherheitsstufen werden gemeinsam definiert – mit besonderem Fokus auf die Absicherung privilegierter Konten und kritischer Anwendungen. Das Ergebnis ist ein durchdachtes Policy-Framework, das Sicherheit und Betriebsstabilität miteinander vereint und einen schrittweisen, risikoarmen Rollout ermöglicht.

Vor dem flächendeckenden Rollout wird die geplante Konfiguration in einer kontrollierten Pilotphase mit ausgewählten Benutzergruppen validiert. So wird das

Risiko für den laufenden Betrieb minimiert und sichergestellt, dass technische Abhängigkeiten frühzeitig erkannt und Nutzerfeedback in die finale Konfiguration eingearbeitet werden.

- Validierung der MFA-Einstellungen und Conditional Access Policies
- Identifikation technischer Abhängigkeiten und Kompatibilitätsprobleme
- Einarbeitung von Nutzerfeedback in die finale Konfiguration

Endanwender-Kommunikation und Rollout

Der Erfolg einer MFA-Einführung hängt maßgeblich davon ab, wie gut die Mitarbeitenden auf die Veränderung vorbereitet werden. Deshalb wird eine verständliche, anwenderfreundliche Registrierungsanleitung erstellt, die den Registrierungsprozess Schritt für Schritt beschreibt und intern als Kommunikations- und Schulungsgrundlage eingesetzt werden kann – ob als Self-Service-Dokumentation, Helpdesk-Referenz oder Bestandteil eines Onboarding-Prozesses.

Abschließend definieren wir gemeinsam das konkrete Vorgehen für den produktiven Rollout – strukturiert, kommunikativ begleitet und mit klaren Support- und Monitoring-Prozessen abgesichert. So gelingt die Einführung von MFA so reibungslos wie möglich, ohne den laufenden Betrieb zu gefährden.

Medialine als Ihr IT-Security-Partner

Als erfahrener Microsoft-Partner begleiten wir Sie durch die gesamte Einführung von Entra ID MFA – von der ersten Analyse bis zum erfolgreichen Rollout. Profitieren Sie von bewährten Methoden, praxisnahem Know-how und einer strukturierten Vorgehensweise, die Sicherheit und Betriebsstabilität in den Mittelpunkt stellt.

Kontaktieren Sie uns unter **sales@medialine.ag** und erfahren Sie, wie wir Ihre Organisation mit unserem Workshop optimal auf eine moderne, sichere Authentifizierungslandschaft vorbereiten können.