yubico

Ankündigung der obligatorischen Multi-Faktor-Authentifizierung für die Azure-Anmeldung

Von Naj Shahid, leitender Produktmanager; Bill DeForeest, leitender Produktmanager, Azure Compute
am 15.08.2024

Erfahren Sie, wie Multifaktor-Authentifizierung (MFA) Ihre Daten und Ihre Identität schützen kann, und bereiten Sie sich auf die kommende Multifaktor-Anforderung von Azure vor.

Da Cyberangriffe immer häufiger, raffinierter und schädlicher werden, war der Schutz Ihrer digitalen Ressourcen noch nie so wichtig wie heute. Als Teil von Microsofts 20-Milliarden-Dollar-Investitionen in die Sicherheit in den nächsten fünf Jahren und unserer Verpflichtung, die Sicherheit unserer Dienste bis 2024 zu verbessern, führen wir die obligatorische Multifaktor-Authentifizierung (MFA) für alle Azure-Anmeldungen ein.

Der Bedarf an verbesserter Sicherheit

Eine der Säulen von Microsofts Secure Future Initiative (SFI) ist dem Schutz von Identitäten und Geheimnissen gewidmet. Wir möchten das Risiko eines unbefugten Zugriffs verringern, indem wir erstklassige Standards für die gesamte Infrastruktur für Identitäten und Geheimnisse sowie für die Authentifizierung und Autorisierung von Benutzern und Anwendungen implementieren und durchsetzen. Im Rahmen dieser wichtigen Priorität ergreifen wir die folgenden Maßnahmen:

- Schutz der Signier- und Plattformschlüssel der Identitätsinfrastruktur durch schnelle und automatische Rotation mit Hardwarespeicherung und -schutz (z. B. Hardwaresicherheitsmodul (HSM) und vertrauliche Datenverarbeitung).
- Stärkung der Identitätsstandards und Förderung ihrer Einführung durch Verwendung von Standard-SDKs für 100 % der Anwendungen.
- Sicherstellung, dass 100 % der Benutzerkonten durch eine sicher verwaltete, phishing-resistente Multifaktor-Authentifizierung geschützt sind.
- Sicherstellung, dass 100 % der Anwendungen mit systemverwalteten Anmeldeinformationen geschützt sind (z. B. Managed Identity und Managed Certificates).
- Sicherstellung, dass 100 % der Identitäts-Tokens durch zustandsabhängige und dauerhafte Validierung geschützt sind.
- Einführung einer feineren Partitionierung von Identitätssignierschlüsseln und Plattformschlüsseln.
- Sicherstellen, dass die Identitäts- und Public-Key-Infrastruktur (PKI)-Systeme für eine Post-Quantum-Kryptographie-Welt bereit sind.

Eine unserer wichtigsten Maßnahmen ist der Schutz von Azure-Konten durch eine sicher verwaltete, phishing-resistente Multifaktor-Authentifizierung.

Jüngste Forschungsergebnisse von Microsoft zeigen, dass die **Multifaktor-Authentifizierung (MFA) mehr als 99,2 % der Angriffe zur Kompromittierung von Konten abwehren** kann, was sie zu einer der effektivsten verfügbaren Sicherheitsmaßnahmen macht.

Im Mai 2024 sprachen wir über die Implementierung der automatischen Durchsetzung der Multifaktor-Authentifizierung als Standard für mehr als eine Million Microsoft Entra ID-Tenants bei Microsoft, einschließlich Tenants für Entwicklung, Tests, Demos und Produktion. Wir weiten diese Best Practice zur Durchsetzung von MFA auf unsere Kunden aus, indem wir sie zur Voraussetzung für den Zugriff auf Azure machen.

Auf diese Weise verringern wir nicht nur das Risiko einer Kontokompromittierung und eines Datenverstoßes für unsere Kunden, sondern helfen Organisationen auch bei der Einhaltung verschiedener Sicherheitsstandards und -vorschriften wie dem Payment Card Industry Data Security Standard (PCI DSS), dem Health Insurance Portability and Accountability Act (HIPAA), der General Data Protection Regulation (GDPR) und dem National Institute of Standards and Technology (NIST).

Vorbereitung auf die obligatorische Azure MFA

Die obligatorische MFA für alle Azure-Benutzer wird in Phasen eingeführt, die in der zweiten Hälfte des Kalenderjahres 2024 beginnen, um unseren Kunden Zeit für die Planung ihrer Implementierung zu geben:

- **Phase 1:** Ab Oktober wird MFA für die Anmeldung beim Azure-Portal, Microsoft Entra Admin Center und Intune Admin Center erforderlich sein. Die Durchsetzung wird schrittweise auf alle Mieter weltweit ausgeweitet. Diese Phase wird sich nicht auf andere Azure-Clients wie Azure Command Line Interface, Azure PowerShell, Azure Mobile App und Infrastructure as Code (IaC) Tools auswirken.

- **Phase 2:** Ab Anfang 2025 wird die schrittweise Durchsetzung von MFA bei der Anmeldung für Azure CLI, Azure PowerShell, Azure Mobile App und Infrastructure as Code (IaC)-Tools beginnen.

Ab sofort wird Microsoft eine 60-tägige Vorankündigung an alle globalen Entra-Administratoren per E-Mail und über Azure Service Health Notifications senden, um das Startdatum der Durchsetzung und die erforderlichen Maßnahmen mitzuteilen. Weitere Benachrichtigungen werden über das Azure-Portal, das Entra-Admin-Center und die M365-Nachrichtenzentrale verschickt.

Für Kunden, die zusätzliche Zeit benötigen, um sich auf die obligatorische Azure MFA vorzubereiten, wird Microsoft erweiterte Zeitrahmen für Kunden mit komplexen Umgebungen oder technischen Hindernissen prüfen.

yubico

Wie man Microsoft Entra für flexible MFA nutzt

Organisationen haben mehrere Möglichkeiten, ihren Benutzern die Nutzung von MFA über Microsoft Entra zu ermöglichen:

- Microsoft Authenticator ermöglicht es Benutzern, Anmeldungen über eine mobile App mithilfe von Push-Benachrichtigungen, biometrischen Merkmalen oder einmaligen Passcodes zu genehmigen. Erweitern oder ersetzen Sie Passwörter durch eine zweistufige Verifizierung und erhöhen Sie die Sicherheit Ihrer Konten von Ihrem mobilen Gerät aus.

- FIDO2-Sicherheitsschlüssel ermöglichen die Anmeldung ohne Benutzernamen oder Passwort mit einem externen USB-, NFC- (Near Field Communication) oder einem anderen externen Sicherheitsschlüssel, der die Fast Identity Online (FIDO)-Standards unterstützt, anstelle eines Passworts.

- Die zertifikatsbasierte Authentifizierung erzwingt Phishing-resistente MFA unter Verwendung von Personal Identity Verification (PIV) und Common Access Card (CAC). Authentifizierung mit X.509-Zertifikaten auf Smartcards oder Geräten direkt gegenüber Microsoft Entra ID für die Browser- und Anwendungsanmeldung.

- Passkeys ermöglichen eine phishing-sichere Authentifizierung mit Microsoft Authenticator.

- Schließlich, und das ist die am wenigsten sichere Version von MFA, können Sie auch eine SMS- oder Sprachbestätigung verwenden, wie in dieser Dokumentation beschrieben.

Externe Multifaktor-Authentifizierungslösungen und föderierte Identitätsanbieter werden weiterhin unterstützt und erfüllen die MFA-Anforderung, wenn sie so konfiguriert sind, dass sie einen MFA-Antrag senden.

Weitere Schritte

Bei Microsoft hat Ihre Sicherheit höchste Priorität. Durch die Durchsetzung von MFA für Azure-Anmeldungen möchten wir Ihnen den besten Schutz vor Cyber-Bedrohungen bieten. Wir schätzen Ihre Kooperation und Ihr Engagement, die Sicherheit Ihrer Azure-Ressourcen zu verbessern.

Unser Ziel ist es, ein reibungsloses Erlebnis für legitime Kunden zu bieten und gleichzeitig sicherzustellen, dass robuste Sicherheitsmaßnahmen vorhanden sind. Wir empfehlen allen Kunden, so bald wie möglich mit der Planung für die Einhaltung der Vorschriften zu beginnen, um Geschäftsunterbrechungen zu vermeiden.

Beginnen Sie noch heute!