yubico

Yubico Blog von Shakeel Aziz zum Thema Break-Glass-Konten vom 15.08.2024

Break-Glass-Konten sind wichtige Konten, die in einer Vielzahl von Notfällen Zugang zu kritischen Systemen bieten. Microsofts jüngste Ankündigung zur Durchsetzung der Multi-Faktor-Authentifizierung (MFA) für Microsoft Entra ID-Anmeldungen verdeutlicht die Auswirkungen auf Break-Glass-Konten und verbesserte Sicherheitsmaßnahmen: „Wir haben Ihre Fragen zu Break-Glass- oder 'Notfallzugangs'-Konten gehört. Wir empfehlen, diese Konten so zu aktualisieren, dass sie FIDO2 oder zertifikatsbasierte Authentifizierung verwenden (wenn sie als MFA konfiguriert sind), anstatt sich nur auf ein langes Passwort zu verlassen. Beide Methoden werden die MFA-Anforderungen erfüllen.“

Als Sicherheitsnetz für verschiedene Notfälle sind Break-Glass-Konten unter anderem für folgende Szenarien wichtig:

- **Netzwerk- oder Service-Ausfall:** Wenn die Netzwerkkonnektivität oder der Internetzugang unterbrochen ist, was die Authentifizierung über Telefonietransporte und drahtlose Netzwerke verhindert.

- **Ausfall von Federation Services:** Wenn der Identitätsanbieter, der die Verbundauthentifizierung anbietet, von einer Dienstunterbrechung betroffen ist.

- **Nichtverfügbarkeit von Mitgliedern privilegierter Rollen:** Wenn Mitglieder von privilegierten Rollen, wie z. B. der globale Administrator, das Unternehmen verlassen haben oder nicht verfügbar sind.

- **Nichtverfügbarkeit des Privileged Access Management Tools (PAM):** Wenn PAM-Tools, die zur sicheren Speicherung von Zugangsdaten für Benutzer mit hohen Privilegien verwendet werden, aufgrund von Unterbrechungen oder Wartungsarbeiten nicht verfügbar sind.

Die Sicherheit dieser Konten wird jedoch häufig vernachlässigt. Dieses Versäumnis kann durch den Einsatz von gerätegebundenen Passkeys, die in speziell für die Sicherheit entwickelten Geräten wie YubiKeys gespeichert sind, behoben werden, um eine hochgradig sichere Authentifizierung zu erreichen.

Während wir uns mit den Besonderheiten der Verwendung von YubiKeys für Break-Glass-Konten befassen, ist es wichtig, die überzeugenden Vorteile zu verstehen, die eine Verbesserung der Kontosicherheit bietet.

Warum YubiKeys ein wichtiges Sicherheitstool für Einbruchskonten sind

Einer der größten Vorteile von YubiKeys ist ihre Fähigkeit, die passwortlose Authentifizierung mit Passkeys zu unterstützen. Passkeys eliminieren den operativen Overhead der Passwortverwaltung und reduzieren das Risiko von passwortbezogenen Sicherheitsverletzungen.

Die passwortlose Authentifizierung ist nicht nur sicherer, sondern auch bequemer und gewährleistet, dass der Zugang im Notfall sowohl einfach als auch sicher ist.

Weitere Vorteile sind:

- **Phishing-resistente MFA mit Hardware-Unterstützung**
  - Auf YubiKeys gespeicherte Passwörter bieten robuste Sicherheit durch das FIDO2-Protokoll, das eine fälschungssichere MFA ermöglicht. Im Gegensatz zu Passwörtern, die gefälscht oder gestohlen werden können, verwenden gerätegebundene Passkeys auf YubiKeys Public-Key-Kryptographie, die die Domäne an den Berechtigungsnachweis bindet. Passkeys befinden sich im YubiKey-Hardware-Formfaktor und können nicht exfiltriert oder aus der Ferne kompromittiert werden, da der private Schlüssel den Authentifikator nie verlässt - dies gewährleistet ein Höchstmaß an Sicherheit für Unternehmen.

- **Geringere Serviceabhängigkeit**
  - Passkeys auf YubiKeys funktionieren unabhängig von herkömmlichen MFA-Methoden, die auf externe Systeme wie SMS oder Push-Benachrichtigungen angewiesen sind, die von Netzwerkverbindungen und Telekommunikationsdiensten abhängen. In Fällen, in denen diese Dienste unterbrochen werden, gewährleisten gerätegebundene Passkeys auf YubiKeys eine zuverlässige Authentifizierungsmethode, die von solchen Abhängigkeiten unbeeinflusst bleibt.

- **Ideal für Offsite-Speicherung**
  - YubiKeys enthalten keine beweglichen Teile und sind so konzipiert, dass sie einfach und robust sind, mit einer Solid-State-Konstruktion, die zu ihrer Zuverlässigkeit beiträgt. Sie benötigen weder Batterien noch eine externe Stromquelle, da sie bei Gebrauch direkt über die USB- oder NFC-Verbindung mit Strom versorgt werden, was sie ideal für die Offsite-Speicherung macht.

Nachdem wir nun verstanden haben, warum YubiKeys ein wichtiges Sicherheitstool für Einbruchskonten sind, wollen wir nun die praktischen Schritte zu ihrer effektiven Einrichtung erkunden.

Die Umsetzung dieser Schritte wird sicherstellen, dass Ihre Notzugangskonten sowohl sicher als auch bei Bedarf leicht zugänglich sind.

yubico

Einrichten von YubiKeys für Break-Glass-Konten

1. **Erstellen Sie eine Sicherheitsgruppe:** Beginnen Sie mit der Erstellung einer Sicherheitsgruppe speziell für Ihre Konten für den Einbruchschutz. Weisen Sie dieser Gruppe die Rolle des globalen Administrators zu.

2. **Verwenden Sie Cloud-Only-Konten:** Erstellen Sie Konten, die für Identitäts- und Service-Provider-Plattformen nativ sind und stellen Sie sicher, dass sie nicht föderiert oder synchronisiert werden.

3. **Registrieren Sie zwei YubiKeys:** Für jedes Break-Glass-Konto sollten zwei YubiKeys registriert sein, um Redundanz zu gewährleisten.

Einige weitere Best Practices für die Sicherheit von Konten umfassen:

- **Ausschlüsse in der Police:** Vergewissern Sie sich, dass Ihre Policen nicht den Zugang zu Break-Glass-Konten blockieren, die im Notfall ungehinderten Zugang erfordern.

- **Sichere Aufbewahrung:** Bewahren Sie YubiKeys an sicheren, separaten Orten auf, um unbefugten Zugriff zu verhindern.

- **Dokumentieren Sie die Verfahren:** Dokumentieren Sie klar und deutlich, wie der Zugriff auf und die Nutzung von Break-Glass-Konten erfolgt, und schulen Sie Ihr Team in diesen Verfahren.

- **Regelmäßige Tests:** Testen Sie die Verfahren regelmäßig, um sicherzustellen, dass sie in einem Notfall wie erwartet funktionieren.

Überwachen Sie außerdem konsequent die Aktivitäten im Zusammenhang mit Break-Glass-Konten und richten Sie Warnmeldungen für alle Änderungen oder die Nutzung ein. Überprüfen Sie regelmäßig, wer Zugang hat, um sicherzustellen, dass nur autorisiertes Personal diese Konten nutzen kann. Dies trägt dazu bei, die Sicherheit und Integrität Ihrer Notfallzugangsverfahren aufrechtzuerhalten.

YubiKeys bieten eine hervorragende Lösung für die Sicherung von Break-Glass-Konten, da sie passwortlose Authentifizierung, starke phishing-resistente MFA, reduzierte Serviceabhängigkeit und ein Solid-State-Design unterstützen, das sich ideal für die externe Speicherung eignet.

Durch den Einsatz von YubiKeys und die Einhaltung der empfohlenen Praktiken können Sie sicherstellen, dass Ihre Notfallkonten immer sicher und einsatzbereit sind. Regelmäßige Schulungen, strenge Tests und eine kontinuierliche Überwachung sorgen dafür, dass alles in Ordnung bleibt, und geben Ihnen die Gewissheit, dass der Zugriff auf Ihre kritischen Systeme auch im Krisenfall möglich ist.

Wenn Sie Fragen haben oder wissen möchten, wie Sie YubiKeys für Ihr Unternehmen einführen können, kontaktieren Sie uns!