Rublon Business Continuity – Vorbereitungsleitfaden

Inhaltsverzeichnis

1. Überblick

Warum Sie diesen Guide benötigen

Selbst die robustesten Systeme können gelegentlich Störungen erfahren. Rublon MFA ist für hohe Verfügbarkeit ausgelegt (mit einer Erfolgsquote von über 99,9 % Betriebszeit), doch kein Cloud-Service ist völlig immun gegen Ausfälle.

Ein kurzer Zeitraum der Nichtverfügbarkeit – so selten er auch sein mag – könnte die Fähigkeit Ihrer Benutzer beeinträchtigen, auf kritische Systeme zuzugreifen. Solche Ausfälle können die Produktivität der Belegschaft vorübergehend stören und sogar Ihre Sicherheitslage schwächen, wenn sie nicht ordnungsgemäß gehandhabt werden.

Als Ihr vertrauenswürdiger Anbieter für Multi-Faktor-Authentifizierung möchte Rublon, dass Sie auf jede Situation vorbereitet sind. Dieser Guide hilft Ihnen, einen Plan zu erstellen, um sicheren Zugriff während Rublon-Dienstausfällen oder -Beeinträchtigungen aufrechtzuerhalten. Planen Sie im Voraus, damit Ihr Unternehmen auch dann reibungslos weiterarbeiten kann, wenn der Rublon-MFA-Dienst auf ein Problem stößt.

Umfang

Dieser Guide konzentriert sich auf Kontinuitätsstrategien für Rublon MFA.

Wir erklären:

- Unterschiedliche Arten von Dienstunterbrechungen
- Wie sich Rublon-integrierte Anwendungen in jedem Szenario verhalten
- Welche Konfigurationsoptionen und Workarounds Sie anwenden können

Der Guide enthält außerdem Beispielkommunikationen, um Ihre Endbenutzer während eines Vorfalls informiert zu halten. Mit diesem Wissen können Sie einen auf die Bedürfnisse Ihrer Organisation zugeschnittenen Notfallplan erstellen.

2. Liegt es an Rublon oder an Ihrer Firewall?

Was wie ein Rublon-Ausfall erscheinen mag, kann durch umgebungsbedingte Faktoren wie die Netzwerkkonfiguration verursacht werden.

Berücksichtigen Sie, wie Ihre durch Rublon geschützten Anwendungen eine Verbindung zur Rublon API herstellen und welche Abhängigkeiten bestehen. Wenn Ihre Organisation strenge Firewall-Regeln hat oder bestimmten Datenverkehr filtert, müssen Sie sicherstellen, dass der Rublon-Dienst zugelassen ist. Rublon läuft auf Amazon Web Services und verwendet dynamische IP-Adressen, die sich im Laufe der Zeit ändern können. Wenn Ihre Firewall nicht auf diese Adressen oder den Rublon-API-Endpunkt aktualisiert ist, könnte sie Rublon-Anfragen blockieren, was zu Authentifizierungsfehlern führen würde, obwohl der Rublon-Dienst verfügbar ist. (Mit anderen Worten: Eine fehlerhafte interne Netzwerkkonfiguration kann einen Rublon-Ausfall **imitieren**.)

Um zukünftige Probleme zu vermeiden, stellen Sie sicher, dass Ihre Umgebung vorbereitet ist: Konfigurieren Sie Ihre Firewall für Rublon. Stellen Sie außerdem sicher, dass Standardanforderungen wie DNS-Auflösung und TLS 1.2+ unterstützt werden, sodass alle Systeme die Rublon-Server erreichen können.

So lassen sich viele durch Umgebungsblockaden verursachte Verbindungsprobleme vermeiden, und es wird sichergestellt, dass Rublon mit Ihren Anwendungen zuverlässig kommunizieren kann.

3. Vorbereitung auf Ausfälle

Vorbereitung ist entscheidend, um die Auswirkungen eines Ausfalls zu minimieren. Sobald Sie die möglichen Ausfallszenarien und das Verhalten Ihrer Anwendungen (mit oder ohne Rublon) verstanden haben, empfehlen wir dringend die Erstellung **anwendungsspezifischer Disaster-Recovery(DR)-Pläne.**

Jedes durch Rublon geschützte System kann leicht unterschiedliche Kontinuitätsverfahren erfordern. Die frühzeitige Planung dieser Details stellt sicher, dass Sie im Falle eines Ausfalls schnell und sicher reagieren können. Ziel ist es, dass **niemand unvorbereitet ist** – Administratoren wissen, was zu tun ist, und Benutzer wissen, was sie erwartet.

Bei der Entwicklung Ihrer Pläne sollten Sie Folgendes berücksichtigen:

- **Failover/Bypass-Verfahren:** Dokumentieren Sie den Prozess, um Rublon MFA manuell zu umgehen oder eine Anwendung im „Fail Open"-Modus laufen zu lassen, wenn der Rublon-Dienst nicht verfügbar ist und kein automatisches Failover funktioniert. Dies kann beispielsweise eine Änderung einer Einstellung, ein Update eines Registry-Keys oder das Umleiten der Authentifizierung zur temporären Umgehung von Rublon MFA beinhalten. Wissen Sie, wie Sie diese Bypass-Optionen schnell auslösen können und wie der Fail Mode auf jedem Rublon-Connector eingerichtet wird?

- **Mehrere registrierte MFA-Methoden fördern:** Im Rahmen des Standard-Onboarding-Prozesses sollte jeder Benutzer mindestens zwei MFA-Methoden registrieren (z. B. Mobile Push, TOTP, SMS, E-Mail und FIDO-Sicherheitsschlüssel). Dadurch wird sichergestellt, dass Benutzer bei einem Ausfall einer Methode ohne Unterbrechung auf eine andere Methode wechseln können, ohne interne Helpdesk-Tickets zu erzeugen.

- **Entfernungs-/Deaktivierungsschritte:** Beschreiben Sie, wie Rublon bei Bedarf aus dem Authentifizierungsprozess einer geschützten Anwendung entfernt werden kann. Dies kann das Deinstallieren, Abschalten eines Rublon-Connectors, das Deaktivieren einer MFA-Erzwingungseinstellung in der Rublon Admin Console oder das Zurücksetzen auf eine lokale Login-Methode umfassen. Identifizieren Sie die notwendigen Schritte und erforderlichen Berechtigungen im Voraus, damit Administratoren diese auch in Ausfallszenarien sicher ausführen können.

- **Verantwortliches Personal:** Bestimmen Sie, wer in Ihrer Organisation für die Sicherstellung der Geschäftskontinuität verantwortlich ist. Stellen Sie sicher, dass diese Personen über die nötigen Zugänge und Anmeldedaten verfügen, um Konfigurationsänderungen vorzunehmen (z. B. Zugriff auf Server, auf denen Rublon-Connectoren installiert sind, ein Administratorkonto in der Rublon Admin Console usw.). Es empfiehlt sich, dass mehr als eine Person mit dem Plan vertraut ist, falls der primäre Verantwortliche nicht verfügbar ist.

- **Tests und Übungen:** Warten Sie nicht auf einen echten Vorfall, um herauszufinden, ob Ihr Plan funktioniert. Führen Sie Ihre Failover-Verfahren so oft wie möglich in einer kontrollierten Umgebung durch (z. B. Simulation eines Rublon-Ausfalls in einer Staging-Umgebung). Regelmäßige Übungen stellen sicher, dass die dokumentierten Schritte funktionieren, falls Rublon nicht erreichbar ist, und helfen den Mitarbeitern, sich mit deren Durchführung vertraut zu machen. Sollte sich während eines Tests herausstellen, dass der Plan nicht wie vorgesehen funktioniert, passen Sie die Dokumentation entsprechend an.

- **Kommunikationsplan:** Legen Sie fest, wie Sie während eines Ausfalls mit IT-Teams und Endbenutzern kommunizieren. (In diesem Guide stellen wir Beispielvorlagen für Benutzerkommunikation bereit.) Vorgefertigte Nachrichten und ein interner Benachrichtigungsprozess sparen wertvolle Zeit, wenn jede Minute zählt. Stellen Sie außerdem sicher, dass sowohl primäre als auch alternative Kommunikationskanäle vorbereitet sind, wie z. B. E-Mail-Benachrichtigungen oder dedizierte Chat-Kanäle. So steht eine verlässliche Alternative zur Verfügung, falls der Hauptkanal ausfällt. Etablieren Sie einen klar definierten Prozess für die Zustellung von Nachrichten, einschließlich Backup-Verfahren, um Ihre Vorbereitung auf Ausfälle weiter zu verbessern.

4. Konfigurationsentscheidung: Fail Safe vs. Fail Secure

Ein wesentlicher Bestandteil der Kontinuitätsplanung ist die Entscheidung, wie sich jede Anwendung verhalten soll, wenn Rublon nicht verfügbar ist. Die meisten Rublon-Connectoren ermöglichen die Konfiguration eines **Fail Mode**, bei dem im Wesentlichen zwischen „fail open“ (Zugriff erlauben) und „fail closed“ (Zugriff verweigern), wenn MFA nicht abgeschlossen werden kann, gewählt wird. Wir bezeichnen dies manchmal als **Fail Safe** (Bypass) und **Fail Secure** (Zugriff verweigern). Welche Betriebsart für jede Anwendung gewählt wird, ist ein Abwägen zwischen Sicherheit und Benutzerfreundlichkeit und sollte mit den Richtlinien Ihrer Organisation übereinstimmen. Siehe Abschnitt “Rublon Fail Mode” für eine detaillierte Erklärung des Fail-Mode-Verhaltens.

Die meisten Rublon-Connectoren erlauben die Konfiguration des Fail Mode. In den nächsten Abschnitten gehen wir darauf ein, was in den einzelnen Ausfallszenarien passiert und wie der Fail Mode dabei eine Rolle spielt. Behalten Sie im Hinterkopf, welchen Modus Sie für jede Anwendung festgelegt haben (oder festlegen werden), und dokumentieren Sie diese Entscheidungen, da sie Ihre Notfallplanung direkt beeinflussen.

Berücksichtigen Sie die folgenden Faktoren bei der Wahl des Fail Mode für eine Anwendung:

- **Richtlinien- und Compliance-Anforderungen:** Gibt es regulatorische Vorgaben oder interne Sicherheitsrichtlinien, die vorschreiben, dass Zugriffe blockiert werden müssen, sollte MFA nicht verifiziert werden können? Beispielsweise schreiben manche Standards vor, dass auf bestimmten Systemen jederzeit MFA verwendet werden muss. In diesem Fall ist Fail Secure (Zugriff verweigern ohne MFA) für diese Systeme erforderlich. Weniger regulierte Umgebungen können dagegen Fail Safe (Bypass MFA) zulassen, um die Verfügbarkeit zu wahren. Die Entscheidung sollte dokumentiert und regelmäßig überprüft werden, da sich Vorgaben und organisatorische Prioritäten ändern können.

- **Sensibilität von Daten und Systemen:** Bewerten Sie den Typ der Daten und Ressourcen, die die Anwendung schützt. Für Systeme mit hochsensiblen Informationen (z. B. Finanzdaten, Patientendaten, kritische Infrastrukturen) sollte eine höhere Sicherheit priorisiert werden, also Fail Secure, um das Risiko unbefugten Zugriffs ohne MFA zu verringern. Für Anwendungen mit weniger sensiblen, niedrig priorisierten Daten kann dagegen die Verfügbarkeit durch Fail Safe priorisiert werden, damit Benutzer während eines Ausfalls weiterarbeiten können.

- **Benutzergruppen und Zugriffsebenen:** Eine einheitliche Lösung lässt sich nicht auf alle Szenarien anwenden. Unterschiedliche Benutzer können unterschiedliche Risikoprofile haben. Beispielsweise kann für Benutzer mit privilegiertem Zugriff die Nutzung von Fail Secure (kein Bypass) verpflichtend sein, während allgemeine Mitarbeiter über Fail Safe zugreifen dürfen.

- **Balance zwischen Sicherheit und Benutzerfreundlichkeit:** Prüfen Sie sowohl die Folgen einer Zugriffssperre für die Benutzer als auch die Folgen für die Sicherheit, wenn MFA außer Kraft gesetzt wird. Fail Safe (Bypass) stellt sicher, dass Benutzer niemals den Zugriff auf ihre Systeme aufgrund eines MFA-Ausfalls verlieren. Das verbessert die Produktivität, jedoch auf Kosten einer temporär fehlenden zweiten Authentifizierungsstufe. Fail Secure stellt sicher, dass die MFA-Sicherheitsanforderungen eingehalten werden, allerdings können sich Benutzer erst wieder anmelden, wenn der MFA-Dienst verfügbar ist. Sie können Fail Safe für Systeme wählen, bei denen kontinuierlicher Zugriff oberste Priorität hat (z. B. Windows-Endpunkte), und Fail Secure für Systeme, bei denen ein MFA-Bypass ein inakzeptables Risiko darstellen würde (z. B. VPN-Zugriff auf ein Produktionsnetzwerk).

5. Arten von Ausfällen

Nicht alle Dienstunterbrechungen sind gleich. Störungen im Rublon-MFA-Dienst lassen sich in zwei Hauptkategorien einteilen:

- **Rublon API Unreachable –** Ein vollständiger Ausfall, bei dem Rublon-Connectoren die Rublon API nicht erreichen können. Dies löst in der Regel den konfigurierten Fail Mode des Connectors aus (Fail Safe oder Fail Secure) und erlaubt oder verweigert Anmeldungen automatisch.

- **Rublon Service Degradation** – Eine teilweise Störung, bei der die Rublon API weiterhin erreichbar ist, aber bestimmte Rublon-Dienste langsam reagieren, intermittierend ausfallen oder nicht verfügbar sind. In diesem Fall wird der Fail Mode nicht automatisch ausgelöst, sodass Administratoren möglicherweise manuell eingreifen müssen.

Warum zwischen „Unreachable“ und „Degraded“ unterscheiden?

Der Hauptgrund ist, dass sich Ihre Reaktion unterscheidet. Wenn Rublon vollständig unerreichbar ist, hängt Ihr Kontinuitätsplan stark von den **Fail Safe- oder Fail Secure-Einstellungen** ab, die Sie im Voraus festgelegt haben. Wenn der Dienst hingegen beeinträchtigt ist, kann es erforderlich sein, **aktiv einzugreifen** (z. B. Benutzer über Workarounds zu informieren oder Einstellungen vorübergehend zu ändern), da das System nicht automatisch in den Failover-Modus wechselt. Behalten Sie diese Szenarien im Hinterkopf, und überlegen Sie, wie sich Ihre Anwendungen in jedem Szenario verhalten sollen.

Rublon API Unreachable

Dieses Szenario beschreibt eine vollständige Unterbrechung der Konnektivität zur Rublon API. Im Wesentlichen können Rublon-Connectoren die **Rublon API überhaupt nicht erreichen (HTTP Code 404) oder eine Verbindung wird hergestellt, aber ein HTTP-Code 500–599 wird zurückgegeben**. In diesem Szenario greift der Fail Mode.

Wenn die Rublon API unerreichbar ist, wird der Rublon Prompt (der Bildschirm für die zweite Faktorabfrage) während der Anmeldung nicht geladen, oder die Anfrage an die Rublon API läuft bei promptlosen Integrationen aus. Rublon-Connectoren warten in der Regel eine vordefinierte Zeit auf eine Antwort, bevor sie entscheiden, ob die Rublon API unerreichbar ist. Danach wird der konfigurierte **Fail Mode** aktiv, der je nach Einstellung automatisch Anmeldungen erlaubt oder

verweigert. Dies wird als „Failover“-Szenario bezeichnet, da der Connector auf seinen vordefinierten Modus (safe/bypass oder secure/deny) zurückgreift.

Mögliche Ursachen für ein „Rublon API Unreachable“-Ereignis sind unter anderem:

- **Rublon Downtime:** Die Rublon API ist vorübergehend ausgefallen oder reagiert nicht. Dies ist selten, kann aber vorkommen (z. B. bei geplanter Wartung).
- **Netzwerkkonnektivitätsprobleme:** Probleme im Netzwerkpfad zwischen Ihrer Umgebung und der Rublon API können die Dienste unerreichbar machen. Typischerweise entstehen solche Probleme beim Kunden selbst oder innerhalb der Internetinfrastruktur. Beispiele sind ISP-Ausfälle, Routing-Probleme, ein DNS-Fehler bei der Auflösung der Rublon-Domains oder ein Vorfall (z. B. ein Glasfaserkabelbruch), der die Konnektivität unterbricht. Eine häufige Ursache sind lokale Fehlkonfigurationen – etwa wenn eine geänderte Firewall-Regel oder ein Proxy den Datenverkehr zu Rublon blockiert und es so unerreichbar erscheinen lässt.
- **Fehlkonfigurationen von Integrationen:** Ist ein Rublon-Connector falsch eingerichtet, kann er die Rublon API möglicherweise nicht erreichen. Ein falscher Rublon System Token oder Rublon Secret Key in der Konfiguration kann dazu führen, dass Authentifizierungsanfragen fehlschlagen. In diesem Fall behandelt der Connector die Situation ähnlich wie einen unerreichbaren Dienst, da er keine gültige Antwort erhält. Ebenso kann die Verwendung einer veralteten Rublon-Connector-Version, die nicht kompatibel ist, Fehler bei der Kontaktaufnahme mit Rublon verursachen.

Rublon Service Degradation

Dies bezeichnet ein Szenario, in dem die Rublon API zwar **noch erreichbar** ist, jedoch bestimmte Aspekte des MFA-Dienstes nicht ordnungsgemäß funktionieren. In einem solchen Fall können Ihre Anwendungen weiterhin eine Verbindung zu Rublon herstellen (die Connectoren lösen also keinen Fail Mode aus), jedoch können Benutzer Fehler oder Verzögerungen bei der MFA-Verifizierung erleben.

In einem Degradation-Szenario **lösen Connectoren den Fail Mode nicht automatisch aus**, da die Rublon API noch antwortet. Verantwortliche für Geschäftskontinuität müssen die Anzeichen eines beeinträchtigten Dienstes erkennen (z. B. wenn mehrere Benutzer melden, dass ihre SMS-Passcodes oder E-Mails nicht funktionieren) und dann entscheiden, ob Maßnahmen

erforderlich sind, etwa ein manuelles temporäres Außer-Kraft-Setzen der MFA für die Dauer des Problems.

Beispiele für Degradation:

- **Ausfälle bestimmter Methoden:** Eine oder mehrere Zweitfaktor-Methoden funktionieren nicht, während andere weiterhin verfügbar sind. Beispielsweise könnte Rublons Telefonieanbieter für SMS oder Telefonanrufe einen Ausfall haben, sodass SMS-Passcodes nicht zugestellt werden. Andere Methoden wie Mobile Push oder FIDO-Sicherheitsschlüssel funktionieren jedoch weiterhin.

- **Teilweiser Ausfall oder Langsamkeit:** Die Rublon-Infrastruktur kann unter hoher Last stehen oder eine lokale Störung aufweisen, die zu Verzögerungen bei der Authentifizierung führt. Benutzer können Verzögerungen oder sporadische Fehlschläge bei MFA-Aufforderungen erleben, bis eine Authentifizierung schließlich erfolgreich ist. Dies kann auftreten, wenn eine Komponente der Rublon-Cloud (z. B. ein bestimmter Server-Cluster) beeinträchtigt ist, während andere weiterhin funktionieren. Benutzer könnten melden, dass „MFA hängt“ oder dass sie mehrere Versuche benötigen, um sich erfolgreich anzumelden.

- **Softwareprobleme:** In sehr seltenen Fällen kann ein Softwarefehler den Dienst beeinträchtigen. Beispielsweise kann eine neue Version einen Fehler enthalten, wodurch manche Authentifizierungsversuche fehlschlagen, auch wenn der Dienst an sich verfügbar ist. Auch wenn solche Ereignisse selten sind, sollte Ihnen bewusst sein, dass sie möglich sind. In diesem Fall ist der Dienst technisch ‚erreichbar‘, jedoch nicht vollständig funktionsfähig.

6. Erkennen von Ausfällen

Wie wissen Sie, ob ein Ausfall vorliegt? Früherkennung ist entscheidend. Mithilfe der folgenden Monitoring-Schritte lassen sich Ausfälle schnell erkennen und den Szenarien ‚unerreichbar' oder ‚beeinträchtigt' zuordnen. So kann Ihr konkreter Notfallplan rechtzeitig umgesetzt werden.

Die folgenden Schritte und Tools helfen Ihnen dabei, ein Rublon-Serviceproblem schnell zu identifizieren:

- **Rublon Status Page überwachen:** Rublon stellt eine Echtzeit-Statusseite unter status.rublon.com bereit. Diese Seite sollte Ihr erster Anlaufpunkt sein, wenn Sie einen großflächigen Vorfall vermuten. Die Statusseite meldet den Zustand zentraler Komponenten wie der Rublon API, Admin Console, Support-Portal, Webseite und sogar spezifischer Funktionen wie SMS-/Telefon-/E-Mail-Zustellung. Bei bevorstehenden Dienstunterbrechungen oder Wartungsarbeiten werden Updates auf der Rublon Status Page veröffentlicht. Wir empfehlen, Updates zu abonnieren. Auf diese Weise werden Sie proaktiv benachrichtigt, sobald ein Vorfall auftritt, und verpassen keine wichtigen Ankündigungen zu Ausfällen oder Wartungen.

- **Lokale Diagnose:** Zeigt die Statusseite alle Rublon-Dienste als funktionsfähig an, Sie jedoch weiterhin Störungen erfahren , liegt die Ursache möglicherweise in Ihrer Umgebung oder im dazwischenliegenden Netzwerk. In diesem Fall sollten Sie einige Diagnoseschritte durchführen:

    - **Konnektivität zur Rublon API prüfen:** Versuchen Sie, den Rublon-API-Endpunkt aus Ihrer Umgebung zu erreichen. Öffnen Sie dazu einen Webbrowser auf einem betroffenen Gerät und navigieren Sie zu **https://core.rublon.net**. Dies ist der Core Authentication Server von Rublon. Bei erfolgreicher Erreichbarkeit zeigt der Browser die Meldung *„Rublon Authentication Server works!"*. Führen Sie diesen Test von mehreren Netzwerken und Geräten durch. Zeigt ein Netzwerk die Meldung, ein anderes nicht, deutet das auf ein lokales Problem (z. B. Firewall- oder Routing-Problem) hin.

    - **Traceroute/DNS:** Standard-Netzwerktools helfen Probleme sichtbar zu machen. Verwenden Sie z. B. **tracert/traceroute**, um zu prüfen, ob der Datenverkehr das Internet erreicht. Gibt der DNS-Befehl (**nslookup core.rublon.net**) keine IP-Adresse zurück, liegt vermutlich ein DNS-Problem vor. Stoppt die Traceroute innerhalb Ihres Netzwerks, handelt es sich wahrscheinlich um eine lokale Störung.

    - **Firewall-/Proxy-Logs:** Nutzen Sie einen Webproxy oder eine Firewall, prüfen Sie die Logs rund um den Zeitpunkt der Störung. Dort finden sich möglicherweise Hinweise darauf, dass Verbindungen zu den Rublon-Domains oder -IPs blockiert oder abgebrochen wurden. Beachten Sie, dass sich Rublons IP-Adressen ändern können (z. B. bei Hosting-Änderungen), sodass unter Umständen ein Update erforderlich ist. Achten Sie insbesondere auf kürzlich vorgenommene Firewall-Regeländerungen oder sicherheitsrelevante Alerts (z. B. von IDS/IPS-Systemen), die zeitgleich mit dem Vorfall auftreten.

- **Unterscheiden zwischen weit verbreiteten und isolierten Störungen:** Prüfen Sie, ob das Problem alle Benutzer bzw. Anwendungen betrifft oder nur bestimmte. **Schlagen alle Authentifizierungsmethoden fehl**, deutet dies auf einen großflächigen Ausfall hin (z. B. Rublon API oder ein größeres Netzwerkproblem). Betrifft es dagegen nur eine spezifische Methode oder Anwendung, handelt es sich wahrscheinlich um einen Degradation-Fall oder ein app-spezifisches Problem.
    - Beispiel: Nur SMS-Codes kommen nicht an, während Push und E-Mail funktionieren → wahrscheinlich Rublon-Degradation im SMS-Kanal oder ein Problem beim SMS-Provider.
    - Beispiel: Nur Ihr VPN (mit Rublon Authentication Proxy) ist betroffen, Windows-Logins mit Rublon funktionieren jedoch → das Problem liegt vermutlich am Proxy oder an dessen Konfiguration.
- **Rublon Support kontaktieren:** Sollten Sie nach Durchführung aller oben genannten Schritte weiterhin unsicher sein oder Unterstützung benötigen, zögern Sie nicht, den Rublon Support zu kontaktieren. Geben Sie in Ihrer Anfrage so viele Details wie möglich an (z. B. was genau fehlschlägt, Fehlermeldungen, Screenshots, relevante Log-Auszüge).

7. Rublon Fail Mode

Rublon-Connectoren enthalten ein Konzept namens **Fail Mode**, das steuert, wie sich der Connector verhält, wenn die MFA aufgrund fehlender Verbindung zur Rublon API nicht möglich ist.

Die möglichen Optionen für den Fail Mode sind:

- **Fail Safe (Bypass)** – Wenn die Rublon API nicht erreichbar ist, erhalten Benutzer **Zugriff** auf Rublon-integrierte Anwendungen, sofern sie die Primärauthentifizierung bestehen.
- **Fail Secure (Deny)** – Wenn die Rublon API nicht erreichbar ist, wird Benutzern der **Zugriff** auf Rublon-integrierte Anwendungen **verweigert**, selbst wenn sie die Primärauthentifizierung bestehen.

Beide Optionen haben ihre Vorteile. Mit Rublon können Sie flexibel für jeden Connector den passenden Modus festlegen und bei Bedarf kombinieren, z. B. die meisten Connectoren auf **Fail Safe** und besonders sensible Systeme auf **Fail Secure**. Definieren und dokumentieren Sie die Einstellungen im Voraus, um auf geplante Wartungen und ungeplante Ausfälle vorbereitet zu sein.

Fail Safe Mode („Bypass When Unreachable“)

Fail Safe bedeutet, dass, wenn die Rublon API nicht erreichbar ist, sich der Benutzer **ohne Abschluss der MFA anmelden kann**. Mit anderen Worten: Der zweite Faktor wird übersprungen (Bypass), und die Primäranmeldedaten (normalerweise Benutzername/Passwort) allein gewähren Zugriff.

- **Priorität:** Fail Safe priorisiert Verfügbarkeit. Benutzer können weiterarbeiten, auch wenn der MFA-Dienst ausgefallen ist. Allerdings geht Fail Safe zulasten der Sicherheit während des Ausfalls, da Benutzer nicht mit dem zweiten Faktor konfrontiert werden..
- **Verhalten:** Aus Sicht des Endbenutzers wirkt ein Fail Safe-Ereignis wie eine normale Anmeldung, nur dass keine 2FA-Abfrage erfolgt. Beispielsweise kann sich ein Mitarbeiter wie gewohnt an seinem Windows-Laptop anmelden, Benutzername und Passwort eingeben, und anstelle der Rublon Prompt wird die Anmeldung direkt abgeschlossen. Das System hat den MFA-Prozess des Benutzers ausgelassen.

- **Wann verwenden:** Fail Safe wird in der Regel für Systeme empfohlen, bei denen die Aufrechterhaltung des Zugangs wichtiger ist als die Durchsetzung von MFA. Viele Organisationen setzen ihn für benutzerorientierte Systeme wie Workstations oder interne Anwendungen ein, um ein Aussperren von Mitarbeitern zu vermeiden. Wenn Sie Fail Safe implementieren, achten Sie darauf, zusätzliche Kontrollen einzusetzen (z. B. starke Primärauthentifizierung, Netzwerküberwachung, Zugriffsbeschränkungen), um den temporären Verlust von MFA während eines Ausfalls abzumildern.

- **Konfiguration:** Jeder Rublon-Connector bietet eine eigene Einstellungsmöglichkeit für **Fail Safe** (in der Regel durch Setzen der Option **FailMode** auf „bypass“). **Rublon-Connectoren sind standardmäßig auf Fail Safe gesetzt**, um zu vermeiden, dass Administratoren sich während der ersten Einrichtung versehentlich aussperren.

Fail Secure Mode („Deny When Unreachable“)

Fail Secure bedeutet, dass dem Benutzer der Zugriff **verweigert** wird, wenn die Rublon API nicht erreichbar ist. Selbst wenn die Primäranmeldedaten korrekt eingegeben werden, bleibt der **Zugriff blockiert, solange der zweite Faktor nicht überprüft werden kann**.

Die Auswirkungen von Fail Secure sind eindeutig: Keine Rublon API bedeutet keine Anmeldung. Damit wird die Sicherheit maximiert, jedoch auf Kosten der Verfügbarkeit. Wenn Sie diesen Modus wählen, sollte Ihr **Business Continuity Plan festlegen, wie mit Ausfallzeiten umzugehen ist.** Dies kann bedeuten, Benutzer warten zu lassen oder eine alternative Anmeldemethode bereitzustellen (z. B. ein Notfallkonto ohne Rublon, das jedoch eigene Risiken birgt). Viele Organisationen setzen Fail Secure für Systeme mit kleiner Benutzerbasis oder dort ein, wo Unterbrechungen akzeptabler sind als das Risiko unbefugter Zugriffe.

- **Priorität:** Dieser Modus priorisiert Sicherheit. Eine Anmeldung ohne MFA ist nicht möglich, wodurch jedoch das Risiko entsteht, dass die Anwendung während eines Ausfalls nicht verfügbar ist (selbst für legitime Benutzer, bis MFA wieder funktioniert).

- **Verhalten:** In einem Fail Secure-Szenario wird Benutzern der Zugriff verweigert, wenn keine Verbindung zur Rublon API hergestellt werden kann. Nachdem sie Benutzername und Passwort eingegeben haben, erhalten sie unmittelbar eine Meldung wie „Access Denied!“. Für die Benutzer wirkt dies verwirrend, da sie keinen Fehler gemacht haben, sondern ausschließlich aufgrund der MFA-Einstellung blockiert werden. Daher sollten

Benutzer im Voraus über das Verhalten von Fail Secure während eines Ausfalls informiert werden.

- **Wann verwenden:** Fail Secure eignet sich für hochsichere Systeme, bei denen das Verweigern von Zugriffen gegenüber einer Anmeldung ohne MFA vorzuziehen ist. Das gilt insbesondere für Anwendungen, die sensible Daten schützen oder als Zugang zu einem größeren Netzwerk dienen. Manche Organisationen setzen Fail Secure für externe Einstiegspunkte wie VPNs oder privilegierte IT-Administrationsportale ein. Vor der Entscheidung für Fail Secure sollten Sie folgende Auswirkungen berücksichtigen:
    - Wie kritisch ist es, dass dieses System zugänglich bleibt?
    - Gibt es alternative Möglichkeiten, auf das System zuzugreifen, falls MFA ausfällt (z. B. Break-Glass-Admin-Konto oder Konsolenzugriff)?
    - Wissen die Benutzer, dass ein MFA-Ausfall bedeutet „Bitte warten, Sie können sich jetzt nicht anmelden“?
- **Konfiguration:** Fail Secure wird aktiviert, indem die **Fail Mode**-Einstellung auf „deny“ gesetzt wird. Detaillierte Anleitungen finden Sie unter: Wie wird der Fail Mode in Rublon-Connectoren eingestellt?. Es empfiehlt sich, das Fail Secure-Verhalten in einer Testumgebung zu überprüfen (z. B. durch temporäres Blockieren des Internetzugangs des Connectors), um sicherzustellen, dass der Zugriff tatsächlich wie vorgesehen verweigert wird.

8. Fail Mode-Unterstützung durch Rublon-Integration

Rublon-Anwendungen, Plugins und Connectoren, die **Fail Mode-Modus** unterstützen:

- Rublon Authentication Proxy
- Rublon Access Gateway
- Rublon MFA for Windows Logon & RDP
- Rublon MFA for Remote Desktop Gateway
- Rublon MFA for RD Web Access
- Rublon MFA for RD Web Client
- Rublon MFA for Outlook Web App (OWA)
- Rublon MFA for Active Directory Federation Services (AD FS)
- Rublon MFA for Linux SSH
- Rublon MFA for Veritas NetBackup
- Rublon MFA for Jira
- Rublon MFA for Confluence

Rublon-Integrationen, die **keinen Fail Mode-Modus** unterstützen:

- Rublon MFA for Roundcube
- Rublon MFA for WordPress

Detaillierte Anleitungen zum Konfigurieren des Fail Mode für jeden Connector finden Sie unter:

Wie wird der Fail Mode in Rublon-Connectoren eingestellt?

9. Szenarien und Reaktionen bei nicht erreichbarer Rublon API

Die Rublon API kann auf verschiedene Weise nicht erreichbar sein:Entweder fällt sie vollständig aus (kein Zugriff von irgendeinem Netzwerk oder Endpunkt), oder sie ist nur für bestimmte Connectoren oder Standorte blockiert. In beiden Fällen erhält der Connector keine gültige Antwort und wendet seinen Fail Mode an.

Kommunikation und Monitoring sind entscheidend:

Halten Sie Ihr IT-Sicherheitsteam und das Management über temporäre Maßnahmen informiert. Wenn Sie z. B. allen Benutzern der Finanzabteilung den MFA-Bypass erlauben, informieren Sie den Sicherheitsbeauftragten. Dies kann ein erhöhtes Risiko darstellen, das im Nachhinein dokumentiert und bewertet werden muss. Protokollieren Sie daher genau, welche Maßnahmen durchgeführt wurden (z. B. ‚Um 10:00 Uhr VPN auf Bypass gesetzt aufgrund eines Rublon-Ausfalls'). Diese Dokumentation unterstützt spätere Nachbearbeitungen und Audits.

Stellen Sie außerdem sicher, dass Ihr Helpdesk und die Benutzer wissen, dass ein Ausfall vorliegt und welche Fail Mode-Einstellung aktiv ist:

- Wenn Sie **Fail Safe (bypass)** verwenden, könnten Benutzer überrascht sein, dass keine MFA-Abfrage erscheint.
- Wenn Sie **Fail Secure (deny)** verwenden, könnten Benutzer überrascht sein, dass sie keinen Zugriff auf Anwendungen erhalten.
- Eine kurze Nachricht kann hier viel Verwirrung vermeiden. Später in diesem Leitfaden finden Sie entsprechende Beispielkommunikationsvorlagen für Benutzer.

Beispiel: Die Rublon API ist nicht erreichbar, es kann keine Verbindung von irgendeinem Netzwerk oder Endpunkt hergestellt werden. Dadurch ist sie für alle Rublon-Connectoren nicht verfügbar.

Auswirkung: Ist Fail Secure aktiv, können sich Benutzer nicht anmelden, da die MFA nicht abgeschlossen werden kann. Bei Fail Safe hingegen erhalten Benutzer Zugriff ohne MFA..

Erkennung: Die Rublon Status Page zeigt Probleme mit der Rublon API an. Werden dort keine Probleme gemeldet, weist dies stark auf ein Konfigurationsproblem des Connectors oder auf eine fehlerhafte Firewall-Konfiguration hin.

Reaktionsmöglichkeiten:

- **Wechsel zu Bypass (Fail Safe) Mode:** Wird eine Anwendung normalerweise im Fail Secure-Modus betrieben, kann im Ausfall eine schnelle Lösung sein, temporär auf Fail Safe umzuschalten. Dazu setzen Sie den Fail Mode auf „bypass“. Beispiel: Ist der Rublon Auth Proxy auf „deny“ gesetz, bearbeiten Sie die Konfigurationsdatei, ändern fail_mode: "bypass" und starten den Proxy-Dienst neu. Dadurch wird Benutzern vorübergehend Zugriff ohne MFA gewährt, bis die Einstellung zurückgesetzt wird. Viele Administratoren nutzen dieses Vorgehen auch proaktiv bei geplanten Ausfällen (z. B. während Wartungsarbeiten).

  Wichtig: Protokollieren Sie alle Änderungen, um eine spätere Rücksetzung sicherzustellen. Eine versehentlich dauerhaft aktivierte Bypass-Einstellung stellt eine Sicherheitslücke dar.

- **Firewall-/Netzwerkeinstellungen anpassen:** Wird der Zugriff auf die Rublon API durch Firewall- oder Netzwerkrichtlinien blockiert (z. B. verhindert eine neue Richtlinie den Zugriff auf **core.rublon.net**), muss die Konfiguration so schnell wie möglich korrigiert werden.
  Mögliche Maßnahmen:
  - Ausgangsport 443 öffnen und **https://core.rublon.net** zur Allowlist hinzufügen.
  - Die aktuellen Rublon AWS IP-Ranges zur Firewall hinzufügen.
  - Eine restriktive Regel vorübergehend deaktivieren (mit entsprechender Freigabe), bis sie so angepasst ist, dass Rublon zugelassen wird.
  - Mehr erfahren: Wie muss ich meine Firewall für Rublon konfigurieren?

10. Szenarien und Reaktionen bei eingeschränktem Dienst

Ist die Infrastruktur von Rublon nur teilweise beeinträchtigt, sind möglicherweise zusätzliche Schritte erforderlich, um Störungen zu minimieren. Anders als bei einem vollständigen Ausfall funktioniert die MFA in einem eingeschränkten Szenario noch teilweise, sodass kein automatisches Failover (Fail Mode) ausgelöst wird.

Kommunikation und Monitoring sind entscheidend:

Informieren Sie Ihr Helpdesk-Team und die Benutzer über das Problem und die verfügbaren Workarounds. Andernfalls könnten Benutzer mit MFA-Problemen wiederholt Anmeldeversuche starten oder fälschlich annehmen, ihr Gerät sei defekt. Eine kurze Nachricht kann hier viel Verwirrung vermeiden. Später in diesem Leitfaden finden Sie entsprechende Beispielkommunikationsvorlagen.

Wenn die Einschränkung nur einen Connector oder eine Integration betrifft:

Beispiel: Nur die MFA für Ihr VPN schlägt fehl, während andere Anwendungen mit Rublon normal funktionieren. In diesem Fall kann Ihr Continuity-Plan vorsehen, diese einzelne Anwendung temporär von Rublon-MFA auszunehmen (z. B. Rublon für das VPN deaktivieren, bis die Integration repariert ist). Prüfen Sie dabei stets, ob das Problem global oder isoliert auftritt, da sich die Reaktion entsprechend unterscheidet.

Szenario A: Ausfall einer spezifischen Authentifizierungsmethode

Beispiel: Der SMS-Dienst von Rublon ist ausgefallen, und Passcodes per SMS erreichen die Benutzer nicht. Andere Methoden (Push-Benachrichtigungen, TOTP-Codes, E-Mail-Links, Telefonanrufe) funktionieren weiterhin.

Auswirkung: Benutzer, die ausschließlich die betroffene Methode (in diesem Beispiel SMS) nutzen, können die MFA nicht abschließen. Sie fordern SMS-Codes an, die jedoch nicht zugestellt werden. Benutzer anderer Methoden sind nicht betroffen.

Erkennung: Die Rublon Status Page zeigt Probleme bei der SMS-Zustellung an (z. B. „SMS Message Delivery“ als eingeschränkt). Benutzer beschweren sich: *„SMS-Codes kommen nicht an.“*

Reaktionsmöglichkeiten:

- **Alternative Authentifizierungsmethode vorschlagen:** Informieren Sie die Benutzer über das Problem und raten Sie zur Verwendung einer anderen Methode, z. B. Mobile Push oder E-Mail-Link. Voraussetzung ist, dass Benutzer eine zusätzliche Authentifizierungsmethode registriert haben.Idealerweise verfügen Benutzer immer über mindestens zwei Faktoren (z. B. Rublon Authenticator + Telefonnummer oder FIDO2-Sicherheitsschlüssel + Drittanbieter-App) als Backup.

- **Einen Bypass Code verwenden:** Steht keine andere Methode zur Verfügung und ist ein Benutzerzugriff erforderlich, kann ein Administrator einen Bypass Code generieren (ein einmaliger Code, der MFA überspringt) und den Benutzer in der Anwendung anleiten.

- **Status überwachen:** Beobachten Sie die Rublon Status Page. Falls Sie die Statusseite abonniert haben, erhalten Sie automatische Benachrichtigungen, sobald das Problem behoben ist. Solche Ausfälle einzelner Methoden werden in der Regel schnell vom Drittanbieter behoben.

- **Fail Mode nicht ändern:** In diesem Szenario ist es normalerweise nicht erforderlich, den Fail Mode anzupassen, da MFA insgesamt weiterhin funktioniert. Der Fokus liegt darauf, den Benutzern klare Anweisungen zu geben.

Szenario B: Allgemeine Dienstverlangsamung oder teilweiser Ausfall

Beispiel: Die Rublon API antwortet verzögert oder einzelne Authentifizierungsanfragen schlagen sporadisch fehl. Benutzer berichten von ablaufenden MFA-Prompts (Timeout) oder Fehlermeldungen, während die Anmeldung nach mehreren Versuchen doch funktioniert.

Auswirkung: Die Authentifizierung ist unzuverlässig. Das kann Benutzer verunsichern und den Arbeitsablauf erheblich beeinträchtigen. Der Zugriff wird nicht vollständig blockiert, jedoch treten Verzögerungen auf.

Erkennung: Typische Benutzermeldungen sind „MFA funktioniert nicht zuverlässig“ oder „MFA ist langsam“. Die Rublon Status Page zeigt in diesem Fall eine Beeinträchtigung eines oder mehrerer Dienste an.

Reaktionsmöglichkeiten:

- **Rublon Status Page prüfen:** Beeinträchtigungen werden in der Regel relativ schnell behoben (oft innerhalb von Minuten bis zu einer Stunde). Planen Sie daher, wie lange Sie bereit sind, im eingeschränkten Modus zu bleiben, bevor Sie Maßnahmen ergreifen (z. B. nach 30 Minuten mit hoher Fehlerquote den Bypass-Plan aktivieren).
- **Benutzer informieren:** Wenn das Problem geringfügig ist und die Statusseite eine schnelle Behebung erwarten lässt, teilen Sie den Benutzern mit: *„Derzeit kommt es bei der MFA zu zeitweisen Störungen. Bitte versuchen Sie es erneut, falls ein Fehler auftritt, und rechnen Sie mit möglichen Verzögerungen.“* Bereits eine kurze Kommunikation kann Support-Tickets deutlich reduzieren.
- **MFA-Überprüfung vorübergehend überspringen:** Wenn der eingeschränkte Dienst die Arbeit erheblich behindert (z. B. Anmeldungen dauern zu lange oder Arbeit kommt zum Stillstand), können Sie einen temporären Bypass aktivieren, bis das Problem gelöst ist:
  - Alle oder ausgewählte Benutzer auf Bypass umstellen.
  - Benutzer gesammelt einer Gruppe mit Bypass-Status hinzufügen.
  - **Fail Safe** (FailMode=bypass) in einem oder mehreren Rublon-Connectoren aktivieren und per Firewall-Regel den Zugriff auf **core.rublon.net** auf TCP-Port 443 blockieren, um den Bypass zu erzwingen.
  - Falls unbedingt nötig, Rublon-Connectoren temporär deaktivieren oder deinstallieren (**nicht empfohlen**).
  - Stellen Sie sicher, dass alle Änderungen kommuniziert werden, damit klar ist, dass MFA bewusst umgangen wird. Vergessen Sie nicht, die Änderungen nach der Behebung des Vorfalls zurückzusetzen.

11. Kommunikationsvorlagen für Endbenutzer

Klare Kommunikation mit Endbenutzern ist während eines Ausfalls oder einer Dienstunterbrechung entscheidend. Ohne Information könnten Benutzer verunsichert sein oder das Helpdesk mit Tickets überfluten, wenn sie sich plötzlich nicht anmelden können oder ihre MFA-Prompts anders reagieren. Vorgefertigte Nachrichten helfen, Benutzer schnell zu informieren, was passiert und ob Handlungen erforderlich sind. Nachfolgend finden Sie professionelle Vorlagen, die Sie anpassen und über geeignete Kanäle wie E-Mail, Chat oder andere Kommunikationsmittel Ihrer Organisation verteilen können.

Entscheidung, wann Benutzer informiert werden sollen:

Bevor Sie die Vorlagen verwenden, überlegen Sie, wann eine Benachrichtigung sinnvoll ist. Sie können Benutzer direkt informieren, sobald ein Problem bestätigt ist (insbesondere wenn viele Benutzer oder kritische Systeme betroffen sind). Alternativ können Sie einige Minuten abwarten, ob sich das Problem schnell von selbst löst (um unnötigen Alarm zu vermeiden), vor allem außerhalb der Geschäftszeiten oder wenn nur wenige Benutzer betroffen sind. Orientieren Sie sich an Zeitpunkt und Kritikalität: Ein Vorfall am Montagmorgen um 9:00 Uhr erfordert z. B. eine schnelle Kommunikation. Ein Vorfall am Samstag um Mitternacht, der nur ein werktags genutztes System betrifft, möglicherweise nicht. Wenn die Rublon Status Page eine kurze Wartung (z. B. eine Minute) ankündigt, können Sie mit einer Meldung warten, es sei denn, die Situation verlängert sich.

Vorlage 1: Allgemeiner Ausfall – Fail Safe (Bypass)

Szenario: Die Rublon API ist nicht erreichbar oder einer bzw. mehrere Rublon-Dienste sind beeinträchtigt. Daher wurde MFA außer Kraft gesetzt (Fail Safe/Bypass), sodass sich Benutzer vorübergehend nur mit ihrer Primärauthentifizierung anmelden können.

Betreff: Authentifizierungsprobleme – MFA vorübergehend deaktiviert

Text:
Unser Multi-Faktor-Authentifizierungsanbieter (Rublon) meldet aktuell ein Problem mit seinen Diensten. Um sicherzustellen, dass alle Benutzer weiterarbeiten können, haben wir die **MFA-Anforderung beim Login vorübergehend deaktiviert**. Das bedeutet: Sie müssen derzeit keinen zweiten Faktor eingeben, sondern melden sich nur mit Benutzername und Passwort an. Bitte bleiben Sie in dieser Zeit aufmerksam. Nach Behebung des Problems wird die MFA-Anforderung wieder aktiviert, und Sie werden darüber informiert.

Vorlage 2: Allgemeiner Ausfall – Fail Secure (kein Bypass)

Szenario: Die Rublon API ist nicht erreichbar oder einer bzw. mehrere Rublon-Dienste sind beeinträchtigt. Da **kein Bypass** aktiviert ist (Fail Secure aktiv), wird der Zugriff verweigert, bis das Problem behoben ist.

Betreff: Authentifizierungsprobleme – Zugriff vorübergehend nicht verfügbar

Text:
Unser Multi-Faktor-Authentifizierungsanbieter (Rublon) meldet aktuell ein Problem mit seinen Diensten. Anmeldungen bei <betroffene Systeme> sind daher momentan nicht möglich. Diese Einschränkung ist eine bewusste Vorsichtsmaßnahme, da diese Systeme besonders sensibel sind und wir ohne MFA keinen Zugriff gewähren können. Uns ist bewusst, dass dies eine Beeinträchtigung darstellt. Unser IT-Team arbeitet eng mit Rublon zusammen, um das Problem schnellstmöglich zu beheben.**Bitte verzichten Sie auf wiederholte Anmeldeversuche.** Wir informieren Sie, sobald das Problem behoben ist oder eine alternative Zugriffsmethode zur Verfügung steht.

Vorlage 3: Problem mit einer spezifischen Authentifizierungsmethode

Szenario: Eine einzelne MFA-Methode ist beeinträchtigt, während andere weiterhin funktionieren. Beispiele: E-Mail-basierte Authentifizierung schlägt fehl, SMS-Codes werden verzögert zugestellt, Telefonanrufe sind nicht verfügbar.

Betreff: Hinweis zum MFA-Dienst – Bitte alternative Authentifizierungsmethode verwenden

Text:
Unser Multi-Faktor-Authentifizierungsanbieter (Rublon) meldet derzeit ein Problem mit <betroffene Methode>. Wenn Sie normalerweise <Push/SMS/Telefon> als zweiten Faktor nutzen, kann die Anmeldung fehlschlagen. Bitte verwenden Sie stattdessen <alternative Methode>. Wir überwachen die Situation und informieren Sie, sobald <betroffene Methode> wieder verfügbar ist. Wenn Sie Unterstützung bei der Nutzung einer alternativen Methode benötigen oder weiterhin Probleme bei der Anmeldung haben, wenden Sie sich bitte an den IT-Service-Desk.

Zusätzliche Kommunikationstipps

- **Nachverfolgung:** Senden Sie Folgemeldungen, sobald Probleme behoben sind. Beispiel: „Das MFA-Problem wurde behoben. Rublon MFA ist wieder voll funktionsfähig. Wenn Sie zuvor auf eine alternative Methode gewechselt haben, können Sie jetzt wieder Ihre bevorzugte Methode verwenden. Vielen Dank für Ihre Geduld.“
- **Sachlich bleiben:** Kommunizieren Sie ruhig und hilfreich. Während Ausfällen können Benutzer nervös reagieren („Ich kann mich nicht anmelden, was nun?“). Versichern Sie, dass das IT-Team daran arbeitet, und geben Sie klare Hinweise, ob Handlungen erforderlich sind.
- **Gezielt informieren:** Wenn nur bestimmte Benutzergruppen betroffen sind (z. B. eine Abteilung), richten Sie die Nachricht gezielt an diese, um Verwirrung zu vermeiden.
- **Regelmäßig updaten:** Bei längeren Ausfällen oder geänderten Workarounds informieren Sie die Benutzer in festen Abständen. Beispiel: „Der MFA-Dienst ist um 11:30 Uhr weiterhin nicht verfügbar. Wir haben MFA vorübergehend deaktiviert, um den Zugang zu ermöglichen. Nächstes Update in 1 Stunde oder sobald neue Informationen vorliegen.“

12. Nachbearbeitung eines Vorfalls (Post-Incident Review)

Nach jedem Rublon-Ausfall oder einer teilweisen Dienstbeeinträchtigung ist es empfehlenswert, mit Ihrem IT- oder Security-Team eine kurze Nachbesprechung durchzuführen. So lässt sich feststellen, was gut funktioniert hat und was beim nächsten Mal verbessert werden sollte

Fragen zur Überprüfung:

- Hatten Benutzer wie vorgesehen Zugriff auf Systeme entsprechend den konfigurierten Fail-Mode-Einstellungen?
- Haben Administratoren die richtigen Reaktionsschritte angewendet (z. B. Umschalten auf Bypass oder Nutzung alternativer Methoden)?
- War die Kommunikation an die Benutzer klar und rechtzeitig?
- Wurden alle Sicherheitsausnahmen (z. B. temporäres Außerkraftsetzen/Bypass) korrekt protokolliert und behoben?

Basierend auf den Ergebnissen sollten Sie Ihre dokumentierten Verfahren, Kommunikationsrichtlinien und Konfigurationseinstellungen aktualisieren. Die regelmäßige Nachbearbeitung realer Vorfälle stellt sicher, dass Ihr Continuity-Plan korrekt, praktikabel und an die sich verändernden Anforderungen Ihrer Organisation angepasst bleibt.

13. Häufig gestellte Fragen (FAQ)

Nachfolgend finden Sie einige häufige Fragen im Zusammenhang mit Rublon MFA-Ausfällen und Business Continuity sowie die entsprechenden Antworten:

F1: Woran erkenne ich, dass ein Connector in den „Fail Mode“ gewechselt ist ?

A: Es gibt mehrere Anzeichen:

Wurde ein Connector auf **Fail Safe (FailMode=bypass)** gesetzt, können sich Benutzer **anmelden können, ohne zur MFA aufgefordert zu werden**, wie sie es normalerweise würden.

Wenn also plötzlich niemand mehr bei der Anmeldung nach MFA gefragt wird, ist es wahrscheinlich, dass der Connector im „Bypass“-Modus läuft – entweder aufgrund eines Ausfalls oder einer Fehlkonfiguration.
Ist hingegen **Fail Secure (FailMode=deny)** aktiv, werden Benutzer sich beschweren, dass sie sich überhaupt nicht anmelden können.

Um die Fail-Mode-Aktivierung im Backend zu bestätigen, können Sie die Konfiguration des Connectors prüfen oder die Logdatei des Connectors kontrollieren. Viele Rublon-Connectoren protokollieren dort Ereignisse, sobald der Fail Mode ausgelöst wird.

Die Rublon API selbst sendet keine direkte Benachrichtigung, wenn ein lokaler Connector in den Fail Mode wechselt, da sie dies ggf. gar nicht erkennt. Deshalb empfehlen wir, ein Monitoring-System oder SIEM einzusetzen, um die Logs Ihrer kritischen Connectoren zu überwachen. So lassen sich z. B. Warnungen konfigurieren, wenn plötzlich ein Anstieg von „Bypass“-Authentifizierungen auftritt. Proaktives Monitoring ermöglicht eine frühzeitige Erkennung von Problemen.

F2: Funktioniert Rublon MFA auch ohne Internetzugang oder wenn der Benutzer offline ist?

A: Grundsätzlich nein. Rublon MFA ist ein Cloud-Service, daher muss der Client während der Anmeldung die Rublon-Server erreichen. Ohne Internetverbindung kann der Rublon-MFA-Schritt nicht ausgeführt werden, und es greift die Fail Mode-Logik (Bypass oder Deny).

Eine Ausnahme bildet lediglich die Funktion Rublon for Windows’ Offline Mode.

14. Anhang A: Glossar wichtiger Begriffe

- **Rublon API:** Der zentrale Webservice, der Multi-Faktor-Authentifizierungsanfragen verarbeitet.
- **Rublon Prompt:** Der interaktive Bildschirm, der nach erfolgreicher Primärauthentifizierung in GUI-unterstützten Rublon-integrierten Anwendungen angezeigt wird. Er ermöglicht es Benutzern, eine verfügbare Authentifizierungsmethode auszuwählen und neue Geräte für die Multi-Faktor-Authentifizierung zu registrieren.
- **Primary Authentication (Primärauthentifizierung):** Der erste Prozess zur Überprüfung der Identität eines Benutzers, wenn er versucht, auf ein System oder eine Anwendung zuzugreifen – typischerweise durch Eingabe von Benutzername und Passwort.
- **Secondary Authentication (Sekundärauthentifizierung):** Der Prozess, bei dem nach erfolgreicher Primärauthentifizierung eine zusätzliche Überprüfung erfolgt, in der Regel über einen zweiten Faktor (z. B. TOTP-Codes, Push-Benachrichtigungen oder FIDO-Sicherheitsschlüssel), um die Identität des Benutzers zu bestätigen.
- **Second Factor (Zweiter Faktor):** Eine Verifizierungsmethode, die Teil der Multi-Faktor-Authentifizierung ist und sich von den primären Zugangsdaten (Benutzername + Passwort) unterscheidet. Dies kann etwas sein, das der Benutzer hat (z. B. ein Mobiltelefon), oder etwas, das er ist (z. B. ein Fingerabdruck).
- **Fail Mode:** Eine Einstellung, die festlegt, wie sich eine Anwendung verhält, wenn sie die Rublon API nicht erreicht. Der Fail Mode kann auf Fail Safe (Bypass, Benutzer erhält Zugriff ohne MFA) oder Fail Secure (Deny, Benutzerzugriff wird verweigert) gesetzt werden.
- **Fail Safe (Bypass):** Erlaubt einem Benutzer, der die Primärauthentifizierung bestanden hat, die Anmeldung ohne MFA, wenn die Rublon API nicht erreichbar ist.
- **Fail Secure (Deny):** Verweigert die Anmeldung vollständig, wenn MFA nicht abgeschlossen werden kann.
- **Bypass Code:** Ein einmaliger Code, den Administratoren generieren können, um einem Benutzer die Anmeldung ohne MFA zu ermöglichen (z. B. wenn der Benutzer sein Gerät für den zweiten Faktor verloren hat).
- **Service Degradation (Dienstbeeinträchtigung):** Ein teilweiser Ausfall, bei dem die Rublon API zwar weiterhin erreichbar ist, jedoch einzelne Rublon-Dienste (z. B. Admin Console, SMS-Zustellung) nicht verfügbar, langsam oder unzuverlässig sind.

Rublon sp. z o.o.
ul. Stanisława Wyspiańskiego 11
65-036 Zielona Góra

www.rublon.de