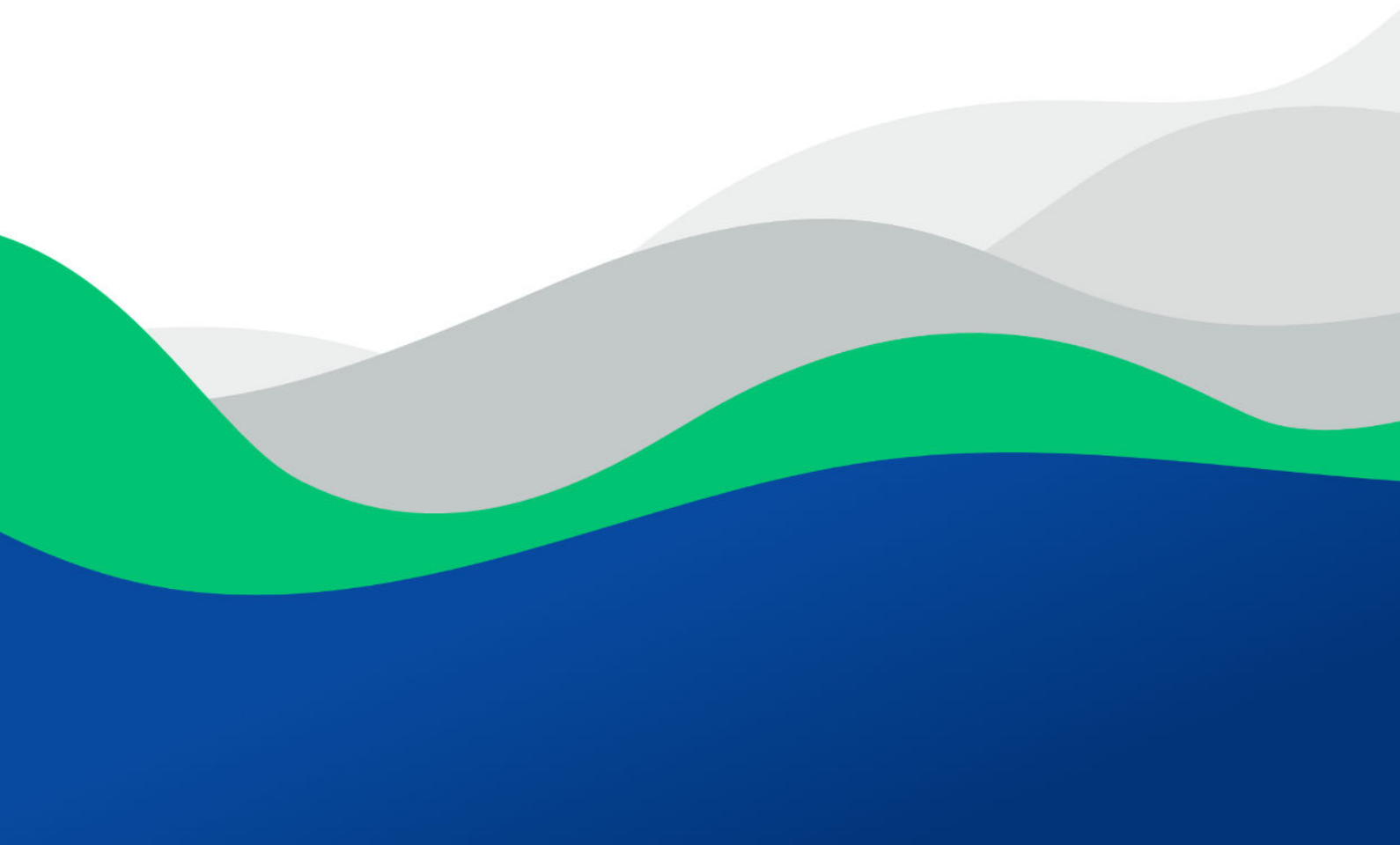




Rublon End-User Communication Templates





Inhaltsverzeichnis

1. Allgemeine Hinweise für die E-Mail-Kommunikation	3
2. Rublon MFA-Grundlagen: Glossar und häufig gestellte Fragen	5
Glossar	5
Häufig gestellte Fragen (FAQ)	6
3. Rublon MFA Rollout (Phasenbasierte E-Mail-Vorlagen)	10
E-Mail #1 – Phase I: Erste Ankündigung („Rublon MFA wird bald eingeführt“)	10
E-Mail #2 – Phase II: Erinnerung und weitere Details	12
E-Mail #3 – Phase III: Letzte Erinnerung vor der Registrierung	14
E-Mail #4 – Phase IV: Tag der Registrierung – Aktion erforderlich	16
4. Änderung der Rublon-Richtlinie – E-Mail-Vorlagen	19
E-Mail #1 – Ankündigung einer Änderung der Rublon-Richtlinie	19
E-Mail #2 – Mitteilung am Tag der Richtlinienänderung	22
5. Rublon MFA-Ausfall – E-Mail-Vorlagen	25

1. Allgemeine Hinweise für die E-Mail-Kommunikation

Wenn Sie Ihre Benutzer über die Einführung von Rublon Multi-Factor Authentication (MFA) informieren, halten Sie die Kommunikation klar, zeitgerecht und benutzerfreundlich. Hier sind einige allgemeine Empfehlungen:

- **Der Zeitpunkt zählt:** Senden Sie wichtige Mitteilungen zur MFA-Einführung in der Wochenmitte (z. B. Dienstag, Mittwoch oder Donnerstag). Diese Tage haben in der Regel höhere Öffnungsraten. Vermeiden Sie Montage (wenn Posteingänge voll sind) sowie Freitage oder Feiertage (wenn Personen möglicherweise abwesend sind).
- **Erkennbarer Absender:** Versenden Sie die E-Mails von einer Person oder einem Team, dem die Benutzer vertrauen. Verwenden Sie beispielsweise den Namen oder die E-Mail-Adresse des IT-Managers oder des Helpdesk anstelle einer generischen No-Reply-Adresse. Ein vertrauter Absender erhöht die Wahrscheinlichkeit, dass Benutzer die E-Mail öffnen und lesen.
- **Freundlicher, professioneller Ton:** Schreiben Sie in einem einladenden und klaren Stil. Vermeiden Sie schwer verständlichen Fachjargon. Erklären Sie technische Begriffe in einfacher Sprache. Lassen Sie die Benutzer wissen, dass die Änderung ihrem Schutz und dem Schutz des Unternehmens dient. Klingen Sie hilfreich und positiv.
- **Wichtige Punkte und Aktionen hervorheben:** Machen Sie es den Benutzern leicht zu erkennen, was zu tun ist. Wenn keine unmittelbare Aktion erforderlich ist, erwähnen Sie das gleich zu Beginn. Wenn eine Aktion erforderlich ist, heben Sie diese deutlich hervor (z. B. „Aktion erforderlich: Registrierung bis [DATUM]“). Verwenden Sie Fettdruck oder Überschriften für Abschnitte wie „Aktion erforderlich“, um die Aufmerksamkeit zu erhöhen.
- **Benutzer einbinden und informieren:** Nutzen Sie die Einführung als Gelegenheit, Benutzer über Sicherheit zu informieren. Fügen Sie in den ersten Mitteilungen eine kurze Erklärung wie „Was ist Rublon MFA?“ ein, damit Benutzer Zweck und Vorteile verstehen. Verlinken Sie weiterführende Ressourcen für Interessierte, halten Sie die E-Mail selbst jedoch prägnant.

- **Support-Kanäle bereitstellen:** Weisen Sie stets darauf hin, dass Unterstützung verfügbar ist. Fügen Sie in jeder Mitteilung Kontaktinformationen für Ihr IT-Helpdesk oder Support-Team hinzu. So wissen Benutzer, an wen sie sich wenden können, sollten sie Fragen haben oder während der Registrierung auf Probleme stoßen.
- **Mehrere Erinnerungen einplanen:** Verlassen Sie sich nicht auf eine einzige E-Mail. Verwenden Sie einen gestaffelten Ansatz mit mehreren Erinnerungen und Aktualisierungen. Durch die Wiederholung wichtiger Informationen durch mehrere E-Mails stellen Sie sicher, dass Benutzer, die frühere Nachrichten verpasst haben, die Informationen dennoch erhalten.

2. Rublon MFA-Grundlagen: Glossar und häufig gestellte Fragen

Wenn Sie Rublon MFA den Endbenutzern vorstellen, können häufig wiederkehrende Fragen auftreten. Nachfolgend finden Sie ein Glossar mit wichtigen Begriffen sowie eine Liste häufig gestellter Fragen, die Ihnen helfen soll, klar mit Ihren Benutzern zu kommunizieren. Sie können diese Inhalte gerne in Ihre Mitteilungen oder Schulungsunterlagen aufnehmen und bei Bedarf an die Anforderungen Ihrer Organisation anpassen.

Glossar

- **Zwei-Faktor-Authentifizierung (2FA):** Eine zusätzliche Sicherheitsebene über das Passwort hinaus. 2FA (eine Form von MFA) bedeutet, dass Sie Ihre Identität mit zwei Faktoren verifizieren: etwas, das Sie wissen (z. B. Ihr Passwort), und etwas, das Sie besitzen (z. B. Ihr Telefon), oder etwas, das Sie sind (z. B. Ihr Fingerabdruck). Auf diese Weise wird verhindert, dass sich Unbefugte anmelden können, selbst wenn Ihr Passwort bekannt ist.
- **Mehrfaktor-Authentifizierung (MFA):** Ähnlich wie 2FA, kann jedoch zwei oder drei Überprüfungsfaktoren umfassen. Rublon ist eine MFA-Lösung. In der Praxis werden „MFA“ und „2FA“ häufig austauschbar verwendet, wenn zwei Authentifizierungsfaktoren genutzt werden.
- **Rublon Authenticator:** Eine mobile Anwendung, die Sie auf Ihrem Smartphone oder Tablet installieren, um Ihre Identität bei der Anmeldung zu bestätigen. Die App kann Push-Benachrichtigungen zur Einmalbestätigung empfangen, QR-Codes scannen und Einmalpasscodes generieren.
- **Push-Benachrichtigung (Rublon Mobile Push):** Eine sichere Benachrichtigung, die an Ihr Telefon über die Rublon Authenticator App gesendet wird. Sie werden aufgefordert, eine Anmeldeanfrage zu bestätigen oder abzulehnen. Durch das Tippen auf Bestätigen (Approve) verifizieren Sie, dass Sie selbst derjenige sind, der sich anmeldet. Push-Benachrichtigungen sind schnell und bequem und ermöglichen die Anmeldung mit nur einem Fingertipp. Außerdem zeigen sie Details an, wie welche Anwendung den Login anfordert, sowie von welchem Ort, sodass verdächtige Aktivitäten leichter erkannt werden können.

- **Einmalpasscode (One-Time Passcode):** Ein einmalig gültiger Code zur Verifizierung Ihrer Identität. Einmalpasscodes werden von der Rublon Authenticator App generiert (auch wenn keine Internet- oder Mobilfunkverbindung besteht). Alternativ kann auch ein Drittanbieter-Dienst wie Google Authenticator verwendet werden, zusätzlich kann ein Hardware-Token (z. B. YubiKey OTP) für die Erzeugung des Codes verwendet werden. Diese Codes bestehen in der Regel aus sechs Ziffern, die Sie beim Login eingeben müssen. Einmalpasscodes dienen auch als Backup, wenn z. B. Push-Benachrichtigungen nicht verfügbar sind.
- **Self-Service Portal (Ansicht „Authentifikatoren verwalten“):** Eine Funktion, mit der Sie Ihre Authentifikatoren verwalten können (sofern von den IT-Administratoren aktiviert). In der Ansicht Authentifikatoren verwalten können Sie ein neues Gerät, eine Telefonnummer oder einen Sicherheitsschlüssel hinzufügen, ein altes Gerät entfernen und den Gerätenamen ändern. Dies ermöglicht es Ihnen, Ihre Authentifikatoren selbst zu verwalten, ohne den IT-Support kontaktieren zu müssen.
- **Registrierung (Enrollment):** Der Vorgang zur Einrichtung von Rublon MFA für Ihr Konto. Während der Registrierung erhalten Sie einen Link, um Ihr Gerät (z. B. Ihr Smartphone) zu registrieren. Nach Abschluss der Registrierung erfordert Ihr Konto bei jeder Anmeldung eine zusätzliche MFA-Verifikation.
- **Rublon Prompt:** Die Rublon-Anmeldeoberfläche, die erscheint, wenn Sie auf eine geschützte Anwendung zugreifen (sofern von der jeweiligen Anwendung unterstützt). Nachdem Sie Benutzername und Passwort eingegeben haben, fordert Sie die Rublon Prompt-Oberfläche auf, Ihren zweiten Faktor zu verwenden (z. B. Push-Benachrichtigung bestätigen oder einen Passcode eingeben). Wenn die Selbstregistrierung aktiv ist, wird in der Eingabeaufforderung die Option Authentifikatoren verwalten angezeigt.

Häufig gestellte Fragen (FAQ)

F1: Benötige ich ein Smartphone, um Rublon MFA zu verwenden?

A: Nein, ein Smartphone ist nicht zwingend erforderlich, jedoch ist es die empfohlene und einfachste Methode zur Authentifizierung. Die Rublon Authenticator App macht den MFA-Prozess schnell (über Push-Benachrichtigungen). Sollten Sie jedoch kein Smartphone besitzen oder keines verwenden möchten, können Sie ein herkömmliches Mobiltelefon oder ein Festnetztelefon nutzen. In diesem Fall können Sie sich über einen SMS-Code oder einen

Telefonanruf authentifizieren. Das IT-Team Ihrer Organisation hat die Möglichkeit verschiedene Methoden zu aktivieren und festzulegen, welche für Sie verfügbar sind.

F2: Was ist die Rublon Authenticator Mobile App?

A: Der Rublon Authenticator ist eine kostenlose mobile App, die Sie auf Ihrem Smartphone (iOS, Android, HarmonyOS) installieren. Sie wird verwendet, um den zweiten Authentifizierungsfaktor bereitzustellen. Die App kann Push-Benachrichtigungen zur Bestätigung von Anmeldeversuchen empfangen, Einmalpasscodes generieren und QR-Codes scannen, die während der Anmeldung angezeigt werden. Die Rublon Authenticator App verwandelt Ihr Smartphone damit in einen sicheren Schlüssel für die Anmeldung. Die App funktioniert ausschließlich mit Rublon MFA. Sie gibt Ihre Daten nicht weiter, sie dient nur zur Bestätigung Ihrer Identität („Ja, ich bin es, der sich anmeldet“).

F3: Welche Authentifizierungsmethode wird empfohlen?

A: Wenn Sie ein Smartphone besitzen, wird die Verwendung von Mobile Push über die Rublon Authenticator App empfohlen. Das Bestätigen einer Push-Benachrichtigung in der App ist schnell, einfach und sicher. Ein Fingertipp genügt, was deutlich schneller ist als das Eingeben eines Codes. Wenn Sie kein Smartphone verwenden, können Sie sich alternativ über einen SMS-Code oder einen Telefonanruf authentifizieren. Push-Benachrichtigungen bieten jedoch die bequemste Nutzung für die meisten Benutzer. Die sicherste Methode ist die Verwendung von FIDO-Sicherheitsschlüsseln, die allerdings ein physisches Gerät erfordern.

F4: Ich erhalte keine Push-Benachrichtigungen mehr auf meinem Telefon. Was soll ich tun?

A: Wenn Push-Benachrichtigungen nicht mehr ankommen, überprüfen Sie bitte Folgendes:

1. **Internetverbindung:** Stellen Sie sicher, dass Ihr Telefon über eine aktive Internetverbindung verfügt (mobile Daten oder WLAN). Push-Benachrichtigungen erfordern eine Internetverbindung, um Ihr Gerät zu erreichen.
2. **Benachrichtigungseinstellungen:** Überprüfen Sie die Benachrichtigungseinstellungen Ihres Telefons. Stellen Sie sicher, dass Benachrichtigungen für die Rublon Authenticator App aktiviert sind.
3. **Zum Aktualisieren nach unten ziehen:** Öffnen Sie die Rublon Authenticator App und ziehen Sie den Bildschirm nach unten, um manuell ausstehenden Authentifizierungsanfragen zu laden.

4. **Alternative Methode:** Sollte keine der oben genannten Lösungen funktionieren, können Sie sich weiterhin mit einem Einmalpasscode authentifizieren. Öffnen Sie dazu die Rublon Authenticator App und verwenden Sie den sechsstelligen Code für den Login oder eine andere vom IT-Team bereitgestellte Backup-Methode. Wenden Sie sich anschließend an den IT-Support, um das Problem mit den Push-Benachrichtigungen zu beheben.

F5: Wie kann ich mich anmelden, wenn ich kein Mobilfunksignal oder WLAN habe?

A: Verwenden Sie den Einmalpasscode in der Rublon Authenticator App. Diese Funktion funktioniert auch offline. Öffnen Sie einfach die App, um den sechsstelligen Code anzuzeigen, und geben Sie diesen während der Anmeldung ein. Weitere Informationen finden Sie im Artikel: [Funktioniert Rublon MFA auch ohne Internetzugang?](#)

F6: Wie kann ich neue Geräte für Rublon MFA registrieren oder verwalten?

A: Wenn das IT-Team die Self-Service-Funktion aktiviert hat, können Sie Ihre Authentifikatoren selbst verwalten. Normalerweise sehen Sie nach der Eingabe Ihres Passworts in der Rublon Prompt-Oberfläche die Option „Authentifikatoren verwalten“. Nach der Bestätigung mit einem vorhandenen Authentifikator können Sie Folgendes tun:

- **Neues Gerät hinzufügen:** Zum Beispiel eine Drittanbieter-App wie Google Authenticator oder einen FIDO-Sicherheitsschlüssel registrieren.
- **Standardgerät festlegen:** Wenn Sie mehrere Geräte registriert haben, können Sie eines als Standard festlegen.
- **Gerät reaktivieren oder ersetzen:** Wenn Sie ein neues Smartphone besitzen, müssen Sie es registrieren und das alte Gerät entfernen, da es nicht mehr verwendet werden kann.
- **Gerät umbenennen oder entfernen:** Sie können Geräte benennen (z. B. „Diensttelefon“ oder „Privates Telefon“) und nicht mehr benötigte Geräte löschen.

Detaillierte Anleitungen mit Screenshots finden Sie im [Rublon User Guide - Authentifikatoren verwalten](#).

Sollte diese Funktion nicht aktiv sein, kontaktieren Sie den IT-Support, um Geräte hinzuzufügen oder zu ändern. Das IT-Team kann Ihnen einen neuen Registrierungslink zusenden oder beim Gerätemanagement unterstützen.

F7: Was soll ich tun, wenn ich mein Telefon verliere oder es gestohlen wurde?

A: Informieren Sie den IT-Support sofort, wenn Ihr primärer Authentifikator (z. B. Ihr Smartphone mit der Rublon Authenticator App) verloren gegangen oder gestohlen wurde. Das IT-Team hilft Ihnen dabei, Ihr Konto zu sichern und den Zugriff zu sperren. Je früher Sie den Verlust melden, desto schneller kann Ihr Konto vor unbefugtem Zugriff geschützt werden.

F8: Können Rublon oder das IT-Team mein Passwort sehen?

A: Nein, Ihr Passwort bleibt privat. Rublon erhält oder speichert Ihr Passwort nicht. Rublon wird erst aktiv, nachdem Sie das korrekte Passwort eingegeben haben, um den zweiten Authentifizierungsfaktor aufzufordern. Rublon bestätigt lediglich, dass Sie ein vertrauenswürdiges Gerät haben oder eine vertrauenswürdige Person sind. Das Passwort selbst wird zu keinem Zeitpunkt von Rublon eingesehen.

F9: Ändert die Rublon Authenticator App irgendwelche Einstellungen auf meinem Telefon?

A: Nein, die Rublon Authenticator App kann keinen Zugriff auf Einstellungen oder Daten Ihres Telefons. Nach der Installation fordert die App bestimmte Berechtigungen an (z. B. das Empfangen von Push-Benachrichtigungen), sie kann grundlegende Geräteinformationen abfragen (z. B. Betriebssystemversion oder Bildschirm-Sperrstatus), um Sicherheitsanforderungen zu erfüllen. Rublon kann jedoch keine Aktionen auf Ihrem Gerät ausführen. Die App kann Sie lediglich dazu auffordern, eine Anmeldung zu bestätigen. Sie behalten stets die volle Kontrolle über Ihr Gerät.

3. Rublon MFA Rollout (Phasenbasierte E-Mail-Vorlagen)

Bei der Einführung von Rublon MFA ist es wichtig, Ihre Endbenutzer frühzeitig und mit klaren Anweisungen vorzubereiten. Die folgenden E-Mail-Vorlagen sollen Benutzer durch die Einführung von Rublon führen.

Jede Vorlage enthält einen empfohlenen Zeitplan für den Versand, eine Beispielbetreffzeile und den E-Mail-Text. **Bitte ersetzen Sie Platzhalter wie [DATUM]** und passen Sie Details bei Bedarf an. Der Ton dieser E-Mails sollte klar, freundlich und unterstützend sein.

E-Mail #1 – Phase I: Erste Ankündigung („Rublon MFA wird bald eingeführt“)

Timeline: Versenden Sie diese E-Mail etwa **30 Tage vor dem Start** der Registrierung oder dem Go-Live-Datum.

Betreff: Rublon MFA wird bald eingeführt.

Text:

Hallo zusammen,

im Rahmen unserer laufenden Maßnahmen zur Verbesserung der IT-Sicherheit führen wir in Kürze Rublon Multi-Faktor-Authentifizierung (MFA) in unseren Anmeldeprozess ein.

Was ist Multi-Faktor-Authentifizierung (MFA)?

Die Multi-Faktor-Authentifizierung ist ein Sicherheitsverfahren, bei dem Sie Ihre Identität mit mindestens zwei Nachweisen bestätigen. Diese Faktoren sind in der Regel (1) Ihr Passwort und (2) etwas Zusätzliches – in unserem Fall Ihr Telefon. Das bedeutet, dass Sie zusätzlich zu Benutzername und Passwort einen weiteren Schritt ausführen, zum Beispiel das Bestätigen einer Benachrichtigung auf Ihrem Telefon, während Sie sich bei einer Anwendung anmelden.

Warum führen wir MFA ein?

Passwörter allein reichen nicht mehr aus, um Konten sicher zu halten. Durch einen zweiten Faktor, der nur Ihnen zur Verfügung steht, erhöhen wir die Sicherheit unserer Systeme deutlich.

Selbst wenn Ihr Passwort bekannt sein sollte, kann ohne den zweiten Schritt der Authentifizierung nicht auf Ihr Konto zugegriffen werden.

Was ist Rublon MFA?

Rublon MFA ist eine Plattform der Multi-Faktor-Authentifizierung, die den MFA-Prozess für uns verwaltet. Sie basiert auf einer Cloud-Lösung, der Organisationen weltweit vertrauen, um ihre Anmeldungen zu schützen. Rublon ergänzt die Anmeldung um einen zusätzlichen Schritt und stellt sicher, dass nur Sie selbst auf Ihr Konto zugreifen können.

Erforderliche Aktion:

Derzeit ist keine Aktion erforderlich. Diese E-Mail dient als Vorabinformation zur bevorstehenden Einführung von Rublon MFA.

In den nächsten Wochen erhalten Sie weitere Informationen dazu, wie Sie sich für Rublon MFA registrieren, welche Schritte notwendig sind und wann die Umstellung erfolgt. Diese Nachricht soll Sie lediglich darüber informieren, was geplant ist und warum.

Zusammenfassung:

Rublon MFA wird in etwa einem Monat eingeführt und erhöht die Sicherheit unserer Anmeldungen. In Kürze erhalten Sie Anleitungen, welche für die Einrichtung benötigt werden. Vielen Dank für Ihre Aufmerksamkeit.

Bitte achten Sie auf weitere E-Mails zu diesem Thema. Sollten Sie bereits Fragen haben, wenden Sie sich an unseren IT-Helpdesk.

Mit freundlichen Grüßen
Ihr IT-Sicherheitsteam

E-Mail #2 – Phase II: Erinnerung und weitere Details

Zeitplan: Versenden Sie diese E-Mail etwa **15 Tage vor dem Start** der Registrierung oder dem Go-Live-Datum.

Betreff: Erinnerung: Registrierung für Rublon MFA beginnt am **[DATUM]**

Text:

Hallo zusammen,

dies ist eine Erinnerung daran, dass wir in etwa zwei Wochen (am **[DATUM]**) mit der Registrierung aller Benutzer für Rublon Multi-Faktor-Authentifizierung (MFA) beginnen werden. Rublon wird künftig ein verpflichtender Bestandteil des Anmeldeprozesses sein, um die Sicherheit unserer Systeme zu erhöhen.

Was passiert am [DATUM]?

An diesem Tag erhalten Sie eine offizielle **Registrierungs-E-Mail** von Rublon. Die E-Mail enthält einen persönlichen Link, über den Sie Rublon MFA auf Ihrem Gerät einrichten können. Die Einrichtung ist einfach und dauert nur etwa zwei bis drei Minuten. Sie installieren die Rublon Authenticator App auf Ihrem Smartphone und verknüpfen sie mit Ihrem Konto. Sie erhalten dazu eine detaillierte Anleitung.

Warum Rublon MFA und warum jetzt?

Wie bereits erwähnt, verbessert die Einführung von MFA mit Rublon unsere Sicherheitsmaßnahmen erheblich. Cyberangriffe beginnen häufig mit einem gestohlenen Passwort. Rublon hilft, solche Vorfälle zu verhindern, indem ein zweiter Nachweis Ihrer Identität erforderlich wird. Wir haben Rublon gewählt, da es benutzerfreundlich ist (Anmeldung mit nur einem Fingertipp auf Ihrem Smartphone) und gleichzeitig höchste Sicherheit bietet.

Erforderliche Aktion:

Derzeit müssen Sie noch nichts unternehmen. Diese E-Mail dient zur Information, dass die Registrierung für Rublon MFA am **[DATUM]** beginnt. Wir möchten sicherstellen, dass alle Mitarbeitenden rechtzeitig informiert und vorbereitet sind.

Was passiert als Nächstes?

- Am **[DATUM]**: Achten Sie auf eine E-Mail von Rublon mit dem Betreff "Enroll your authenticator". Diese E-Mail enthält Ihren persönlichen Registrierungslink.
- **Registrierungsvorgang**: Die Registrierungs-E-Mail führt Sie durch die Installation der Rublon Authenticator App auf Ihrem mobilen Gerät. Der Vorgang ist unkompliziert, zusätzlich stellen wir eine Schritt-für-Schritt-Anleitung bereit.

Wir senden kurz vor dem Start noch eine weitere Erinnerung. Markieren Sie sich den **[DATUM]** in Ihrem Kalender, um die Registrierung an diesem Tag abzuschließen.

Sollten Sie Fragen haben oder Unterstützung benötigen, wenden Sie sich bitte an unseren IT-Support unter **[Kontaktdaten des Helpdesk]**.

Mit freundlichen Grüßen
Ihr IT-Sicherheitsteam

E-Mail #3 – Phase III: Letzte Erinnerung vor der Registrierung

Zeitplan: Versenden Sie diese E-Mail etwa **drei Tage vor dem Start** der Registrierung oder dem Go-Live-Datum.

Betreff: Letzte Erinnerung: Rublon MFA startet am **[DATUM]**

Text:

Hallo zusammen,

in wenigen Tagen führen wir Rublon Multi-Faktor-Authentifizierung (MFA) ein. Diese E-Mail ist die letzte Erinnerung und enthält wichtige Informationen.

Was passiert am [DATUM]?

- Am **[DATUM]**: Achten Sie auf eine E-Mail von Rublon mit dem Betreff „Enroll your authenticator“. Diese Nachricht enthält Ihren persönlichen Registrierungslink.
- **Registrierungsvorgang:** Die E-Mail führt Sie Schritt für Schritt durch die Installation der Rublon Authenticator App auf Ihrem mobilen Gerät. Der Prozess ist unkompliziert, eine detaillierte Anleitung wird bereitgestellt.
- Sollten Sie kein Smartphone besitzen, können Sie alternativ eine andere Authentifizierungsmethode verwenden. Während der Registrierung können Sie eine normale Mobil- oder Festnetznummer angeben, um Ihre Identität per SMS oder Telefonanruf zu bestätigen. Rublon unterstützt mehrere Authentifizierungsmethoden, die Rublon Authenticator App ist keine zwingende Voraussetzung.

Erforderliche Aktion:

Am heutigen Tag ist noch keine Aktion erforderlich. Am **[DATUM]** müssen Sie jedoch Ihre Registrierung für Rublon MFA abschließen. Planen Sie bitte ein paar Minuten Zeit ein, um die Einrichtung an diesem Tag durchzuführen.

Welche Vorteile bietet Rublon MFA?

- **Komfort:** Durch die Verwendung des Smartphones können Sie Anmeldeversuche mit einem Fingertipp mittels einer Push-Benachrichtigung bestätigen.

- **Sicherheit:** Durch die Zwei-Faktor-Authentifizierung mit Rublon bleibt Ihr Konto geschützt, auch wenn Ihr Passwort kompromittiert wird. Dies verringert das Risiko unbefugter Zugriffe erheblich.

Wie ändert sich die Anmeldung mit Rublon MFA?

Ab dem **[DATUM]** melden Sie sich bei geschützten Anwendungen wie folgt an:

1. Geben Sie wie gewohnt Ihren Benutzernamen und Ihr Passwort ein.
2. Anschließend werden Sie von Rublon MFA zur Durchführung eines zweiten Authentifizierungsschritts aufgefordert. Auf Ihrem Smartphone erscheint eine Push-Benachrichtigung, die Sie bestätigen, alternativ werden Sie aufgefordert, einen Einmalpasscode aus Ihrer App einzugeben.
3. Nach der Bestätigung oder Eingabe des Codes erfolgt der Zugriff wie gewohnt.

Ihr Passwort bleibt unverändert. Rublon fügt lediglich einen zusätzlichen Schritt in den Anmeldeprozess hinzu, um die Anmeldung sicherer zu gestalten.

Fragen oder Unterstützung benötigt?

Unser Team steht Ihnen zur Verfügung. Sollten Sie Fragen haben oder während der Registrierung Unterstützung benötigen, wenden Sie sich bitte an unseren Helpdesk:

- Helpdesk-Telefon: 123-456-7890
- Helpdesk-E-Mail: support@yourcompany.com

Vielen Dank für Ihre Unterstützung bei dieser wichtigen Sicherheitsmaßnahme.

Mit freundlichen Grüßen
Ihr IT-Sicherheitsteam

E-Mail #4 – Phase IV: Tag der Registrierung – Aktion erforderlich

Zeitplan: Versenden Sie diese E-Mail **am Tag des Beginns der Rublon-MFA-Registrierung** (Go-Live-Tag), idealerweise am Morgen, kurz bevor oder während die Registrierungs-E-Mails versendet werden.

Betreff: Aktion erforderlich: Heute für Rublon MFA registrieren

Text:

Hallo zusammen,

heute ist es so weit! Wir haben offiziell mit der Einführung von Rublon MFA begonnen. Sie sollten in Ihrem Posteingang die Registrierungs-E-Mail von Rublon mit dem Betreff „Enroll your authenticator“ erhalten haben. Bitte öffnen Sie diese E-Mail und folgen Sie den Anweisungen, um die Registrierung abzuschließen.

Was müssen Sie jetzt tun?

1. Suchen Sie die Registrierungs-E-Mail mit dem Betreff „Enroll your authenticator“, die Ihnen zugesendet wurde.
2. Öffnen Sie die E-Mail und klicken Sie auf „Enroll Your Authenticator“. Sie werden anschließend zur Einrichtungsseite von Rublon weitergeleitet.
3. Richten Sie Ihr Gerät ein. Die Seite führt Sie Schritt für Schritt durch den Registrierungsprozess. Detaillierte Anweisungen finden Sie in der Anleitung: [How to enroll a mobile device with Rublon Authenticator?](#). Wenn Sie einen alternativen Authentifikator registrieren möchten, lesen Sie die Anleitung: [Rublon User Guide - Enrollment](#).
4. Nach Abschluss der Einrichtung ist Rublon MFA für Ihr Konto aktiv. Ab diesem Zeitpunkt ist bei jeder Anmeldung zu geschützten Systemen ein zusätzlicher MFA-Schritt erforderlich.

Wenn Sie keine Registrierungs-E-Mail erhalten haben:

Überprüfen Sie Ihren Spam-Ordner. Sollte die E-Mail dort nicht zu finden sein, wenden Sie sich an den IT-Support. Die Registrierungs-E-Mail ist personalisiert, verwenden Sie daher keine E-Mail eines anderen Benutzers.

Wenn Sie kein Smartphone besitzen:

Während des Registrierungsprozesses können Sie eine alternative Methode wählen, zum Beispiel Ihre Telefonnummer für eine Anrufverifizierung. Folgen Sie den Anweisungen auf dem Bildschirm, lesen Sie bei Bedarf die Anleitung [Rublon User Guide - Registrierung](#) oder wenden Sie sich an den IT-Support, wenn Sie Unterstützung bei der Einrichtung ohne Smartphone benötigen.

Frist:

Bitte schließen Sie die Registrierung für Rublon MFA bis spätestens **[DATUM]** ab. Nach diesem Datum ist der Zugriff auf Anwendungen nur noch mit aktivierter Rublon MFA möglich. Ohne abgeschlossene Registrierung können Sie sich nicht mehr anmelden. Es gibt eine kurze Übergangsfrist von wenigen Tagen, wir bitten Sie jedoch, die Registrierung so bald wie möglich durchzuführen.

Warum ist das wichtig?

Die Registrierung in Rublon MFA schützt sowohl Ihr Benutzerkonto als auch die Daten unseres Unternehmens. Die Einrichtung dauert nur wenige Minuten und erhöht die Sicherheit erheblich. Nach **[DATUM]** ist der Zugriff nur noch für registrierte Benutzer möglich. Bitte führen Sie die Registrierung daher rechtzeitig durch, **um Unterbrechungen bei der Arbeit zu vermeiden.**

Benötigen Sie Unterstützung?

Wenn Sie während der Registrierung auf Probleme stoßen oder Fragen haben, wenden Sie sich bitte an unseren Helpdesk. Unser Support-Team steht heute bereit, um Sie bei der Einrichtung von Rublon MFA zu unterstützen.

- Helpdesk-Telefon: 123-456-7890
- Helpdesk-E-Mail: support@yourcompany.com

Vielen Dank für Ihre Unterstützung bei der Verbesserung unserer IT-Sicherheit. Mit Ihrer Teilnahme tragen Sie aktiv dazu bei, die Daten unseres Unternehmens und Ihre eigenen Konten zu schützen.

Mit freundlichen Grüßen,
Ihr IT-Sicherheitsteam

4. Änderung der Rublon-Richtlinie – E-Mail-Vorlagen

Zusätzlich zu den ersten Informations-E-Mails zur Einführung kann es erforderlich sein, Ihre Benutzer später über Änderungen an den Rublon-Richtlinien oder an bestimmten Connectoreinstellungen zu informieren. Ersetzen Sie dabei Platzhalter wie [DATUM] und passen Sie Details bei Bedarf an. Sie können auch Teile dieser Nachricht entfernen, wenn nur bestimmte Richtlinien (z. B. die Remembered Devices Policy) geändert wurden. Der Ton dieser Mitteilungen sollte stets klar, hilfreich und unterstützend sein.

E-Mail #1 – Ankündigung einer Änderung der Rublon-Richtlinie

Zeitplan: Senden Sie die E-Mail etwa **7 Tage**, bevor die neuen Rublon-Richtlinien in Kraft treten.

Betreff: Wichtige Mitteilung: Bevorstehende Änderungen an den Rublon-Sicherheitsrichtlinien

Text:

Hallo zusammen,

im Rahmen unserer laufenden Bemühungen zur Gewährleistung höchster Sicherheitsstandards werden wir unsere Rublon Multi-Faktor-Authentifizierungsrichtlinien am [DATUM] aktualisieren. Bitte lesen Sie die folgenden Informationen:

Wer ist betroffen?

Diese Änderungen betreffen die Art und Weise, wie die Multi-Faktor-Authentifizierung (MFA) durchgeführt wird. Sie gelten **[global/für bestimmte Anwendungen oder Benutzergruppen]**.

Was ändert sich?

1. Richtlinie für vertrauenswürdige Geräte (Remembered Devices Policy):

- **Was ist das?** Diese Richtlinie legt fest, ob und wie lange ein Gerät als vertrauenswürdig gespeichert werden kann, um die Häufigkeit von MFA-Abfragen zu reduzieren.
- **Änderungsdetails:**

- Der Zeitraum, in dem Ihr Gerät als vertrauenswürdig gespeichert bleibt, wird **[verlängert/verkürzt]** auf **[Wert in Stunden/Tagen]**.
- Die Richtlinie für vertrauenswürdige Geräte wird **[aktiviert/deaktiviert]**.

- **Was bedeutet das für Sie?**

- Nach der Anpassung der Richtlinie, bleiben Ihre Geräte für einen **[längeren/kürzeren]** Zeitraum als vertrauenswürdig gespeichert.
- Wenn die Richtlinie aktiviert ist, werden Sie seltener zur MFA aufgefordert, nachdem Sie ein Gerät als vertrauenswürdig markiert haben.
- Wenn die Richtlinie deaktiviert ist, werden Sie bei jeder Anmeldung zur MFA aufgefordert.

2. Richtlinie für Authentifizierungsmethoden (Authentication Methods Policy):

- **Was ist das?** Diese Richtlinie legt fest, welche Authentifizierungsmethoden für die Multi-Faktor-Authentifizierung zur Verfügung stehen, einschließlich der standardmäßig verwendeten Methode beim Anmelden.

- **Änderungsdetails:**

- Die Authentifizierungsmethode **[Name der Methode]** wird **[aktiviert/deaktiviert]**.
- Die Standard-Authentifizierungsmethode wird auf **[Name der Authentifizierungsmethode]** festgelegt.

- **Was bedeutet das für Sie?**

- Wenn eine von Ihnen verwendete Methode deaktiviert wird, wechseln Sie bitte rechtzeitig zu einer alternativen Methode, um Unterbrechungen zu vermeiden. Eine Anleitung finden Sie hier: [Anleitung zur Registrierung einer alternativen MFA-Methode](#).
- Wenn eine Methode als Standard festgelegt wird, werden Sie automatisch mit dieser Methode authentifiziert, ohne diese im [Rublon Prompt](#) auswählen zu müssen. Wenn Sie eine andere Methode bevorzugen oder zusätzliche

Authentifikatoren hinzufügen möchten, wählen Sie im Rublon Prompt „Zurück“ und dann „Authentifikatoren verwalten“.

3. Richtlinie für autorisierte Netzwerke (Authorized Networks Policy)

- **Was ist das?** Diese Richtlinie definiert bestimmte IP-Bereiche, die als sicher gelten. Bei einer Anmeldung aus diesen Netzwerken entfällt die Multi-Faktor-Authentifizierung, da der Zugriff als vertrauenswürdig eingestuft wird.
- **Änderungsdetails:**
 - Benutzer, die sich aus autorisierten Netzwerken anmelden, werden ohne Multi-Faktor-Authentifizierung angemeldet.
 - Wird die Richtlinie für autorisierte Netzwerke deaktiviert, ist bei allen Anmeldungen eine Multi-Faktor-Authentifizierung erforderlich, unabhängig vom Netzwerkstandort.
- **Was bedeutet das für Sie?**
 - Wenn Sie sich über eine autorisierte IP-Adresse anmelden, erfolgt eine vereinfachte Authentifizierung ohne MFA. Wenn Sie sich jedoch außerhalb autorisierter IP-Bereiche anmelden oder die Richtlinie deaktiviert wurde, ist MFA bei jeder Anmeldung erforderlich.

Wenn Sie Fragen haben oder Unterstützung benötigen, wenden Sie sich bitte an unseren IT-Helpdesk unter **[Help Desk Contact Info]**.

Vielen Dank für Ihre Aufmerksamkeit und Ihre Mithilfe bei der Umsetzung dieser Sicherheitsaktualisierung.

Mit freundlichen Grüßen
Ihr IT-Sicherheitsteam

E-Mail #2 – Mitteilung am Tag der Richtlinienänderung

Zeitplan: Senden Sie diese E-Mail am Tag, an dem die Änderungen der Rublon-Richtlinien in Kraft treten.

Betreff: Rublon-Sicherheitsrichtlinien aktualisiert – das hat sich geändert

Text:

Hallo zusammen,

ab heute wurden unsere Rublon Multi-Faktor-Authentifizierungsrichtlinien aktualisiert. Diese Änderungen sind ab sofort wirksam und können Auswirkungen auf den Anmeldeprozess haben.

Wer ist betroffen?

Diese Richtlinienänderungen gelten **[global/für bestimmte Anwendungen oder Benutzergruppen]**. Wenn Sie zu einer betroffenen Gruppe gehören, kann sich Ihr Anmeldevorgang ab heute leicht ändern.

Was hat sich geändert?

1. Richtlinie für vertrauenswürdige Geräte (Remembered Devices Policy)

- **Was ist neu?**

- Die Funktion für vertrauenswürdige Geräte wurde **[aktiviert/deaktiviert]**.
- Der Zeitraum, in dem ein Gerät als vertrauenswürdig gilt, wurde auf **[Wert in Stunden/Tagen]** festgelegt.

- **Was bedeutet das für Sie?**

- Nach der Änderung der Richtlinie behalten Geräte ihren vertrauenswürdigen Status für einen **[längeren/kürzeren]** Zeitraum.
- Wenn die Richtlinie aktiviert ist, behalten als [vertrauenswürdig markierte Geräte](#) ihren Status für einen definierten Zeitraum, wodurch die Häufigkeit von MFA-Abfragen reduziert wird.

- Bei deaktivierter Richtlinie ist für jede Anmeldung eine erneute Multi-Faktor-Authentifizierung erforderlich.

2. Richtlinie für Authentifizierungsmethoden (Authentication Methods Policy):

- Was ist neu?

- Die Authentifizierungsmethode **[Name der Methode]** wurde **[aktiviert/deaktiviert]**.
- Die Standard-Authentifizierungsmethode wurde auf **[Name der Methode]** gesetzt.

- Was bedeutet das für Sie?

- Wenn Sie bisher eine Methode verwendet haben, die deaktiviert wurde, wechseln Sie bitte zu einer alternativen verfügbaren Methode. Eine Anleitung finden Sie hier: [So registrieren Sie eine alternative MFA-Methode](#).
- Wenn die Standard-Authentifizierungsmethode aktiviert ist, werden Sie automatisch aufgefordert, sich mit der Methode **[Name der Authentifizierungsmethode]** zu verifizieren. Möchten Sie eine andere Methode verwenden oder ein neues Gerät registrieren, klicken Sie im Rublon Prompt auf „Zurück“ und wählen Sie anschließend „Authentifikatoren verwalten“.

3. Richtlinie für autorisierte Netzwerke (Authorized Networks Policy)

- Was ist neu?

- Für Benutzer, die sich aus bestimmten autorisierten IP-Adressen anmelden, wird MFA künftig übersprungen.

- Was bedeutet das für Sie?

- Wenn Sie sich über eine autorisierte IP-Adresse anmelden, entfällt der zweite Authentifizierungsschritt.
- Wenn die Richtlinie deaktiviert ist, wird MFA künftig bei jeder Anmeldung erforderlich sein – unabhängig von der IP-Adresse.

Benötigen Sie Unterstützung?

Wenn Sie Fragen zu diesen Änderungen haben, Hilfe beim Wechsel Ihrer Authentifizierungsmethode oder beim Verwalten Ihrer Authentifikatoren benötigen, wenden Sie sich bitte an unseren IT-Helpdesk:

- **Telefon:** 123-456-7890
- **E-Mail:** support@yourcompany.com

Vielen Dank für Ihre Aufmerksamkeit und Ihre Zusammenarbeit, während wir unsere Sicherheitsrichtlinien weiter verbessern.

Mit freundlichen Grüßen
Ihr IT-Sicherheitsteam

5. Rublon MFA-Ausfall – E-Mail-Vorlagen

Für E-Mail-Vorlagen im Zusammenhang mit Ausfällen oder Dienstunterbrechungen von Rublon MFA verweisen wir auf den [Rublon-Leitfaden zur Geschäftskontinuität](#).



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

www.rublon.pl

© 2025 Rublon sp. z o.o.



www.rublon.pl