



Szablony komunikacji z użytkownikami końcowymi Rublon

Wersja 1.0

Spis treści

1. Ogólne porady dotyczące komunikacji e-mailowej	1
2. Podstawy Rublon MFA: Słownik i często zadawane pytania	2
Słownik	2
Często zadawane pytania	3
3. Wdrożenie Rublon MFA – Szablony wiadomości e-mail dla poszczególnych etapów	6
E-mail nr 1 – Etap I: Wstępne ogłoszenie („Rublon MFA już wkrótce”)	6
E-mail nr 2 – Etap II: Przypomnienie i więcej szczegółów	7
E-mail nr 3 – Etap III: Ostatnie przypomnienie o rejestracji	9
E-mail nr 4 – Etap IV: Dzień rejestracji – Wymagane działanie	10
4. Zmiana polityki Rublon – Szablony e-maili	13
E-mail nr 1 – Powiadomienie o nadchodzącej zmianie polityki Rublon	13
E-mail nr 2 – Ogłoszenie o zmianie polityki w dniu wprowadzenia zmiany	15
5. Awaria Rublon MFA – Szablony e-maili	18

1. Ogólne porady dotyczące komunikacji e-mailowej

Informując użytkowników o wdrożeniu Rublon Multi-Factor Authentication (MFA), zadbaj o to, aby komunikacja była jasna, terminowa i przyjazna dla użytkownika. Oto kilka ogólnych porad:

- **Czas ma znaczenie:** Wysyłaj ważne e-maile dotyczące wdrożenia MFA w środku tygodnia (np. we wtorek, środę lub czwartek). W te dni wskaźniki otwarć e-maili są zazwyczaj wyższe. Unikaj poniedziałków (kiedy skrzynki odbiorcze są pełne) i piątków lub świąt (kiedy ludzie mogą być poza domem).
- **Rozpoznawalny nadawca:** Wysyłaj wiadomości e-mail od osoby lub zespołu, któremu użytkownicy ufają. Na przykład użyj imienia/e-maila kierownika IT lub działu pomocy technicznej zamiast ogólnego adresu no-reply. Znajomy nadawca zwiększa prawdopodobieństwo, że użytkownicy otworzą i przeczytają wiadomość.
- **Przyjazny, profesjonalny ton:** Pisz w przyjaznym i zrozumiałym tonie. Unikaj ciężkiego żargonu. Wyjaśniaj terminy techniczne prostym językiem. Daj użytkownikom znać, że zmiana ma na celu pomóc chronić ich oraz firmę. Brzmij pomocnie i przyjaźnie, nie wzbudzaj zaniepokojenia.
- **Podkreśl kluczowe punkty i działania:** Ułatw użytkownikom zrozumienie, co mają zrobić. Jeśli nie jest potrzebne natychmiastowe działanie, powiedz o tym z góry. Jeśli działanie jest wymagane, wyraźnie to zaznacz (np. „*Wymagane działanie: Zarejestruj się do [DATA]*”). Użyj pogrubionego tekstu lub nagłówków w sekcjach takich jak „Wymagane działanie” lub pytaniach w wiadomości e-mail, aby przyciągnąć uwagę.
- **Angażuj i edukuj:** Wykorzystaj wdrożenie jako okazję do edukacji użytkowników na temat bezpieczeństwa. Dołącz krótką informację „*Czym jest Rublon MFA?*” we wczesnej komunikacji, aby użytkownicy rozumieli cel i korzyści. Dołącz link dla tych, którzy chcą dowiedzieć się więcej, ale upewnij się, że sam e-mail jest zwięzły.
- **Zapewnij kanały wsparcia:** Zawsze zapewnij użytkowników, że dostępna jest pomoc. W każdej komunikacji z użytkownikami zawsze dołączaj dane kontaktowe do swojego biura pomocy technicznej lub zespołu wsparcia IT. W ten sposób użytkownicy wiedzą, gdzie się udać, jeśli mają pytania lub napotkają problemy podczas rejestracji.
- **Zaplanuj wiele przypomnień:** Nie polegaj na jednym e-mailu. Użyj podejścia etapowego, wysyłając przypomnienia i aktualizacje. Powtórzenie kluczowych informacji w kilku e-mailach gwarantuje, że użytkownicy, którzy przegapili wcześniejsze wiadomości, znajdą te same informacje w późniejszych.

2. Podstawy Rublon MFA: Słownik i często zadawane pytania

Podczas wprowadzania platformy Rublon MFA dla użytkowników końcowych możesz natknąć się na kilka typowych pytań. Poniżej znajduje się słownik kluczowych terminów i lista często zadawanych pytań, które pomogą Ci jasno komunikować się z użytkownikami. Możesz je uwzględnić w materiałach komunikacyjnych lub szkoleniowych i dostosować je w razie potrzeby do swojej organizacji.

Słownik

- **Uwierzytelnianie dwuskładnikowe (2FA):** Dodatkowa warstwa zabezpieczeń wykraczająca poza samo hasło. 2FA (rodzaj uwierzytelniania wieloskładnikowego) oznacza, że weryfikujesz swoją tożsamość za pomocą dwóch składników: czegoś, co *wiesz* (hasło) oraz czegoś, co *posiadasz* (na przykład telefon) lub czegoś, co potwierdza, kim *jesteś* (na przykład odcisk palca). W ten sposób, nawet jeśli ktoś zna Twoje hasło, nie może się zalogować bez drugiego składnika.
- **Uwierzytelnianie wieloskładnikowe (MFA):** Podobnie jak 2FA, ale może obejmować dwa lub trzy składniki weryfikacji. Rublon jest rozwiązaniem MFA. W praktyce często używamy zamiennie „MFA” i „2FA”, gdy wykorzystywane są dwa składniki uwierzytelniania.
- **Rublon Authenticator:** Aplikacja mobilna instalowana na smartfonie lub tablecie w celu potwierdzenia tożsamości podczas logowania. Może odbierać powiadomienia push w celu zatwierdzenia jednym dotknięciem, skanować kody QR i generować jednorazowe kody dostępu.
- **Powiadomienie push (Powiadomienie mobilne Rublon):** Bezpieczna notyfikacja wysyłana na Twój telefon z zainstalowaną aplikacją Rublon Authenticator. Notyfikacja zawiera prośbę o zatwierdzenie lub odrzucenie próby logowania. Dotknięcie „Zatwierdź” potwierdza, że to właśnie *Ty* jesteś osobą, która próbuje się zalogować. Powiadomienia push są szybkie oraz wygodne i pozwalają na logowanie jednym dotknięciem. Wyświetlają również szczegóły, takie jak do której aplikacji następuje logowanie i skąd pochodzi żądanie, co pozwala wykryć podejrzaną aktywność.
- **Jednorazowy kod dostępu:** Kod jednorazowy używany do weryfikacji Twojej tożsamości. Kody dostępu mogą być generowane przez aplikację Rublon Authenticator (nawet gdy nie masz dostępu do Internetu ani zasięgu sieci komórkowej), generowane przez aplikację innej firmy, wysyłane za pomocą wiadomości SMS lub dostarczane za pomocą tokena sprzętowego (np. funkcja YubiKey OTP). Zazwyczaj są to kody 6-cyfrowe, które wpisujesz podczas logowania jako drugi składnik. Kod dostępu to

przydatna metoda zapasowa, gdy powiadomienia push nie są dostępne.

- **Portal samoobsługowy (widok Zarządzaj uwierzytelniaczami):** Funkcja, która umożliwia zarządzanie własnymi urządzeniami uwierzytelniającymi (jeśli została włączona przez administratorów IT). Widok Zarządzaj uwierzytelniaczami umożliwia dodanie nowego telefonu, numeru telefonu oraz klucza bezpieczeństwa, usunięcie starego urządzenia i zmianę nazwy urządzenia. Pozwala to zarządzać urządzeniami do 2FA bez konieczności kontaktowania się z działem IT.
- **Rejestracja:** Proces konfiguracji Rublon MFA dla Twojego konta. Podczas rejestracji otrzymasz link do zarejestrowania swojego urządzenia (np. smartfona). Po rejestracji Twoje konto będzie wymagało dodatkowego kroku MFA podczas logowania.
- **Widok Rublon Prompt:** Interfejs logowania Rublon, który zobaczysz podczas uzyskiwania dostępu do chronionej aplikacji (jeśli jest obsługiwany przez daną aplikację). Po wprowadzeniu nazwy użytkownika i hasła, widok Rublon Prompt poprosi o użycie drugiego składnika (np. zatwierdzenie notyfikacji push lub podanie kodu dostępu). Jeśli włączona jest samodzielna rejestracja, widok będzie również zawierał opcję Zarządzaj uwierzytelniaczami.

Często zadawane pytania

Pytanie 1: Czy do korzystania z Rublon MFA potrzebuję smartfona?

A: Nie, nie *potrzebujesz* smartfona, ale jest to zalecany i najłatwiejszy sposób uwierzytelniania. Aplikacja mobilna Rublon Authenticator sprawia, że proces MFA jest bardzo szybki (za pośrednictwem powiadomień push). Jeśli jednak nie masz smartfona lub wolisz go nie używać, możesz użyć zwykłego telefonu komórkowego lub nawet telefonu stacjonarnego. W takim przypadku logowania weryfikowane są za pomocą kodu wysyłanego w wiadomości tekstowej lub podczas połączenia telefonicznego. (Zespół IT Twojej organizacji może włączyć różne opcje, więc sprawdź, które metody są dozwolone.)

P2: Czym jest aplikacja mobilna Rublon Authenticator?

A: Rublon Authenticator to darmowa aplikacja mobilna, którą instalujesz na swoim telefonie (iOS, Android, HarmonyOS). Aplikacja służy do wykonywania drugiego kroku uwierzytelniania. Aplikacja może odbierać powiadomienia push do zatwierdzania logowań jednym dotknięciem oraz generować jednorazowe kody dostępu. Możesz również użyć aplikacji do zeskanowania kodu QR wyświetlanego podczas logowania. Aplikacja Rublon Authenticator zasadniczo zamienia Twój telefon w bezpieczny klucz do logowania. Aplikacja działa tylko z platformą Rublon MFA. Nie udostępnia Twoich danych i nie wysyła spamu; po prostu pomaga potwierdzić, że „Tak, to ja się loguję”.

P3: Jaka metoda uwierzytelniania jest zalecana w przypadku Rublon?

A: Jeśli posiadasz smartfon, zdecydowanie zalecamy korzystanie z metody Powiadomienie mobilne za pośrednictwem aplikacji Rublon Authenticator. Zatwierdzenie powiadomienia push w

aplikacji jest szybkie, łatwe i bezpieczne. Wystarczy jedno dotknięcie w telefonie, co jest znacznie szybsze niż wpisywanie kodu. Jeśli nie masz pod ręką smartfona, najlepszym rozwiązaniem jest użycie lub kodu/linku SMS lub połączenia telefonicznego. Jednak to właśnie powiadomienia push zapewniają najpłynniejsze działanie dla większości użytkowników. Najbezpieczniejszą metodą jest użycie kluczy bezpieczeństwa FIDO, ale wymaga to fizycznego klucza i trzymania go zawsze przy sobie.

P4: Na moim telefonie przestały dochodzić powiadomienia push. Co robić?

A: Jeśli powiadomienia push nie docierają, należy sprawdzić kilka rzeczy:

1. **Połączenie internetowe:** Upewnij się, że Twój telefon ma aktywne połączenie internetowe (dane komórkowe lub Wi-Fi). Wiadomości push potrzebują połączenia z internetem, aby dotrzeć do Twojego urządzenia.
2. **Ustawienia powiadomień:** Sprawdź ustawienia powiadomień w telefonie. Upewnij się, że powiadomienia są dozwolone dla aplikacji Rublon Authenticator.
3. **„Przeciągnij, aby odświeżyć”:** Przesuń palcem w dół (pociągnij), aby ręcznie sprawdzić, czy istnieją oczekujące żądania uwierzytelnienia.
4. **Metoda alternatywna:** Jeśli żaden z powyższych kroków nie zadziała, nadal możesz uwierzytelnić się za pomocą kodu dostępu. Otwórz aplikację Rublon Authenticator i użyj sześciocyfrowego kodu do logowania lub skorzystaj z innej metody zapasowej udostępnionej przez dział IT. Następnie skontaktuj się z działem pomocy IT, aby rozwiązać problem z notyfikacjami push.

P5: Jak mogę się zalogować, jeśli nie mam zasięgu sieci komórkowej ani Wi-Fi?

A: Użyj jednorazowego kodu dostępu w aplikacji Rublon Authenticator, który działa w trybie offline. Sprawdź następujący artykuł: [Czy uwierzytelnianie Rublon MFA działa bez dostępu do internetu?](#)

P6: Jak zarządzać nowymi urządzeniami i rejestrować je w platformie Rublon MFA?

A: Jeśli zespół IT włączył funkcję samoobsługi, możesz samodzielnie zarządzać swoimi urządzeniami 2FA. Zazwyczaj, gdy wyświetla się widok Rublon Prompt (po wpisaniu hasła), jest tam dostępna opcja o nazwie Zarządzaj uwierzytelniaczami. Wybierz tę opcję, a po weryfikacji istniejącym urządzeniem, możliwe będzie następujące:

- **Dodaj nowe urządzenie:** Możesz na przykład zarejestrować aplikację innej firmy, taką jak Google Authenticator, lub klucz bezpieczeństwa FIDO.
- **Ustaw urządzenie domyślne:** Jeśli masz zarejestrowanych wiele urządzeń, możesz dla wygody wybrać jedno z nich jako domyślne.

- **Ponowna aktywacja lub wymiana urządzenia:** Jeśli masz nowy telefon, musisz go zarejestrować, a następnie usunąć stary telefon, ponieważ nie będzie już używany.
- **Zmień nazwę lub usuń urządzenie:** Możesz nadać nazwy dla swoich urządzeń („Telefon służbowy” czy „Telefon prywatny”) i usunąć te, których już nie używasz.

Więcej informacji oraz szczegółowe instrukcje ze zrzutami ekranu znajdziesz tutaj: [Przewodnik użytkownika Rublon - Widok Zarządzaj uwierzytelniaczami](#).

Jeśli widok Zarządzaj uwierzytelniaczami nie jest włączony, musisz skontaktować się z działem pomocy technicznej IT w celu dodania lub zmiany urządzenia. Mogą wysłać Ci nowy link do rejestracji lub pomóc w aktualizacji urządzeń.

P7: Co należy zrobić, jeśli zgubię telefon (lub zostanie on skradziony)?

A: Natychmiast poinformuj dział pomocy technicznej IT, jeśli Twoje główne urządzenie do 2FA (np. smartfon z aplikacją Rublon Authenticator) zostanie zgubione lub skradzione. Dział IT pomoże zabezpieczyć Twoje konto, a im szybciej zgłosisz zgubę, tym lepiej będzie można ochronić Twoje konto przed nieautoryzowanym dostępem.

P8: Czy Rublon albo dział IT może zobaczyć moje hasło?

A: Nie. Twoje hasło pozostaje sekretem znanym tylko Tobie. Rublon nigdy nie otrzymuje ani nie przechowuje Twojego hasła. Rolą Rublon jest jedynie zapewnienie weryfikacji dwuskładnikowej po wprowadzeniu przez Ciebie poprawnego hasła. Pomyśl o tym w ten sposób: aplikacja najpierw sprawdza Twoje hasło (bez udostępniania go usłudze Rublon), a jeśli jest poprawne, wtedy wkracza Rublon, aby poprosić o weryfikację dwuskładnikową. Rublon potwierdza: „*tak, to jest zaufane urządzenie/osoba*”, ale nigdy nie widzi Twojego hasła w żadnym momencie.

P9: Czy aplikacja Rublon Authenticator zmienia jakiegokolwiek ustawienia w moim telefonie?

A: Nie, aplikacja Rublon Authenticator nie kontroluje Twojego telefonu. Nie zmienia ustawień i nie uzyskuje dostępu do Twoich danych. Aplikacja poprosi o kilka uprawnień po instalacji (takich jak możliwość otrzymywania powiadomień push) i może zbierać podstawowe informacje o urządzeniu (takie jak wersja systemu operacyjnego urządzenia lub czy masz włączoną blokadę ekranu), ale te informacje służą jedynie do sprawdzenia zgodności z wymogami bezpieczeństwa. Rublon nie może podejmować działań na Twoim telefonie; może jedynie zapytać czy chcesz zatwierdzić logowanie. Zachowujesz pełną kontrolę nad swoim urządzeniem. Wszelkie rekomendacje Rublon są tylko sugestiami i to od Ciebie zależy, czy podejmiesz działania.

3. Wdrożenie Rublon MFA – Szablony wiadomości e-mail dla poszczególnych etapów

Podczas wdrażania platformy Rublon MFA konieczne jest przygotowanie użytkowników końcowych korzystając z dużej ilości powiadomień i jasnych instrukcji. Poniższe szablony wiadomości e-mail mają na celu poprowadzenie użytkowników przez proces wprowadzania Rublon.

Każdy szablon zawiera proponowany harmonogram wysłania wiadomości, przykładowy temat i treść wiadomości e-mail. **Pamiętaj o zamianie symboli zastępczych (takich jak *[DATA]*)** i dostosuj wszelkie szczegóły w razie potrzeby. Ton wiadomości e-mail powinien być pomocny i uspokajający.

E-mail nr 1 – Etap I: Wstępne ogłoszenie („Rublon MFA już wkrótce”)

Kiedy wysłać: Wyślij około **30 dni przed** zaproszeniem do rejestracji w Rublon lub datą uruchomienia.

Temat: Rublon MFA już wkrótce!

Treść:

Dzień dobry,

W ramach naszych wysiłków na rzecz **wzmocnienia poziomu bezpieczeństwa**, wkrótce wprowadzimy do naszego procesu logowania **uwierzytelnianie wieloskładnikowe Rublon MFA**.

Czym jest uwierzytelnianie wieloskładnikowe (MFA)?

Uwierzytelnianie wieloskładnikowe to wymyślne określenie prostego procesu bezpieczeństwa: użycia minimum dwóch sposobów potwierdzenia swojej tożsamości podczas logowania. „Dwa składniki uwierzytelniania” to zazwyczaj (1) Twoje hasło i (2) coś innego – w naszym przypadku zazwyczaj Twój telefon. Oznacza to, że oprócz podania nazwy użytkownika i hasła, podczas logowania do aplikacji będzie trzeba wykonać drugi krok (np. zatwierdzić powiadomienie push na telefonie).

Dlaczego dodajemy uwierzytelnianie wieloskładnikowe?

Same hasła nie wystarczają już do ochrony kont. Wymagając drugiego składnika, który masz **tylko Ty**, możemy znacznie poprawić poziom bezpieczeństwa naszych

systemów i lepiej chronić Twoje konta. Nawet jeśli ktoś zna Twoje hasło, nie będzie mógł uzyskać dostępu do Twojego konta bez ukończenia drugiego kroku uwierzytelniania.

Czym jest Rublon MFA?

Rublon MFA jest bezpieczną platformą do uwierzytelniania wieloskładnikowego, która będzie u nas odpowiadała za ten dwuskładnikowy proces logowania. Jest to oparta na chmurze usługa do ochrony logowań, której zaufały organizacje na całym świecie. Rublon dodaje szybki krok do weryfikacji użytkownika i pomaga zapewnić, że **tylko Ty** możesz uzyskać dostęp do swojego konta.

Wymagane działanie:

Na razie brak. Jest to tylko informacja o nadchodzącym wdrożeniu platformy Rublon MFA.

W ciągu najbliższych kilku tygodni wyślemy Ci więcej informacji o tym, jak zarejestrować się w platformie Rublon MFA, jakie kroki będzie trzeba podjąć i kiedy nastąpi zmiana. **Na razie nie musisz nic robić.** Ten e-mail ma na celu jedynie poinformowanie Cię o tym, co nadchodzi i dlaczego.

Podsumowanie:

Platforma Rublon MFA zostanie wprowadzona za około miesiąc, dzięki czemu nasze logowania będą bezpieczniejsze. Niedługo podamy wszystkie instrukcje potrzebne do konfiguracji. Dziękujemy za uwagę poświęconą tej ważnej aktualizacji!

Wkrótce wyślemy Ci więcej e-maili z informacjami o kolejnych krokach. Jeśli masz jakieś pilne pytania, skontaktuj się z naszym działem pomocy technicznej.

Dziękujemy,
Zespół ds. bezpieczeństwa IT

E-mail nr 2 – Etap II: Przypomnienie i więcej szczegółów

Kiedy wysłać: Wyślij około **15 dni przed** e-mailem z informacją o rejestracji lub datą uruchomienia.

Temat: Przypomnienie: Rejestracja w platformie Rublon MFA rozpoczyna się **[DATA]**

Treść:

Dzień dobry,

Przypominamy, że **za około dwa tygodnie ([DATA])**, zaczniemy rejestrować wszystkich użytkowników w platformie **Rublon MFA**. Rublon stanie się wymaganą częścią procesu logowania do naszych systemów w celu zwiększenia poziomu bezpieczeństwa.

Co się stanie [DATA]?

W tym dniu znajdziesz w swojej skrzynce odbiorczej oficjalny **E-mail rejestracyjny Rublon**. W e-mailu będzie spersonalizowany link, który umożliwi Ci skonfigurowanie Rublon MFA na Twoim urządzeniu. Konfiguracja jest szybka i zajmuje około 2-3 minuty. Zainstalujesz aplikację Rublon Authenticator na swoim smartfonie i połączysz ją ze swoim kontem. Nie martw się, otrzymasz szczegółowe instrukcje!

Dlaczego Rublon MFA i dlaczego teraz?

Jak wspominaliśmy już wcześniej, dodanie uwierzytelniania wieloskładnikowego Rublon MFA znacznie poprawi nasze zabezpieczenia przed nieautoryzowanym dostępem. Cyberincydenty często zaczynają się od kradzieży hasła, a Rublon pomaga zapobiegać tym incydentom, wymagając drugiego rodzaju weryfikacji. Wybraliśmy Rublon, ponieważ jest przyjazny dla użytkownika (zatwierdzenia jednym dotknięciem na telefonie) i wysoce bezpieczny.

Wymagane działanie:

Na razie nic nie trzeba robić. Ten e-mail to tylko **przypomnienie**, że rejestracja do Rublon odbędzie się **[DATA]**. Chcemy, żeby wszyscy byli przygotowani i nie byli zaskoczeni.

Czego można się spodziewać dalej?

- **[DATA]:** Spodziewaj się wiadomości e-mail od **Rublon** z tematem „Zarejestruj swój uwierzytelniacz”. Będzie zawierać Twój link do rejestracji.
- **Proces rejestracji:** E-mail rejestracyjny poprowadzi Cię przez proces instalacji aplikacji Rublon Authenticator na Twoim urządzeniu mobilnym. Jest to proste, a my zapewnimy wskazówki krok po kroku.

Wyślemy jeszcze jedno przypomnienie. Na razie zaznacz w kalendarzu datę **[DATA]**, aby tego dnia przeprowadzić konfigurację Rublon MFA. Jeśli masz jakieś pytania dotyczące nadchodzących wydarzeń, skontaktuj się z **działem wsparcia IT [informacje kontaktowe do pomocy technicznej]**. Jesteśmy tutaj, aby pomóc Ci płynnie przeprowadzić przejście na ten nowy system.

Dziękujemy,
Zespół ds. bezpieczeństwa IT

E-mail nr 3 – Etap III: Ostatnie przypomnienie o rejestracji

Kiedy wysłać: Wyślij około **3 dni przed** datą rejestracji/uruchomienia.

Temat: Ostatnie przypomnienie: Rublon MFA zostanie uruchomiony **[DATA]** (Oto co musisz wiedzieć)

Treść:

Dzień dobry,

Pozostało tylko kilka dni do uruchomienia **uwierzytelniania wieloskładnikowego Rublon** w dniu **[DATA]**. Ten e-mail jest ostatnim przypomnieniem i zawiera ważne informacje, które pomogą Ci się na to przygotować.

Czego można się spodziewać w dniu [DATA]:

- **[DATA]:** Spodziewaj się wiadomości e-mail od **Rublon** z tematem „Zarejestruj swój uwierzytelniacz”. Będzie zawierać Twój link do rejestracji.
- **Proces rejestracji:** E-mail rejestracyjny poprowadzi Cię przez proces instalacji aplikacji Rublon Authenticator na Twoim urządzeniu mobilnym. Jest to proste, a my zapewnimy wskazówki krok po kroku.
- Jeśli **nie masz smartfona**, nie martw się. Rejestracja pozwoli Ci zarejestrować zwykły numer telefonu komórkowego lub stacjonarnego (aby zweryfikować swoją tożsamość za pomocą wiadomości SMS lub połączenia telefonicznego). Rublon obsługuje wiele metod, a aplikacja Rublon Authenticator nie jest twardym wymogiem.

Wymagane działanie:

Nie dzisiaj, ale w dniu **[DATA]**, będzie trzeba dokonać rejestracji w platformie **Rublon MFA**. Sugerujemy, aby zaplanować poświęcenie kilku minut tego dnia na tę konfigurację. Jest ona prosta, a my wyślemy instrukcje.

Jakie są korzyści z Rublon MFA?

- **Wygoda:** Jeśli masz smartfon, możesz po prostu wybrać „Zatwierdź” w powiadomieniu (tzw. **powiadomieniu push**), aby dokończyć logowanie.

- **Bezpieczeństwo:** Uwierzytelnianie dwuskładnikowe Rublon oznacza, że nawet jeśli hasło wycieknie, Twoje konto pozostanie bezpieczne. Znacznie zmniejsza to ryzyko naruszeń bezpieczeństwa.

Jak zmieni się moje logowanie po wprowadzeniu Rublon MFA?

Od **[DATA]**, logując się do chronionych aplikacji, przejdziesz przez następujące kroki:

1. Wprowadź nazwę użytkownika i hasło jak zwykle.
2. **Następnie** platforma Rublon MFA poprosi Cię o wykonanie drugiego kroku uwierzytelniania. Na przykład na Twoim telefonie pojawi się powiadomienie push z prośbą o zatwierdzenie lub zobaczysz prośbę o podanie kodu jednorazowego z aplikacji/telefonu.
3. Po zatwierdzeniu powiadomienia lub wprowadzeniu kodu uzyskasz dostęp jak zwykle.

Twoje zwykłe hasło **nadal działa** i się nie zmienia; Rublon dodaje tylko jeden szybki dodatkowy krok do sekwencji logowania. Możesz traktować Rublon jako dodatkowy zamek w drzwiach, który tylko Ty możesz otworzyć (ponieważ masz klucz w telefonie).

Masz pytania lub potrzebujesz pomocy?

Nasz zespół jest gotowy, aby Cię wesprzeć. Jeśli masz jakieś wątpliwości lub napotkasz na problemy podczas rejestracji, skontaktuj się z **działem pomocy technicznej**:

- Telefon do biura pomocy: 123-456-7890
- E-mail pomocy technicznej: support@twojafirma.pl

Doceniamy Twoją współpracę podczas wprowadzania tych ulepszeń bezpieczeństwa. Dziękujemy za pomoc w zapewnieniu bezpieczeństwa naszej organizacji!

Dziękujemy,
Zespół ds. bezpieczeństwa IT

E-mail nr 4 – Etap IV: Dzień rejestracji – Wymagane działanie

Kiedy wysłać: Wyślij w **dniu rozpoczęcia rejestracji w platformie Rublon MFA** (dzień uruchomienia), najlepiej rano, tuż przed lub w momencie rozpoczęcia wysyłania e-maili rejestracyjnych.

Temat: ****Wymagane działanie:** Zarejestruj się dzisiaj w platformie Rublon MFA**

Treść:

Dzień dobry,

Dzisiaj jest ten dzień! Oficjalnie rozpoczęliśmy wdrażanie **uwierzytelniania wieloskładnikowego Rublon MFA**. Na swoją skrzynkę odbiorczą otrzymasz **E-mail rejestracyjny od Rublon** z tematem „**Zarejestruj swój uwierzytelniacz**”. Znajdź ten e-mail i postępuj zgodnie z instrukcjami i zarejestruj się **dziś**.

Co musisz teraz zrobić?

1. **Znajdź e-mail rejestracyjny** zatytułowany „Zarejestruj swój uwierzytelniacz” (zostanie wysłany na Twój firmowy adres e-mail).
2. Otwórz tego maila i wybierz **Zarejestruj uwierzytelniacz**. Przeniesie Cię to na stronę konfiguracji konta Rublon.
3. **Skonfiguruj swoje urządzenie**. Strona przeprowadzi Cię przez proces rejestracji aplikacji Rublon Authenticator. Aby uzyskać szczegółowe instrukcje, zapoznaj się z: [Jak zarejestrować urządzenie mobilne z aplikacją Rublon Authenticator?](#). Jeśli chcesz zarejestrować inne urządzenie, zapoznaj się z: [Przewodnik użytkownika Rublon - Rejestracja](#).
4. Po rejestracji, uwierzytelnianie Rublon MFA będzie włączone na Twoim koncie! Od tej pory logowanie do naszych chronionych systemów będzie wymagało drugiego kroku uwierzytelniania.

Jeśli nie masz E-maila rejestracyjnego:

Sprawdź folder ze spamem lub skontaktuj się z działem IT, aby uzyskać pomoc. E-mail rejestracyjny jest unikalny dla Ciebie, więc nie używaj cudzego.

Jeśli nie masz smartfona:

Proces rejestracji pozwoli Ci wybrać inną opcję (np. rejestrację numeru telefonu w celu weryfikacji SMS-em/połączeniem telefonicznym). Postępuj zgodnie z instrukcjami wyświetlanymi na ekranie, sprawdź instrukcje krok po kroku na stronie [Przewodnik użytkownika Rublon - Rejestracja](#) lub skontaktuj się z działem wsparcia IT, jeśli potrzebujesz pomocy w konfiguracji urządzenia innego niż smartfon.

Termin ostateczny:

Proszę ukończyć rejestrację w Rublon do **[DATA]**. Po tej dacie dostęp do aplikacji będzie **wymagać** Rublon MFA i zalogowanie się nie będzie możliwe bez wcześniejszej rejestracji w Rublon. Dajemy kilkudniowy okres karencji, aby wszyscy zdążyli się zarejestrować, ale najlepiej zrobić to **od razu**.

Dlaczego to jest ważne?

Rejestracja w platformie Rublon MFA chroni Twoje konto i naszą organizację. Zajmie to tylko kilka minut, a znacznie zwiększy nasze bezpieczeństwo. Po dniu **[DATA]** osoby niezarejestrowane nie będą mogły uzyskać dostępu do naszych aplikacji, dopóki nie ukończą rejestracji. Aby uniknąć przerw w pracy, **prosimy o dokonanie rejestracji możliwie jak najszybciej**.

Potrzebujesz pomocy?

Jeśli masz jakiegokolwiek problemy z procesem rejestracji lub pytania, natychmiast skontaktuj się z **biurem pomocy**. Mamy dziś postawiony w gotowości personel wsparcia, który pomoże w problemach z konfiguracją Rublon MFA.

- **Telefon do biura pomocy:** 123-456-7890
- **E-mail pomocy technicznej:** support@twojafirma.com

Dziękujemy za szybką reakcję. Podejmując ten krok, pomagasz zabezpieczyć dane naszej firmy i swoje konta.

Dziękujemy,
Zespół ds. bezpieczeństwa IT

4. Zmiana polityki Rublon – Szablony e-maili

Oprócz wstępnej komunikacji dotyczącej wdrożenia, konieczne może być również późniejsze poinformowanie użytkowników o **zmianach w politykach Rublon lub ustawieniach konkretnego konektora**. Pamiętaj o **zamianie symboli zastępczych (takich jak [DATA])** i dostosuj wszelkie szczegóły w razie potrzeby. Możesz swobodnie usunąć części wiadomości, jeśli to konieczne (np. jeśli zmieniono tylko politykę Remembered Devices, możesz usunąć informacje o innych politykach). Ton wiadomości e-mail powinien być pomocny i uspokajający.

E-mail nr 1 – Powiadomienie o nadchodzącej zmianie polityki Rublon

Kiedy wysłać: Wyślij około **7 dni** przed wejściem w życie nowych polityk Rublon.

Temat: Ważna aktualizacja: Nadchodzące zmiany w politykach bezpieczeństwa Rublon

Treść:

Dzień dobry,

W ramach naszych wysiłków na rzecz utrzymania najwyższego poziomu bezpieczeństwa, nasze polityki bezpieczeństwa dotyczące uwierzytelniania wieloskładnikowego Rublon MFA zostaną zmienione **w dniu [DATA]**. Proszę zapoznać się ze szczegółami poniżej:

Kogo to dotyczy?

Zmiany te wpłyną na sposób działania uwierzytelniania wieloskładnikowego i zostaną zastosowane **[globalnie/w wybranych aplikacjach/dla określonych grup użytkowników]**.

Co się zmienia?

1. Polityka Remembered Devices (Zapamiętane urządzenia):

- **Co to jest?** Polityka Remembered Devices (Zapamiętane urządzenia) określa, czy i na jak długo użytkownicy mogą dodawać swoje urządzenia jako zaufane, aby zmniejszyć częstotliwość wyświetlania monitów MFA.
- **Szczegóły zmian:**
 - Czas zapamiętania Twojego urządzenia zostanie **[zwiększony/zmniejszony]** do **[wartość w godzinach/dniach]**.
 - Polityka dotycząca zapamiętanych urządzeń zostanie **[włączona/wyłączona]**.
- **Co to dla Ciebie oznacza:**

- W przypadku zmiany w polityce, urządzenia zostaną zapamiętane na **[dłuższy/krótszy]** okres czasu.
- W przypadku włączenia polityki, po oznaczeniu urządzenia jako zaufanego nie będzie już tak często pojawiać się monit proszący o uwierzytelnianie wieloskładnikowe.
- W przypadku wyłączenia polityki, przy każdym logowaniu będzie pojawiać się prośba o potwierdzenie tożsamości.

2. Polityka Authentication Methods (Metody uwierzytelniania):

- **Co to jest?** Polityka Authentication Methods (Metody uwierzytelniania) reguluje dostępne metody uwierzytelniania wieloskładnikowego, w tym domyślną metodę uwierzytelniania używaną podczas logowania.
- **Szczegóły zmian:**
 - **[nazwa metody uwierzytelniania]** zostanie **[aktywowana/dezaktywowana]**.
 - Domyślna metoda uwierzytelniania zostanie ustawiona na **[nazwa metody uwierzytelniania]**.
- **Co to dla Ciebie oznacza:**
 - Jeżeli korzystasz z metody uwierzytelniania, która ma zostać wyłączona, zmień ją na inną już teraz, aby uniknąć późniejszych problemów. [Oto jak możesz zarejestrować alternatywną metodę uwierzytelniania.](#)
 - Jeśli metoda uwierzytelniania jest ustawiona jako domyślna, nastąpi prośba o uwierzytelnienie za pomocą tej metody bez konieczności wybierania jej z widoku [Rublon Prompt](#). Jeśli wolisz użyć innej metody lub zarejestrować dodatkowe uwierzytelniacze, wybierz „Wstecz”, a następnie wybierz „Zarządzaj uwierzytelniaczami”.

3. Polityka Authorized Networks (Sieci autoryzowane):

- **Co to jest?** Polityka Authorized Networks (Sieci autoryzowane) definiuje konkretne zakresy adresów IP, które są uważane za bezpieczne. Uwierzytelnianie wieloskładnikowe jest pomijane dla użytkowników z tymi adresami IP.
- **Szczegóły zmian:**
 - Użytkownicy z Sieci autoryzowanych zostaną pominięci (uwierzytelnianie MFA zostanie pominięte).
 - Polityka Sieci autoryzowane zostanie wyłączona, więc wszystkie sieci będą wymagać uwierzytelniania wieloskładnikowego, chyba że zostanie wprowadzona inna polityka.
- **Co to dla Ciebie oznacza:**
 - Jeśli logujesz się z autoryzowanego adresu IP, doświadczysz uproszczonego procesu uwierzytelniania bez MFA. Jednak jeśli jesteś poza autoryzowanymi

zakresami IP lub polityka Authorized Networks została wyłączona, to zostaną zastosowane standardowe procedury MFA.

Jeśli masz jakiegokolwiek pytania lub potrzebujesz pomocy, skontaktuj się z naszym działem pomocy technicznej pod adresem **[dane kontaktowe pomocy technicznej]**.

Dziękujemy za uwagę poświęconą tej ważnej aktualizacji.

Dziękujemy,
Zespół ds. bezpieczeństwa IT

E-mail nr 2 – Ogłoszenie o zmianie polityki w dniu wprowadzenia zmiany

Kiedy wysłać: Wyślij w dniu wejścia w życie zmian w politykach Rublon.

Temat: Zaktualizowano polityki bezpieczeństwa Rublon – Oto, co się zmieniło

Treść:

Dzień dobry,

Dzisiaj zostały zaktualizowane nasze polityki bezpieczeństwa uwierzytelniania wieloskładnikowego Rublon MFA. Zmiany te weszły już w życie i wpływają na sposób logowania do aplikacji.

Kogo to dotyczy?

Niniejsze zmiany polityk mają zastosowanie **[globalnie/w wybranych aplikacjach/dla określonych grup użytkowników]**. Jeśli należysz do grupy dotkniętej zmianami, Twój sposób logowania może się od dzisiaj nieznacznie różnić.

Co się zmieniło?

1. Polityka Remembered Devices (Zapamiętane urządzenia):

- **Co nowego:**
 - Funkcja zapamiętanych urządzeń została **[włączona/wyłączona]**.
 - Czas przez który urządzenia pozostają zapamiętane został ustawiony na **[wartość w godzinach/dniach]**.
- **Co to dla Ciebie oznacza:**
 - W przypadku zmiany w polityce, urządzenia zostaną zapamiętane na **[dłuższy/krótszy]** okres czasu.
 - W przypadku włączenia polityki, możesz teraz [dodać swoje urządzenie do zapamiętanych](#), aby zmniejszyć liczbę próśb o uwierzytelnienie MFA.

- W przypadku wyłączenia polityki, przy każdym logowaniu będzie pojawiała się prośba o uwierzytelnienie MFA, niezależnie od urządzenia.

2. Polityka Authentication Methods (Metody uwierzytelniania):

- **Co nowego:**
 - **[nazwa metody uwierzytelniania]** została **[aktywowana/dezaktywowana]**.
 - Domyślna metoda uwierzytelniania została ustawiona na **[nazwa metody uwierzytelniania]**.
- **Co to dla Ciebie oznacza:**
 - Jeżeli korzystasz z metody uwierzytelniania, która została wyłączona, musisz ją zmienić na inną. [Oto jak to zrobić](#).
 - Jeśli metoda uwierzytelniania **[nazwa metody uwierzytelniania]** została ustawiona jako domyślna, nastąpi prośba o uwierzytelnienie za pomocą tej metody bez konieczności wybierania jej z widoku [Rublon Prompt](#). Jeśli wolisz użyć innej metody lub zarejestrować dodatkowe uwierzytelniacze, kliknij „Wstecz”, a następnie wybierz „Zarządzaj uwierzytelniaczami”.

3. Polityka Authorized Networks (Sieci autoryzowane):

- **Co nowego:**
 - Uwierzytelnianie wieloskładnikowe (MFA) będzie teraz pomijane w przypadku użytkowników uzyskujących dostęp z określonych adresów IP.
- **Co to dla Ciebie oznacza:**
 - Twoje logowanie nie będzie wymagało już drugiego kroku uwierzytelnienia, jeśli Twój adres IP znajduje się w autoryzowanym zakresie.
 - Jeśli ta polityka została wyłączona, wszyscy użytkownicy będą teraz proszeni o uwierzytelnianie wieloskładnikowe bez względu na ich adres IP.

Potrzebujesz pomocy?

Jeśli masz jakiegokolwiek pytania dotyczące tych zmian lub potrzebujesz pomocy w zmianie metody uwierzytelniania lub zarządzaniu swoimi uwierzytelniaczami, skontaktuj się z naszym działem pomocy technicznej IT:

- **Telefon:** 123-456-7890
- **E-mail:** support@twojafirma.com

Dziękujemy za uwagę i współpracę przy dalszym doskonaleniu naszych praktyk bezpieczeństwa.

Dziękujemy,
Zespół ds. bezpieczeństwa IT

5. Awaria Rublon MFA – Szablony e-maili

Szablony wiadomości e-mail dotyczące przerw w działaniu usługi Rublon MFA i zakłóceń w świadczeniu usług można znaleźć na stronie [Przewodnik Rublon dotyczący gotowości do zapewnienia ciągłości biznesowej](#).