Rublon

Najlepsze praktyki wdrażania Rublon MFA

Wersja 1.0

Spis treści

1. Omówienie

Rublon MFA to platforma uwierzytelniania wieloskładnikowego, która chroni aplikacje, serwery i sieci Twojej organizacji przed naruszeniami danych, wymagając drugiego składnika weryfikacji dla logowań użytkowników. Z uwagi na to, że złamane hasła są główną przyczyną incydentów bezpieczeństwa, wdrożenie platformy Rublon MFA dodaje krytyczną warstwę ochrony, która znacznie zmniejsza ryzyko przejęcia konta i nieautoryzowanego dostępu. Ten przewodnik wyjaśni, jak zaplanować, wdrożyć i uruchomić platformę Rublon MFA w Twoim środowisku, stosując najlepsze praktyki na każdym etapie.

(Uwaga: Niniejszy dokument to przewodnik najlepszych praktyk, a nie substytut dokumentacji Rublon. Aby uzyskać szczegółowe instrukcje krok po kroku, zapoznaj się z oficjalną dokumentacją Rublon.)

Dlaczego potrzebujesz tego przewodnika:

Celem tego przewodnika jest zapewnienie administratorom IT i zespołom projektowym przejrzystego planu wdrożenia platformy Rublon MFA.

Co zostanie omówione:

Omówimy wszystko, od wczesnego planowania sukcesu (przygotowanie środowiska administracyjnego i strategii rejestracji) po konfigurowanie aplikacji, ustalanie polityk, komunikowanie się z użytkownikami końcowymi, szkolenie helpdesku i wreszcie uruchomienie. Naszym celem jest, aby wdrożenie przebiegało możliwie najłatwiej i najskuteczniej.

Dla kogo przeznaczony jest ten przewodnik:

Niniejszy przewodnik jest przeznaczony dla wszystkich osób odpowiedzialnych za wdrażanie Rublon w organizacji. Niezależnie od tego, czy jesteś menedżerem ds. bezpieczeństwa, administratorem IT, czy kierownikiem projektu odpowiedzialnym za wdrożenie Rublon, ten przewodnik jest przeznaczony dla Ciebie.

2. Zaplanuj wdrożenie

Udane wdrożenia MFA zaczynają się od dobrego planowania. W tej fazie zaprojektujesz strategię wdrażania Rublon i przygotujesz administracyjne podstawy dla swojej organizacji. Kluczowe działania obejmują skonfigurowanie konta w konsoli Rublon Admin Console, przypisanie ról administracyjnych, zarządzanie subskrypcją Rublon i wybór sposobu, w jaki użytkownicy będą rejestrować się w platformie MFA. Dokładne zaplanowanie wszystkich kroków już teraz pozwoli zaoszczędzić czas i zapobiegnie problemom później. Kluczem jest podjęcie decyzji z wyprzedzeniem i udokumentowanie swoich wyborów.

2.1. Skonfiguruj swoją organizację w konsoli Rublon Admin Console

- Zacznij od zarejestrowania swojej organizacji w konsoli Rublon Admin Console. Obejmuje to założenie konta Rublon, aby utworzyć dzierżawcę swojej organizacji w naszej konsoli w chmurze. Należy się upewnić, że adres e-mail został zweryfikowany i wykonane zostały wszystkie wymagane kroki rejestracji.
- Po zarejestrowaniu się w konsoli Rublon Admin Console utworzona zostanie nowa organizacja z kontem administratora typu **Owner** (Właściciel).
- Po wejściu do konsoli administracyjnej zapoznaj się z jej układem i sposobem zarządzania aplikacjami, użytkownikami i politykami. Zapoznaj się z dokumentacją konsoli Rublon Admin Console, aby uzyskać kompleksowy opis wszystkich zakładek i funkcji konsoli.

2.2. Przypisz role administracyjne

- Rublon obsługuje w swojej konsoli oparty na rolach dostęp administracyjny, dzięki czemu możesz delegować zadania administracyjne innym osobom, zachowując jednocześnie wysoki poziom bezpieczeństwa.
- Określ, kto będzie odpowiedzialny za różne aspekty wdrożenia (ogólny właściciel, zarządzanie użytkownikami, wsparcie pomocy technicznej itp.) i przypisz tym osobom odpowiednie role administratora w konsoli Rublon Admin Console.

- Pierwsze konto, które utworzysz podczas rejestracji w konsoli administracyjnej będzie kontem z rolą **Owner** (superadministrator).
- Najlepszą praktyką jest przypisanie co najmniej jednego dodatkowego administratora z rolą Owner, aby zapewnić redundancję na wypadek niedostępności jednego z administratorów. Administratorzy-właściciele mogą przypisywać role i zarządzać innymi administratorami, więc upewnij się, że takie uprawnienia najwyższego poziomu mają odpowiednie osoby.
- Możesz utworzyć inne konta administratora z rolami takimi jak: **Administrator**, **User Manager** czy **Help Desk**, aby podzielić obowiązki. Na przykład administrator z rolą Help Desk może pomagać w codziennych problemach użytkowników (takich jak ponowne wysyłanie E-maili rejestracyjnych) nie mając pełnego dostępu do wszystkich ustawień.
- Używaj jednostek Administrative Units, aby zarządzać dostępem do określonych grup użytkowników dla określonych administratorów.
- Wczesne ustalenie ról administratorów pozwoli wyjaśnić, kto za co odpowiada podczas wdrażania i późniejszego utrzymania, a także zapobiegnie powstawaniu wąskich gardeł.

2.3. Zarządzaj subskrypcją i licencjonowaniem

- Sprawdź, ile kont użytkowników musisz chronić i upewnij się, że subskrypcja Rublon je obejmie.
- Podczas bezpłatnego okresu próbnego możesz przetestować wszystkie funkcje Rublon ze wszystkimi swoimi użytkownikami. Przed uruchomieniem musisz jednak wybrać odpowiedni plan subskrypcji (liczba chronionych użytkowników i okres). Uporządkowanie kwestii licencjonowania już teraz gwarantuje, że nie przekroczysz limitów użytkowników i nie doświadczysz nieoczekiwanych dodatkowych kosztów podczas wdrażania.
- Jest to również dobry moment na przegląd cennika Rublon. Pamiętaj, że wiadomości SMS i połączenia telefoniczne wiążą się z dodatkowymi kosztami, więc podejmij decyzję, czy potrzebujesz tych metod uwierzytelniania. Jeśli tak, weź dodatkowy koszt kredytów telefonicznych pod uwagę przy ocenie całkowitych kosztów wdrożenia i utrzymania.

- Gdy wszystko będzie gotowe, rozpocznij subskrypcję Rublon Business. (Zobacz: Jak rozpocząć subskrypcję Rublon Business?)

2.4. Określ które aplikacje chcesz chronić

Poświęć czas na utworzenie listy wszystkich aplikacji i systemów, które zamierzasz zabezpieczyć za pomocą platformy Rublon MFA. Ten krok jest niezbędny do zaplanowania zakresu wdrożenia, przypisania obowiązków i przyspieszenia procesu integracji.

Zacznij od przejrzenia swojej infrastruktury IT i zidentyfikowania systemów, które obsługują poufne dane lub zapewniają dostęp do krytycznych operacji biznesowych. Mogą to być usługi w chmurze, sieci VPN, platformy e-mail, dostawcy tożsamości, rozwiązania zdalnego dostępu, aplikacje lokalne, narzędzia programistyczne i portale wewnętrzne.

Wypisz wszystkie systemy, aplikacje i punkty logowania, które chcesz zabezpieczyć. Dla każdej aplikacji, którą chcesz zabezpieczyć za pomocą platformy Rublon MFA, udokumentuj następujące elementy:

- **Nazwa aplikacji** – np. „Outlook Web App (OWA)”, „Fortinet FortiGate SSL VPN”, „Remote Desktop Gateway”.
- **Typ integracji** – np. zdecyduj, czy chcesz zintegrować się z usługą Fortinet FortiGate SSL VPN za pomocą protokołu RADIUS czy protokołu LDAP.
- **Metoda integracji z platformą Rublon MFA** – np. usługa Rublon Authentication Proxy, dedykowany konektor, dedykowana wtyczka.
- **Link do dokumentacji integracji** – link do odpowiedniej dokumentacji integracji Rublon (np. „https://rublon.com/doc/fortinet-ldap/”).

Wprowadzenie tych informacji do prostego arkusza kalkulacyjnego zapewni jasny przegląd tego, co należy chronić i w jaki sposób będzie obsługiwana każda integracja.

Porady:

- Nie musisz od razu chronić każdego systemu za pomocą uwierzytelniania wieloskładnikowego. Dopuszczalne jest rozpoczęcie od najbardziej krytycznych lub najczęściej używanych systemów i rozszerzanie zasięgu z czasem.

- Zidentyfikuj wszystkie systemy, które muszą zostać uwzględnione w początkowej fazie wdrożenia ze względu na politykę bezpieczeństwa i wymogi zgodności (na przykład zabezpieczenie VPN może być wymagane przez przepisy, których musisz przestrzegać).
- Zidentyfikuj wszelkie przypadki brzegowe, które mogą nie wspierać wdrożenia MFA w łatwy sposób (np. starsze systemy). Być może potrzebne jest do nich specjalne podejście lub trzeba zaakceptować ich początkowe pominięcie (zaplanuj jak się nimi zająć później).
- Utworzonej listy aplikacji należy używać jako dokumentu roboczego przez cały czas trwania projektu wdrożenia. W miarę przechodzenia do fazy integracji i testowania aktualizuj ją o notatki na temat stanu wdrożenia, przypisanych inżynierów i linki do wewnętrznej dokumentacji konfiguracyjnej.
- Po wdrożeniu utrzymuj dokumentację i aktualizuj ją, aby móc uwzględnić nowe aplikacje, gdy zdecydujesz się chronić więcej zasobów za pomocą platformy Rublon MFA.

2.5. Skonfiguruj swoją organizację w konsoli Rublon Admin Console

Udokumentuj dozwolone metody uwierzytelniania oraz, o ile istnieją, te niedozwolone, z rozróżnieniem na aplikację i grupę. Podczas wdrożenia należy skonfigurować polityki Rublon Policies, aby odzwierciedlić te wybory (np. wyłączyć SMS-y dla określonej grupy użytkowników lub wymusić klucze bezpieczeństwa FIDO tylko dla określonej krytycznej aplikacji itp.) Ważne jest również, aby wziąć pod uwagę wygodę użytkownika: więcej opcji pozwala pokryć więcej scenariuszy i zapewnić większą elastyczność. Infrastruktura krytyczna powinna być jednak chroniona wyłącznie za pomocą najbezpieczniejszych metod, takich jak klucze FIDO.

Platforma Rublon MFA obsługuje wiele metod uwierzytelniania – możesz decydować, które metody włączyć, w oparciu o wymagania bezpieczeństwa i wygodę użytkownika. W konsoli Rublon Admin Console możesz utworzyć polityki, w których skonfigurujesz, które metody uwierzytelniania będą dostępne w każdej polityce. Następnie możesz przypisać te polityki do aplikacji lub grup użytkowników.

Podczas planowania zdecyduj, co ma sens dla Twojego środowiska:

- **Push czy OTP**: Powiadomienia push za pośrednictwem aplikacji Rublon Authenticator są przyjazne dla użytkownika i bezpieczne. Kody TOTP (dynamiczne kody 6-cyfrowe) są dobrym rozwiązaniem zapasowym, gdy użytkownicy są offline. Aby zapewnić

użytkownikom większą elastyczność, możesz włączyć zarówno powiadomienia push (metoda uwierzytelniania Powiadomienie mobilne), jak i kody TOTP (metoda Kod dostępu).

- **SMS i telefon**:
    - Link SMS jest wygodną metodą, ale wymaga aktywnego połączenia internetowego.
    - Kod SMS dotrze do użytkowników, którzy nie posiadają smartfona ani aktywnego połączenia internetowego, jest jednak mniej bezpieczny niż powiadomienia push i klucze bezpieczeństwa FIDO.
    - Połączenie telefoniczne jest świetną alternatywą dla telefonów stacjonarnych.
    - Wszystkie te metody wiążą się z kosztem w postaci kredytów telefonicznych, dlatego warto rozważyć włączenie ich tylko dla użytkowników, którzy naprawdę ich potrzebują.
- **Uwierzytelnianie FIDO**: Jeśli masz użytkowników ze sprzętowymi lub programowymi kluczami dostępu (passkeys) lub kluczami bezpieczeństwa FIDO2, takimi jak YubiKey, rozwiązanie Rublon je obsługuje. Metoda uwierzytelniania Klucz bezpieczeństwa WebAuthn/U2F zapewnia najwyższy poziom bezpieczeństwa dzięki odporności na phishing, ale zakup kluczy FIDO dla wszystkich pracowników może być kosztowny. Realną alternatywą jest użycie odpornych na phishing kluczy programowych zapisanych na komputerze lub telefonie użytkownika.
- **Inne**: Rozważ inne metody uwierzytelniania, takie jak Kod QR czy Link e-mail.

2.6. Określ strategię rejestracji użytkowników

Jedną z najważniejszych decyzji planistycznych jest zdecydowanie w jaki sposób użytkownicy będą rejestrowani w platformie Rublon MFA. Rozwiązanie Rublon zapewnia kilka elastycznych metod rejestracji użytkowników. Wybierz podejście (lub kombinację podejść), które najlepiej pasuje do rozmiaru Twojej organizacji i bazy użytkowników. Metody rejestracji użytkowników Rublon obejmują:

- **Rejestracja automatyczna**: Gdy użytkownik po raz pierwszy loguje się do aplikacji chronionej przez Rublon, Rublon automatycznie dodaje go do Twojej organizacji. Automatyczna rejestracja jest bardzo wygodna, ponieważ nie wymaga wstępnego

dodania wszystkich użytkowników do konsoli Rublon Admin Console – użytkownicy rejestrują się sami przy pierwszym użyciu. Ta metoda sprawdza się dobrze w przypadku stopniowych wdrożeń i grup użytkowników obeznanych z technologią.

- **Rejestracja po zatwierdzeniu**: W mniejszych wdrożeniach lub szczególnych przypadkach możesz chcieć, aby próby logowania użytkowników wyzwalały żądanie zatwierdzenia przez administratora. Użytkownicy nie zostaną zarejestrowani, dopóki jeden z administratorów nie zatwierdzi ich członkostwa w organizacji.

- **Rejestracja ręczna (dodawanie pojedynczych użytkowników)**: Możesz ręcznie dodać użytkowników do platformy Rublon MFA. Ta opcja może być wystarczająca dla testu pilotażowego, ale zwykle jest zbyt uciążliwa w przypadku rejestracji dużej liczby użytkowników.

- **Rejestracja ręczna (importowanie z pliku CSV)**: Możesz zaimportować użytkowników z pliku CSV. Ta opcja zapewnia szybszą i bardziej efektywną rejestrację użytkowników, oszczędzając czas i zmniejszając prawdopodobieństwo wystąpienia błędów.

- **„Cicha" rejestracja w trybie pomijania**: Możesz ustawić typ rejestracji na ręczne pomijanie. Dzięki temu proces uwierzytelniania pozostanie z perspektywy użytkownika taki sam (użytkownicy nie będą proszeni o uwierzytelnienie MFA), ale użytkownicy zaczną pojawiać się w zakładce Users (Użytkownicy) w konsoli Rublon Admin Console. Taka „cicha" rejestracja produkcyjna może być dobrą alternatywą do całościowej rejestracji wszystkich użytkowników za jednym zamachem.

- **Synchronizacja katalogów**: W przypadku większych organizacji ręczne dodawanie użytkowników może być uciążliwe, a czekanie na zalogowanie się każdego użytkownika nie zawsze jest możliwe. Rublon oferuje funkcję Directory Sync, która umożliwia automatyczne importowanie i aktualizowanie użytkowników z istniejących katalogów (Synchronizacja usługi Entra ID, Synchronizacja usługi Active Directory). Ta opcja zapewnia, że wszyscy użytkownicy są synchronizowani z platformą Rublon MFA i utrzymywani w synchronizacji z głównym źródłem tożsamości użytkowników.

Porady:

- Udokumentuj, z których metod rejestracji użytkowników będziesz korzystać i w jakiej kolejności.

- Zaplanuj sposób postępowania z osobami, które chcą zarejestrować się później (np. nowymi pracownikami lub osobami, które nie uczestniczyły w początkowym etapie wdrażania).
- Elastyczność rozwiązania Rublon pozwala na dodawanie użytkowników w dowolnym momencie, ale rozsądnym rozwiązaniem jest wdrożenie do tego konkretnego procesu (np. uwzględnienie rejestracji MFA jako części konfiguracji IT nowego pracownika).

2.7. Zdefiniuj grupy użytkowników

Grupy użytkowników odgrywają kluczową rolę w strukturyzacji wdrożenia Rublon, gdyż umożliwiają grupowanie użytkowników w łatwe do zarządzania jednostki, zarządzanie dostępem do aplikacji i przypisywanie polityk dostępu.

Przed wdrożeniem należy poświęcić czas na zdefiniowanie, które grupy użytkowników powinny istnieć w Rublon i w jaki sposób będą zarządzane.

- **Ręczne tworzenie grupy:**
    - Możesz ręcznie dodawać grupy użytkowników w konsoli Rublon Admin Console. Ta metoda daje Ci pełną kontrolę i jest odpowiednia dla mniejszych środowisk lub wdrożeń pilotażowych.
    - **Użyj tej metody, gdy:** Chcesz szybko zdefiniować małe, niestandardowe grupy do celów testowych lub nie planujesz synchronizacji użytkowników z żadnego zewnętrznego katalogu.
- **Grupy zsynchronizowane z katalogiem:**
    - Jeśli planujesz używać synchronizacji katalogów, Rublon może zaimportować użytkowników i ich członkostwo w grupach z zewnętrznej usługi katalogowej (np. Microsoft Entra ID lub Active Directory). Tych zsynchronizowanych grup można używać bezpośrednio w konfiguracji polityk i przypisaniach aplikacji.
    - **Użyj tej metody, gdy:** Chcesz zarządzać członkostwem w grupie centralnie za pomocą swojego dostawcy tożsamości i uniknąć ręcznego zarządzania grupami w rozwiązaniu Rublon.

2.8. Określ strategię rejestracji uwierzytelniaczy użytkowników

Po podjęciu decyzji, jak zarejestrować użytkowników w platformie Rublon MFA, dobrym pomysłem jest zdecydowanie, jak użytkownicy będą mogli rejestrować swoje uwierzytelniacze.

Uwierzytelniacz jest środkiem używanym do weryfikacji tożsamości użytkownika podczas drugiego etapu uwierzytelniania (zazwyczaj po wprowadzeniu hasła). Uwierzytelniacze obejmują numer telefonu (stacjonarny lub komórkowy), adres e-mail, aplikację mobilną Rublon Authenticator, aplikację mobilną innej firmy i klucz bezpieczeństwa WebAuthn/U2F. Każdy uwierzytelniacz musi zostać zarejestrowany, zanim będzie można go użyć.

Wybierz strategię, która zapewni, że każdy użytkownik będzie miał zarejestrowany co najmniej jeden uwierzytelniacz do czasu wymuszenia uwierzytelniania MFA na jego koncie. Rozwiązanie Rublon oferuje elastyczne opcje rejestrowania uwierzytelniaczy, w zależności od metody integracji aplikacji i polityk organizacji. Należy pamiętać, że można zezwolić na obydwie poniższe opcje, np. poprosić większość użytkowników o samodzielną rejestrację a E-maile rejestracyjne wysłać tylko do tych użytkowników, którzy nie są obeznani z technologią.

- **Samodzielna rejestracja uwierzytelniacza za pośrednictwem opcji Zarządzaj uwierzytelniaczami:**
    - Jeśli twoja aplikacja chroniona przez Rublon obsługuje widok Rublon Prompt, użytkownicy mogą samodzielnie rejestrować swoje uwierzytelniacze bezpośrednio w widoku **Zarządzaj uwierzytelniaczami**.
    - Taka samoobsługa jest intuicyjna i dobrze działa w większości środowisk. Użytkownicy mogą dodać aplikację mobilną Rublon Authenticator, zarejestrować klucze bezpieczeństwa i samodzielnie zarządzać innymi metodami uwierzytelniania. (Zobacz: Przewodnik użytkownika Rublon - Rejestracja).
    - Widok **Zarządzaj uwierzytelniaczami** można włączyć lub wyłączyć dla każdej aplikacji, edytując aplikację i (od/za) znaczając opcję **Let Users Manage Authenticators** (Pozwól użytkownikom zarządzać uwierzytelniaczami).
    - Należy pamiętać, że głównym ograniczeniem samodzielnej rejestracji jest to, że użytkownicy muszą mieć dostęp do co najmniej jednej aplikacji obsługującej widok Rublon Prompt. Jeśli chcesz, aby użytkownicy wstępnie zarejestrowali swoje uwierzytelniacze przed zintegrowaniem rozwiazania Rublon z aplikacjami, wysłanie E-maila rejestracyjnego jest lepszą opcją.

- **Rejestracja uwierzytelniacza za pośrednictwem E-maila rejestracyjnego wysłanego przez administratora:**
    - W środowiskach, w których samodzielna rejestracja jest ograniczona lub widok Rublon Prompt nie jest dostępny, administratorzy mogą wysłać E-mail rejestracyjny z poziomu konsoli administracyjnej. Wiadomość e-mail zawiera link, po którego otwarciu użytkownik jest prowadzony przez proces rejestracji uwierzytelniacza.
    - Ta opcja jest przydatna, gdy widok Rublon Prompt jest wyłączony ze względów bezpieczeństwa lub zgodności, integracja nie obsługuje widoku Rublon Prompt (np. wdrożenia wykorzystujące usługę Rublon Authentication Proxy) lub chcesz mieć większą kontrolę nad tym, kto i kiedy może się zarejestrować.

2.9. Zdefiniuj polityki bezpieczeństwa

Rozwiązanie Rublon pozwala dostosować, kiedy i jak wymagane jest uwierzytelnianie wieloskładnikowe, zdefiniować zapamiętane urządzenia i sieci autoryzowane, a także dostosować zabezpieczenia do konkretnych potrzeb. Warto podjąć decyzję, jakie polityki utworzyć dla różnych aplikacji i grup użytkowników, jeszcze zanim rozpocznie się ich tworzenie w konsoli administracyjnej. Wcześniejsze udokumentowanie polityk pomaga w opracowaniu kompleksowej strategii kontroli dostępu, która będzie łatwa do wdrożenia i utrzymania.

Kluczowe źródła informacji na temat polityk:

- Rublon Admin Console - Policies
- Polityki grup
- Polityka Authentication Methods
- Polityka Authorized Networks
- Polityka Remembered Devices

Najlepsze praktyki dotyczące polityk Rublon:

- Upewnij się, że polityka Global Policy (Polityka globalna) spełnia Twoje najbardziej podstawowe wymagania dotyczące kontroli dostępu, dzięki czemu nie będzie potrzeby jej nadpisywania dla każdej aplikacji i grupy użytkowników.

- Każda polityka Custom Policy (Polityka niestandardowa) powinna mieć unikalną i łatwą do zidentyfikowania nazwę, aby uniknąć pomyłek podczas przypisywania jej do aplikacji lub grupy użytkowników.
- Zawsze zwracaj uwagę na sytuacje, w których spodziewano się uwierzytelniania MFA, ale nie zostało ono wywołane: np. użytkownik spodziewał się MFA, ale nie otrzymał o nie prośby. Sprawdź dokładnie, czy Twoje polityki obejmują wszystkie przypadki.
- **Najlepsze praktyki dotyczące polityki Authentication Methods:**
    - Zdecyduj, czy chcesz włączyć domyślną metodę uwierzytelniania.
- **Najlepsze praktyki dotyczące polityki Authorized Networks:**
    - Wyznaczaj tylko sieci, które są naprawdę bezpieczne.
    - Wiele organizacji odchodzi od zaufania opartego na lokalizacji, ale w Twoim środowisku takie podejście wciąż może mieć sens.
    - Jeśli włączysz tę politykę, regularnie aktualizuj listę adresów IP. Zawsze ją testuj: upewnij się, że logowanie z nieautoryzowanego adresu IP wywołuje MFA, a logowanie z autoryzowanego adresu IP nie.
- **Najlepsze praktyki dotyczące polityki Remembered Devices:**
    - Skonfiguruj czas trwania zgodnie z preferowanym poziomem bezpieczeństwa: typowe wartości to 2 dni, 7 dni i 14 dni.
    - Całkowicie wyłącz politykę Remembered Devices dla aplikacji wymagających wysokiego poziomu bezpieczeństwa.
    - Poinformuj administratorów i dział pomocy technicznej, jak mogą zarządzać zapamiętanymi urządzeniami użytkowników.

2.10. Zdefiniuj ustawienia specyficzne dla aplikacji

- Wybierz tryb **Fail Mode** (Tryb awaryjny) dla każdej aplikacji. (Więcej informacji: Przewodnik Rublon dotyczący gotowości do zapewnienia ciągłości biznesowej).
- Poznaj najlepsze praktyki testowania platformy Rublon MFA na środowisku produkcyjnym (te porady mają zastosowanie również w środowiskach testowych i staging podczas początkowego wdrażania).

2.10.1. Rublon Authentication Proxy

Najlepsze praktyki:

- Najlepsze praktyki instalacji i konfiguracji usługi Rublon Authentication Proxy

Kluczowe zasoby:

- Rublon Authentication Proxy - Dokumentacja
- Centrum Pomocy Rublon - Rublon Authentication Proxy
- Konfigurowanie usługi Rublon Authentication Proxy jako serwera proxy RADIUS
- Konfigurowanie usługi Rublon Authentication Proxy jako serwera proxy LDAP
- Wyjaśnienie trybów RADIUS w usłudze Rublon Authentication Proxy

2.10.2. Konektor Rublon dla Windows

Najlepsze praktyki:

- Przed pierwszą instalacją należy pozostawić przynajmniej jedną aktywną sesję zalogowanego użytkownika (najlepiej sesję lokalną), aby zapobiec sytuacji, w której nieprawidłowa konfiguracja, brak wymaganych bibliotek w systemie lub dodatkowe oprogramowanie zakłócające działanie konektora Rublon dla Windows doprowadzi do utraty dostępu do maszyny.
- Podczas pierwszej instalacji należy włączyć uwierzytelnianie wieloskładnikowe (MFA) tylko dla połączeń RDP, aby w razie problemów z instalacją możliwy był dostęp lokalny bez uwierzytelniania wieloskładnikowego.
- Instalacja konektora kończy się ponownym uruchomieniem systemu, co może przerwać istniejące sesje Remote Desktop Protocol (RDP). Z tego powodu zaplanuj instalację poza godzinami szczytu, aby zminimalizować zakłócenia.
- Jeśli masz wiele punktów końcowych i musisz wdrożyć konektor Rublon dla Windows na wszystkich z nich, użyj narzędzi PDQ Deploy, Microsoft System Center Configuration Manager (SCCM) lub Intune, aby zautomatyzować wdrożenie.
- Upewnij się, że zapora sieciowa na serwerze, na którym zainstalowano Rublon dla Windows, nie ogranicza komunikacji Rublon na porcie TCP 443.

- Włącz tryb offline, aby chronić dostęp użytkowników za pomocą platformy Rublon MFA, nawet gdy nie mają połączenia z Internetem.

Kluczowe zasoby:

- Rublon MFA dla Windows - Dokumentacja
- Rublon MFA dla Windows - FAQ
- Wdrażanie Rublon MFA dla systemu Windows przy użyciu narzędzia PDQ Deploy
- Wdrażanie Rublon MFA dla systemu Windows przy użyciu narzędzia SCCM
- Wdrażanie Rublon MFA dla systemu Windows przy użyciu narzędzia Intune

2.11. Nakreśl harmonogram wdrożenia i zdefiniuj kamienie milowe

Posiadanie jasnego harmonogramu pomaga koordynować komunikację i zadania. Zapewnia również czas na przetestowanie i dostosowanie rozwiązania, zanim wszyscy zostaną dotknięci zmianami. W przypadku dużych przedsiębiorstw zaleca się podejście etapowe (pilotaż → szersze wdrożenie → egzekwowanie), a nie gwałtowne. Jeśli to możliwe, zastosuj „rejestrację etapową" – najpierw oswój podstawową grupę użytkowników z rozwiązaniem Rublon, potem uwzględnij ich opinie, a dopiero potem przejdź do większych grup.

Poniżej znajduje się przykład planu wdrożenia Rublon dla dużego przedsiębiorstwa (ponad 20 000 pracowników). Mniejsze firmy mogą to wszystko zrobić w krótszym czasie; to tylko przykład.

- **Start pilotażowy:** np. „Tydzień 1: Wdrażanie Rublon w trybie testowym dla administratorów IT lub grupy pilotażowej".
- **Okres rejestracji:** np. „Tydzień 2-3: Poinformuj wszystkich pracowników, zarejestruj ich w konsoli administracyjnej i poproś o zarejestrowanie uwierzytelniaczy".
- **Faza integracji aplikacji:** np. „Tydzień 2: Zabezpiecz VPN i jedną krytyczną aplikację za pomocą rozwiązania Rublon (dla użytkowników pilotażowych). Tydzień 4: Rozszerz na wszystkie kluczowe aplikacje".
- **Udoskonalenia:** np. „Tydzień 3: Przegląd wstępnych wyników pilotażu i wprowadzenie udoskonaleń, jeśli to konieczne".

- **Data globalnego wdrożenia:** np. „Tydzień 5, poniedziałek: Włączono wymuszanie MFA dla wszystkich użytkowników we wszystkich systemach objętych zakresem”.
- **Przegląd po uruchomieniu:** np. „Tydzień 5: Sprawdź wskaźniki adopcji, zajmij się użytkownikami, którzy jeszcze się nie zarejestrowali, dostosuj ustawienia w razie potrzeby”.

3. Wdróż platformę Rublon MFA w trybie testowym

Po zakończeniu planowania nadszedł czas na integrację rozwiązania Rublon z aplikacjami i przeprowadzenie dokładnych testów. Celem jest sprawienie, by platforma Rublon MFA działała płynnie w środowisku IT Twojej organizacji bez zakłócania operacji biznesowych.

Pod koniec etapu testowania spełnione powinny być następujące punkty:

- Wszystkie najważniejsze aplikacje zintegrowane z platformą Rublon MFA.
- Sprawdzony proces logowania dla każdej aplikacji zintegrowanej z rozwiązaniem Rublon.
- Pewność, że użytkownicy mogą się pomyślnie zarejestrować i zalogować.
- Wstępna idea jakie polityki i ustawienia zastosować, na podstawie opinii zebranych po pilocie.

Podczas testowania miej pod ręką dokumentację Rublon. Jeśli napotkasz złożony problem, zapoznaj się z odpowiednią dokumentacją:

- Dokumentacja integracji Rublon
- Pliki Rublon do pobrania
- Konsola Rublon Admin Console - Dokumentacja
- Przewodnik użytkownika Rublon
- Przewodnik Rublon dla pomocy technicznej
- Przewodnik Rublon dotyczący gotowości do zapewnienia ciągłości biznesowej

3.1. Testowanie w środowisku stagingowym

Przed wdrożeniem na produkcji możesz przetestować integracje Rublon w kontrolowanym środowisku stagingowym. Jeśli nie masz instancji stagingowych ani aplikacji testowych, rozważ „miękkie uruchomienie” na produkcji dla ograniczonej liczby użytkowników (zobacz następną sekcję).

- Najpierw zintegruj rozwiązanie Rublon z instancją testową. Użyj kont użytkowników testowych, aby przejść przez proces logowania.
- Zasymuluj zarówno udane, jak i nieudane scenariusze MFA. Na przykład, co się stanie, jeśli użytkownik odrzuci powiadomienie push lub wprowadzi zły kod?
- Jeśli konektor Rublon obsługuje tryb Fail Mode, również go przetestuj.
- Sprawdź, czy działa przydzielanie kont użytkowników, np. czy nowy użytkownik testowy jest dodawany do konsoli Rublon Admin Console z prawidłowymi informacjami. Jeśli używasz synchronizacji katalogów Directory Sync, sprawdź, czy użytkownik istnieje i został dodany do odpowiedniej grupy.
- Sprawdź, czy pojawia się widok Rublon Prompt i czy udostępnia oczekiwane metody uwierzytelniania. Jeśli wyłączono pewne metody w polityce, upewnij się, że nie można ich wybrać w widoku. Jeśli dostosowano branding lub komunikaty pomocy, również należy je sprawdzić.

3.2. Pilotaż z małą grupą użytkowników

Najlepszą praktyką przy każdym wdrożeniu uwierzytelniania wieloskładnikowego jest przeprowadzenie pilotażu z udziałem podgrupy rzeczywistych użytkowników przed wdrożeniem w całej organizacji. Wybierz obeznanych z technologią użytkowników (najlepiej sprawdzają się pracownicy działu IT i pracownicy Help Desk). Włącz uwierzytelnianie Rublon MFA tylko dla tych użytkowników w kilku aplikacjach:

- W konsoli Rublon Admin Console utwórz politykę grup skierowana tylko do użytkowników pilotażowych w celu włączenia uwierzytelniania MFA podczas logowania do określonej aplikacji. Na przykład grupa „Dział IT” musi używać MFA podczas

logowania do systemu Windows i połączeń poprzez RDP, podczas gdy wszyscy inni użytkownicy mają ustawiony status **Bypass** (Pomijany).

- Poproś użytkowników pilotażowych, aby przeszli przez rejestrację i zaczęli używać rozwiązania Rublon w swojej codziennej rutynie. Dokładnie zbierz ich opinie: Czy rejestracja była łatwa? Czy napotkali na jakieś systemy, w których rozwiązanie Rublon nie działało? Czy są skargi na monity (zbyt wolne itp.)? Tego typu informacje są nieocenione przy dostosowywaniu ustawień przed wdrożeniem w całej firmie.

- Podczas pilotażu symuluj typowe scenariusze wsparcia z grupą pilotażową: np. jeden użytkownik zgubi telefon – niech spróbuje procesu odzyskiwania (poproś go o użycie zapasowej metody uwierzytelniania lub wydaj mu Kod pominięcia). Taki scenariusz przetestuje również Twoją gotowość do świadczenia pomocy technicznej.

3.3. Udoskonalanie konfiguracji na podstawie testów

Normalnym jest, że podczas testowania i pilotażu odkrywa się drobne problemy i wychodzi konieczność zastosowania poprawek. Poświęć czas na udoskonalenie wdrożenia:

- Na podstawie wyników testów pilotażowych dostosuj ustawienia w konektorach Rublon i konsoli Rublon Admin Console.

- W razie potrzeby zaktualizuj strategię rejestracji uwierzytelniaczy użytkowników.

- Sprawdź dzienniki **Authentication Logs** (Dzienniki uwierzytelniania) i dzienniki **Audit Logs** (Dzienniki audytu) w konsoli Rublon Admin Console. Te dzienniki mogą uwypuklić problemy (np. czy konkretny użytkownik został odrzucony i dlaczego) oraz zachowania administratorów (np. czy konkretny administrator wykonał jakąś akcję i czy powinien mieć na to pozwolenie). Dzienniki pomagają również upewnić się, że Rublon rejestruje wszystko, co dzieje się w Twojej organizacji, co może być przydatne w przypadku audytów.

- Upewnij się, że zastosowano wszystkie wymagane mechanizmy związane z trybem Fail Mode.

4. Przekaż informacje użytkownikom końcowym

Nawet najlepsze wdrożenie MFA może się nie udać bez odpowiedniej komunikacji z użytkownikami. Jasne, terminowe komunikaty zapewniają, że użytkownicy rozumieją, co się dzieje, dlaczego ma to znaczenie i co muszą zrobić.

Kluczowe zasoby:

- Przewodnik użytkownika Rublon
- Przewodnik Rublon dla pomocy technicznej

Szablony komunikacji:

- Szablony komunikacji z użytkownikami końcowymi Rublon

Najlepsze praktyki w zakresie komunikacji z użytkownikiem końcowym:

- Zachowaj prostotę. Używaj krótkich, prostych instrukcji.
- Zacznij wcześnie. Ogłoś zmianę co najmniej dwa tygodnie przed globalnym uruchomieniem.
- Użyj wielu kanałów. E-mail, banery intranetu, wiadomości podczas logowania, posty na czacie.
- Wyjaśnij „dlaczego”. Podkreśl, że MFA chroni zarówno firmę, jak i użytkownika.
- Dołącz elementy wizualne. Zrzuty ekranu pomagają zmniejszyć niepokój i liczbę zgłoszeń do pomocy technicznej.
- Zwiększ dostępność wsparcia. Poinformuj użytkowników, gdzie mogą się udać, jeśli utkną.
- Zachęcaj do przygotowania urządzenia. Poproś użytkowników o zainstalowanie aplikacji Rublon Authenticator z wyprzedzeniem.

- Podkreśl wygodę rozwiązania. Wspomnij o opcji „Zapamiętaj to urządzenie”, gdy to stosowne.

5. Przeszkol dział pomocy technicznej

Twoje biuro pomocy będzie pierwszą linią wsparcia podczas wdrażania platformy Rublon MFA. Przygotuj ich odpowiednio wcześnie, aby ograniczyć zamieszanie i szybko rozwiązywać problemy użytkowników.

Kluczowe zasoby:

- Przewodnik Rublon dla pomocy technicznej
- Artykuły pomocy Rublon
- Konsola Rublon Admin Console - Dokumentacja
- Kontakt z pomocą techniczną Rublon

Główne tematy szkolenia:

- **Ćwiczenia praktyczne:** Zarejestruj personel wsparcia wcześnie, aby mogli doświadczyć platformy Rublon MFA jako użytkownicy końcowi. Pozwól im przetestować każdą metodę uwierzytelniania, którą Twoja organizacja planuje obsługiwać (Push, TOTP, SMS itp.).
- **Umiejętności korzystania z konsoli administracyjnej:** Upewnij się, że agenci wiedzą, jak:
  - Wyszukiwać użytkowników i sprawdzać ich status rejestracji
  - Wysyłać i wysyłać ponownie E-maile rejestracyjne
  - Dodawać i usuwać urządzenia użytkownika
  - Generować Kody pominięcia
  - Analizować dzienniki uwierzytelniania
- **Diagnoza problemu:** Naucz agentów rozwiązywania typowych problemów, takich jak:
  - Nie otrzymano E-maila rejestracyjnego
  - Zgubiono lub wymieniono telefon
  - Powiadomienia push nie działają
  - Użytkownik jest zdezorientowany kodem QR lub procesem konfiguracji

- **Użyj odpowiednich ról administratora:** Poziom 1 wsparcia może mieć ograniczony dostęp (np. rola Help Desk), podczas gdy administratorzy lub pracownicy poziomu 2 zajmują się eskalacją zadań w ramach roli Application Manager lub User Manager.

Najlepsze praktyki:

- Zanim wdrożysz platformę Rublon MFA w środowisku produkcyjnym, przeszkol personel wsparcia.
- Zakładać, że pracownicy pomocy technicznej są nowicjuszami w korzystaniu z platformy Rublon MFA, tak jak użytkownicy końcowi.
- Poinformuj administratorów Rublon o różnicach między kontem administratora i kontem użytkownika. Wyjaśnij wyraźnie, że administratorzy potrzebują obu.
- Podaj proste kroki rozwiązywania typowych problemów za pomocą skryptów i list kontrolnych.
- Przeszkol agentów w zakresie potwierdzania tożsamości użytkownika przed wydaniem Kodów pominięcia.
- Naucz agentów, kiedy mają zgłosić problem do pomocy technicznej Rublon, jeśli problemu nie da się szybko rozwiązać.
- Spodziewaj się wzrostu liczby zgłoszeń podczas globalnego uruchomienia. Przypisz dodatkowe zasoby wsparcia i rozważ dedykowane kanały (np. „Rublon MFA Help Desk”).

6. Wdróż platformę Rublon MFA w środowisku produkcyjnym

Dzień uruchomienia jest kulminacją planowania i przygotowań. Ta sekcja zawiera ostateczną listę kontrolną gotowości, wskazówki dotyczące realizacji wdrożenia oraz kroki, które należy podjąć po wdrożeniu.

6.1. Lista kontrolna gotowości do uruchomienia

a) **Przetestowano i zintegrowano aplikacje:** Sprawdź, czy wszystkie aplikacje są prawidłowo połączone z Rublon i czy uwierzytelnianie wieloskładnikowe działa zgodnie z oczekiwaniami.
b) **Rejestracja użytkowników prawie ukończona:** Dąż do 90%+ rejestracji. Zidentyfikuj i skontaktuj się z jeszcze niezarejestrowanymi użytkownikami.
c) **Przejrzano i dostosowano polityki:** Upewnij się, że wszystkie polityki są prawidłowo przypisane.
d) **Gotowość pomocy technicznej:** Potwierdź, że personel pomocniczy został przeszkolony, jest dostępny i odpowiednio wyposażony na czas uruchomienia.
e) **Zdefiniowano plan awaryjny:** Upewnij się, że poznano i wdrożono w życie porady z dokumentu Przewodnik Rublon dotyczący gotowości do zapewnienia ciągłości biznesowej.
f) **Poinformowano interesariuszy i użytkowników:** Przekaż kierownictwu informacje o czasie uruchomienia i protokołach eskalacji. Wyślij przypomnienie dla całej firmy.
g) **Kontakt ze wsparciem Rublon i najważniejsze dostępne zasoby:** Upewnij się, że wszystkie informacje, takie jak dane kontaktowe pomocy technicznej Rublon i dokumentacja Rublon, są łatwo dostępne i można z nich szybko skorzystać, gdy zajdzie taka potrzeba.

6.2. Uruchomienie

a) **Włącz egzekwowanie MFA:** Zmień ustawienia aplikacji tak, aby wymagały uwierzytelniania wieloskładnikowego (np. o 7:00 rano).
b) **Monitoruj aktywność**: Monitoruj logi pod kątem skoków liczby błędów lub nieudanych logowań i szybko badaj trendy.
c) **Pozostań w kontakcie:** Utrzymuj czat lub połączenie na żywo między liderami wsparcia, aby dzielić się aktualizacjami w czasie rzeczywistym.
d) **Pomóż w razie potrzeby:** Bądź w gotowości, aby pomóc osobom rejestrującym się z opóźnieniem. W razie potrzeby wydaj Kody pominięcia i dopilnuj dalszych kroków.
e) **Przekaż status:** W południe przekaż interesariuszom informacje o postępach prac i wszelkich znanych problemach.

6.3. Co zrobić po uruchomieniu

a) **Radzenie sobie z maruderami:** Śledź i aktywuj użytkowników, którzy nie zdążyli się zarejestrować (urlop, nieobecność itp.).
b) **Zbierz opinie:** Przeprowadź ankietę wśród użytkowników i kierowników zespołów, aby zebrać opinie na temat wdrożenia i obszarach sprawiających trudności.
c) **W razie potrzeby dostosuj polityki:** Dostrój ustawienia i zakres egzekwowania uwierzytelniania MFA na podstawie zebranych opinii.
d) **Aktualizacja wewnętrznej dokumentacji:** W razie potrzeby odśwież swoją wewnętrzną dokumentację i popraw komunikaty dla użytkowników.
e) **Doceń zespół:** Dziel się sukcesami i doceniaj pracowników i użytkowników za współpracę.

6.4. Przykładowy harmonogram uruchomienia

- **Na tydzień przed wdrożeniem:** Ostateczna prośba o rejestrację, dział pomocy technicznej jest już przeszkolony.
- **Dzień uruchomienia rano:** Rozpoczęcie egzekwowania MFA, otwarcie kanałów wsparcia.
- **Środek dnia:** Kontynuacja monitorowania, problemy są rozwiązywane, kierownictwo jest informowane o postępach.
- **Koniec dnia:** Podsumowanie zespołu i udokumentowanie wyciągniętych wniosków.
- **Po pierwszym dniu:** Dalsze wsparcie, sprzątanie i działania następcze.

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

www.rublon.pl