Rublon

Jak przygotować się do Proof of Concept (PoC) rozwiązania Rublon MFA

Spis treści

1. Wymagania, informacje i działania potrzebne do sprawnego rozpoczęcia testów

Proof of Concept (PoC) rozwiązania Rublon MFA pozwala zweryfikować działanie uwierzytelniania wieloskładnikowego w rzeczywistym środowisku organizacji przed podjęciem decyzji o szerszym wdrożeniu.

Zakres PoC może być bardzo prosty i obejmować pojedynczą testową stację roboczą lub serwer, ale może również uwzględniać VPN, usługi zdalnego dostępu, aplikacje webowe, systemy infrastrukturalne czy aplikacje własne.

Nie każdy PoC wymaga przygotowania dodatkowej maszyny wirtualnej ani zmian w dostawcy tożsamości typu Active Directory czy Entra ID. Wymagania zależą przede wszystkim od systemów, które mają zostać objęte testem, oraz wybranej metody integracji z rozwiązaniem Rublon MFA.

Celem tego dokumentu jest pomoc w określeniu zakresu PoC i wcześniejszym przygotowaniu zasobów, dostępów oraz zgód, które mogą być potrzebne do rozpoczęcia testów.

2. Co warto ustalić przed rozpoczęciem PoC?

Najwięcej czasu zajmuje często nie sama konfiguracja rozwiązania Rublon MFA, lecz przygotowanie środowiska, uzyskanie wymaganych dostępów oraz akceptacja zmian przez odpowiednie zespoły.

Dlatego jeszcze przed spotkaniem technicznym warto odpowiedzieć na poniższe pytania.

2.1 Które systemy mają wejść w zakres PoC?

Należy określić konkretny zasób lub zasoby, dla których ma zostać zweryfikowane MFA. Mogą to być na przykład:

- stacje robocze lub serwery Windows,
- połączenia RDP i środowiska Remote Desktop Services,
- VPN i Wi-Fi,
- systemy Linux,
- aplikacje webowe,
- aplikacje korzystające z protokołów LDAP lub RADIUS,

- aplikacje obsługujące SAML, OAuth 2.0 lub OpenID Connect,
- aplikacje chmurowe,
- aplikacje niestandardowe.

Nie jest konieczne testowanie wszystkich planowanych integracji jednocześnie. PoC można rozpocząć od jednego reprezentatywnego scenariusza, a następnie stopniowo rozszerzać jego zakres.

2.2 Jakie scenariusze logowania mają zostać sprawdzone?

Samo wskazanie systemu nie zawsze wystarcza. Warto określić, **które ścieżki logowania są istotne z punktu widzenia PoC**.

Przykładowo, dla systemu Windows można osobno testować logowanie lokalne oraz RDP. W przypadku rozwiązania VPN organizacja może chcieć zweryfikować określony profil połączenia, grupę użytkowników albo sposób uwierzytelniania.

Dobrze zdefiniowany zakres pozwala ustalić kryteria sukcesu PoC i uniknąć zmian środowiskowych, które nie są potrzebne do realizacji testu.

2.3. Jak obecnie odbywa się uwierzytelnianie użytkowników?

Przed PoC należy określić, jaki system odpowiada obecnie za podstawowe uwierzytelnianie użytkowników chronionego zasobu.

Może to być na przykład:

- konto lokalne,
- usługa Active Directory,
- usługa Microsoft Entra ID,
- katalog LDAP,
- serwer RADIUS,
- dostawca tożsamości wykorzystujący SAML,
- rozwiązanie wykorzystujące OAuth 2.0 lub OpenID Connect,
- inny mechanizm uwierzytelniania.

Rozwiązanie Rublon MFA co do zasady **rozszerza istniejący proces logowania o dodatkowy etap uwierzytelniania**, dlatego znajomość obecnej ścieżki logowania jest potrzebna do dobrania właściwej integracji.

2.4. Czy system testowy korzysta z domeny lub centralnego źródła tożsamości?

Warto określić, czy testowana maszyna lub aplikacja:

- należy do domeny Active Directory,
- korzysta z Microsoft Entra ID,
- wykorzystuje zewnętrzny katalog LDAP lub serwer RADIUS,
- korzysta wyłącznie z kont lokalnych,
- wykorzystuje inne centralne źródło tożsamości.

Informacja ta pozwala prawidłowo odwzorować rzeczywisty scenariusz uwierzytelniania.

2.5. Czy PoC ma obejmować synchronizację użytkowników?

Należy wcześniej zdecydować, czy jednym z elementów PoC ma być użycie funkcji Directory Sync, czy wystarczy ręczne przygotowanie niewielkiej liczby użytkowników testowych.

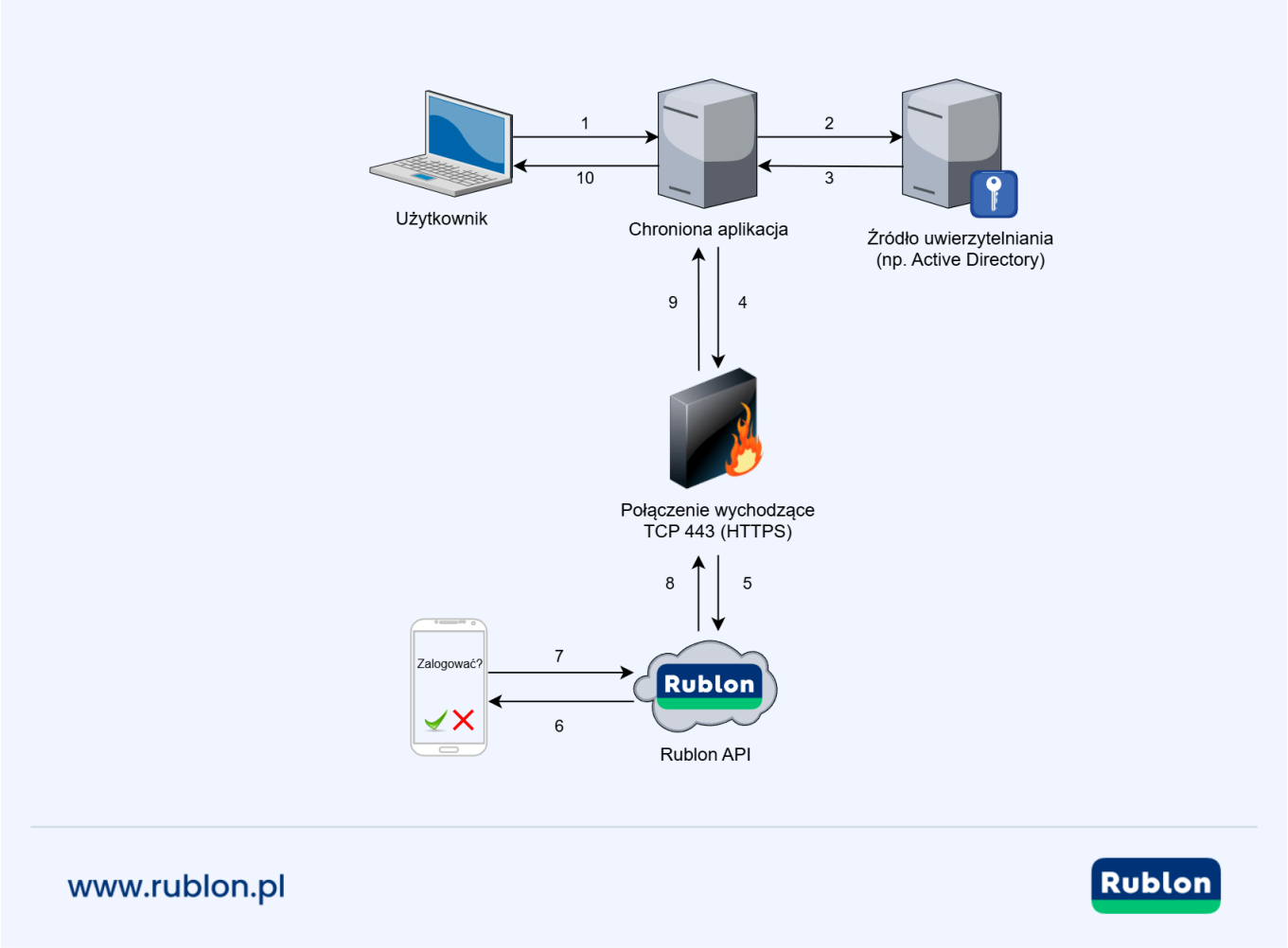
Jeżeli synchronizacja katalogu nie jest jednym z kryteriów PoC, można ją często pozostawić na kolejny etap i dzięki temu ograniczyć liczbę elementów infrastruktury wymaganych do rozpoczęcia pierwszych testów.

Jeżeli synchronizacja katalogów ma zostać uwzględniona, należy dodatkowo ustalić:

- jakie źródło katalogowe będzie synchronizowane,
- których użytkowników lub grup ma dotyczyć test,
- czy dostępna jest wymagana komunikacja z katalogiem i interfejsem Rublon API.

3. Jak wygląda podstawowy przepływ uwierzytelniania?

Szczegółowy przepływ zależy od wybranej integracji, ale w typowym scenariuszu rozwiązanie Rublon MFA działa jako dodatkowa warstwa uwierzytelniania połączona z istniejącym środowiskiem organizacji.



W typowym scenariuszu opartym na loginie i haśle użytkownik najpierw przekazuje dane logowania do chronionej aplikacji, która weryfikuje je w źródle uwierzytelniania, takim jak usługa Active Directory **(1-3)**. Po poprawnym uwierzytelnieniu podstawowym chroniona aplikacja lub komponent integracyjny wysyła żądanie MFA do interfejsu Rublon API **(4-5)**. Rublon API inicjuje wyzwanie MFA dla użytkownika **(6-7)**, przedstawione na diagramie jako powiadomienie mobilne. Po jego zatwierdzeniu wynik uwierzytelniania wraca do chronionej aplikacji **(8-9)**, która może zakończyć proces logowania i przyznać użytkownikowi dostęp **(10)**.

W niektórych integracjach komponent Rublon MFA instalowany jest bezpośrednio na chronionym systemie. W innych działa jako osobna usługa w środowisku organizacji. Rublon Authentication Proxy i Rublon Access Gateway są przykładami komponentów wdrażanych w środowisku klienta.

Niniejszy przewodnik skupia się na wymaganiach i działaniach potrzebnych do przygotowania środowiska do PoC. Natomiast więcej informacji o architekturze rozwiązania, roli poszczególnych komponentów oraz sposobie ich komunikacji można znaleźć w dokumencie Architektura Rublon MFA.

4. Czy do PoC potrzebna jest dodatkowa maszyna?

Nie zawsze.

Wymagania zależą od wybranej integracji.

W przypadku części konektorów Rublon MFA komponent jest instalowany bezpośrednio na chronionym systemie. Przykładowo, konektor Rublon MFA dla Windows Logon i RDP jest instalowany na maszynie Windows, której logowania mają zostać objęte testem. Nie wymaga to uruchamiania osobnej maszyny tylko na potrzeby konektora.

Inne integracje wymagają uruchomienia dodatkowego komponentu w środowisku organizacji. Dotyczy to między innymi scenariuszy wykorzystujących:

- Rublon Authentication Proxy
- Rublon Access Gateway

Zależnie od rozwiązania komponent może zostać uruchomiony na istniejącym odpowiednim serwerze albo na osobnej maszynie fizycznej lub wirtualnej.

Ważne

Komponenty Rublon MFA należy instalować wyłącznie w miejscach wynikających z architektury konkretnej integracji.

Przykładowo, usługa Rublon Authentication Proxy może działać zarówno na osobnej niewielkiej maszynie, jak i - jeżeli środowisko i wymagania danego rozwiązania na to pozwalają - na serwerze wykorzystywanym przez chronioną usługę. Kluczowe jest zapewnienie wymaganej komunikacji sieciowej.

Szczegółowe wymagania systemowe należy każdorazowo sprawdzić w aktualnej dokumentacji wybranej integracji.

5. Szczególne wymagania wybranych komponentów Rublon MFA

Wymagania dotyczące przygotowania środowiska zależą od wybranej integracji. Niektóre konektory instaluje się bezpośrednio na chronionym systemie, natomiast inne wymagają uruchomienia dodatkowego komponentu w środowisku organizacji.

Poniżej przedstawiono najważniejsze kwestie, które warto uwzględnić przed PoC dla najczęściej wykorzystywanych komponentów. Szczegółowe i aktualne wymagania systemowe oraz instrukcje instalacji należy zawsze zweryfikować w dokumentacji wybranej integracji oraz w artykule Wymagania systemowe i przeglądarkowe dla usługi Rublon MFA.

5.1. Rublon MFA dla Windows Logon i RDP

Konektor Rublon MFA dla Windows Logon i RDP jest instalowany na każdej maszynie Windows, do której logowanie ma zostać objęte ochroną. Do przeprowadzenia takiego PoC nie jest wymagany osobny serwer ani instalacja komponentu Rublon MFA na kontrolerze domeny.

Przed rozpoczęciem PoC należy:

- przygotować co najmniej jedną testową maszynę Windows spełniającą aktualne wymagania konektora,
- ustalić, które scenariusze mają zostać zweryfikowane, na przykład logowanie lokalne, RDP lub oba,
- ustalić rodzaj kont używanych podczas testów, na przykład lokalne konta systemu Windows, domenowe konta usługi Active Directory lub konta Microsoft Entra ID,
- zapewnić dostęp administracyjny umożliwiający instalację i konfigurację konektora,
- umożliwić maszynie komunikację z interfejsem Rublon API zgodnie z wymaganiami sieciowymi,
- upewnić się, że polityki zapory sieciowej, oprogramowania antywirusowego lub EDR pozwalają na instalację konektora i jego komunikację z interfejsem Rublon API.

Jeżeli jednym z celów PoC jest również sprawdzenie sposobu wdrożenia konektora na większej liczbie urządzeń, warto wykorzystać jedną z instrukcji masowego wdrażania konektora przy użyciu Microsoft Intune, Microsoft System Center Configuration Manager (SCCM) lub PDQ Deploy. Organizacja powinna w takim przypadku zapewnić dostęp do używanego systemu zarządzania stacjami końcowymi oraz przygotować reprezentatywną grupę urządzeń, na której zostanie zweryfikowany proces dystrybucji.

Aktualne obsługiwane systemy, metody uwierzytelniania oraz instrukcję instalacji zawiera dokumentacja Rublon MFA dla Windows Logon i RDP.

5.2. Rublon Authentication Proxy

Usługa Rublon Authentication Proxy jest komponentem instalowanym w środowisku organizacji i stosowanym przede wszystkim w integracjach wykorzystujących protokół RADIUS lub LDAP.

Usługę Rublon Authentication Proxy można uruchomić na systemie Windows Server lub Linux. Nie jest wymagane przeznaczanie dla niej dedykowanej maszyny w każdym PoC. Może to być osobna maszyna, ale również serwer, na którym jest hostowana chroniona usługa. Miejsce instalacji należy dobrać pod architekturę i wymagania testowanego środowiska.

Przed rozpoczęciem PoC należy:

- przygotować maszynę z obsługiwanym systemem Windows Server lub Linux, na której będzie można zainstalować usługę Rublon Authentication Proxy,
- zapewnić dostęp administracyjny do tej maszyny,

- ustalić, który system lub urządzenie będzie chronione podczas testu i w jaki sposób obecnie realizuje uwierzytelnianie RADIUS lub LDAP,
- umożliwić wymaganą komunikację sieciową pomiędzy chronionym systemem, maszyną z usługą Rublon Authentication Proxy, źródłem uwierzytelniania oraz usługą Rublon MFA,
- przygotować niewielką grupę użytkowników reprezentujących testowany scenariusz,
- w przypadku testowania funkcji Directory Sync wskazać źródło katalogowe oraz użytkowników lub grupy, które mają zostać objęte synchronizacją.

Rublon Authentication Proxy nie jest dostawcą tożsamości. Organizacja musi posiadać źródło, względem którego podczas PoC będzie można zweryfikować podstawowe dane uwierzytelniające użytkowników. Do przetestowanych i zweryfikowanych źródeł należą między innymi Active Directory, Microsoft Entra ID, OpenLDAP, FreeIPA, Google Secure LDAP, FreeRADIUS, Cisco ACS oraz Microsoft NPS. W przypadku korzystania z Microsoft Entra ID lub Google Secure LDAP warto przed PoC zapoznać się również z opisami dedykowanych scenariuszy: Uwierzytelnianie LDAP i RADIUS danymi logowania Microsoft Entra ID oraz MFA oraz Korzystanie z Google Secure LDAP z Rublon Authentication Proxy.

Wysoka dostępność. Podstawowy PoC zazwyczaj nie wymaga konfiguracji wysokiej dostępności, jednak jeżeli odporność na awarię komponentu uwierzytelniającego jest jednym z kryteriów PoC, można również zweryfikować usługę Rublon Authentication Proxy w konfiguracji HA. Taki scenariusz wymaga przygotowania co najmniej dwóch serwerów dla instancji Rublon Authentication Proxy oraz sieciowego load balancera. Zakres testu HA warto uzgodnić przed rozpoczęciem PoC, ponieważ wymaga większej liczby zasobów infrastrukturalnych niż podstawowy test funkcjonalny.

Szczegółowe informacje zawiera dokumentacja Rublon Authentication Proxy.

5.3. Rublon Access Gateway

Usługa Rublon Access Gateway umożliwia objęcie Rublon MFA aplikacji korzystających z uwierzytelniania SAML. Komponent jest instalowany w środowisku organizacji.

Jeżeli PoC ma wykorzystywać usługę Rublon Access Gateway, przed rozpoczęciem testów organizacja powinna:

- wskazać aplikację, dla której ma zostać zweryfikowana integracja SAML,
- upewnić się, że możliwa jest zmiana konfiguracji SAML/SSO tej aplikacji na potrzeby testu,

- przygotować maszynę, na której będzie można zainstalować i uruchomić usługę Rublon Access Gateway,
- zapewnić dostęp administracyjny potrzebny do instalacji i konfiguracji,
- przygotować nazwę domenową/FQDN, która będzie wykorzystywana przez usługę Rublon Access Gateway,
- przygotować odpowiedni certyfikat TLS dla tej nazwy,
- przygotować dostęp do źródła uwierzytelniania, które będzie wykorzystywane w testowanym scenariuszu,
- umożliwić wymaganą komunikację sieciową pomiędzy systemami uczestniczącymi w procesie uwierzytelniania.

Szczegółowy zakres przygotowań zależy od systemu operacyjnego, wybranego sposobu instalacji i aplikacji objętej PoC. Należy go ustalić na podstawie aktualnej dokumentacji Rublon Access Gateway.

5.4. Rublon MFA dla Linux SSH

Rublon MFA dla Linux SSH jest instalowany bezpośrednio na chronionym systemie Linux i integruje się z mechanizmem PAM. Do podstawowego PoC nie jest wymagany osobny serwer przeznaczony dla konektora.

Przed rozpoczęciem PoC należy:

- przygotować testowy system Linux spełniający aktualne wymagania konektora,
- zapewnić dostęp administracyjny root lub odpowiednie uprawnienia sudo umożliwiające instalację pakietu i modyfikację konfiguracji PAM,
- ustalić sposób podstawowego uwierzytelniania użytkowników, na przykład hasło lokalne lub uwierzytelnianie względem usługi Active Directory,
- ustalić, czy PoC ma obejmować logowanie hasłem, kluczem SSH lub oba scenariusze, ponieważ objęcie MFA logowania kluczem SSH wymaga dodatkowej konfiguracji,
- umożliwić chronionemu systemowi komunikację z interfejsem Rublon API przez TCP 443,
- zapewnić bezpieczną alternatywną możliwość dostępu administracyjnego podczas zmian konfiguracji PAM.

Jeżeli testowany system Linux korzysta z usługi Active Directory, warto również wcześniej ustalić wykorzystywany mechanizm integracji, na przykład SSSD lub Winbind. Rublon MFA nie zastępuje ani nie konfiguruje istniejącego połączenia systemu Linux z domeną.

Aktualne obsługiwane dystrybucje, wymagania oraz instrukcje instalacji i konfiguracji zawiera dokumentacja Rublon MFA dla Linux SSH.

5.5. Rublon MFA dla Roundcube

Rublon MFA dla Roundcube jest instalowany jako wtyczka bezpośrednio w istniejącej instalacji Roundcube. Do podstawowego PoC nie jest wymagany osobny serwer przeznaczony dla konektora.

Przed rozpoczęciem PoC należy:

- przygotować działającą testową instalację Roundcube,
- zapewnić dostęp administracyjny do serwera oraz plików instalacyjnych i konfiguracyjnych Roundcube,
- zapewnić możliwość instalacji wtyczki w katalogu plugins oraz uruchomienia narzędzia Composer w katalogu instalacji Roundcube,
- umożliwić wprowadzenie wymaganych zmian w konfiguracji Roundcube, w tym ustawienia sposobu przechowywania sesji zgodnie z dokumentacją konektora,
- umożliwić serwerowi komunikację z interfejsem Rublon API,
- przygotować niewielką grupę użytkowników, którzy mogą poprawnie zalogować się do Roundcube przed włączeniem MFA.

Podczas PoC konektor dodaje dodatkowy etap uwierzytelniania po poprawnej weryfikacji loginu i hasła przez istniejący mechanizm uwierzytelniania Roundcube. Nie jest więc konieczne zastępowanie obecnego źródła uwierzytelniania użytkowników.

Szczegółowe wymagania oraz instrukcje instalacji i konfiguracji zawiera dokumentacja Rublon MFA dla Roundcube.

5.6. Rublon Log Sync

Jeżeli jednym z celów PoC jest również sprawdzenie eksportu dzienników Rublon MFA do systemu SIEM, można do tego wykorzystać aplikację Rublon Log Sync. Aplikacja pobiera

Dzienniki uwierzytelniania, Dzienniki audytu i Dzienniki telefoniczne z interfejsu Rublon Admin API, a następnie przesyła je do systemu SIEM.

Przed rozpoczęciem takiego testu należy:

- przygotować serwer Linux, na którym będzie działać aplikacja Rublon Log Sync,
- przygotować system SIEM, który może odbierać komunikaty przez protokół TCP,
- umożliwić serwerowi komunikację z interfejsem Rublon API oraz systemem SIEM,
- zapewnić dostęp do interfejsu Rublon Admin API i przygotować dane uwierzytelniające aplikacji typu Admin API.

Dostęp do interfejsu Rublon Admin API wymaga płatnego planu Rublon MFA i nie jest dostępny w planach Rublon MFA Free ani Rublon MFA Trial. Szczegółowe wymagania oraz instrukcje konfiguracji zawiera dokumentacja Rublon Log Sync.

5.7. Pozostałe komponenty

W przypadku pozostałych konektorów, aplikacji i integracji Rublon MFA, zakres przygotowań zależy od architektury konkretnego systemu.

Przed PoC należy przede wszystkim upewnić się, że testowany system działa prawidłowo przed instalacją rozwiązania Rublon MFA, dostępne są wymagane uprawnienia administracyjne oraz możliwe jest wprowadzenie zmian opisanych w dokumentacji danej integracji.

Jeżeli PoC dotyczy aplikacji niestandardowej i wykorzystuje jeden z pakietów Rublon SDK lub bezpośrednią integrację z interfejsem Rublon REST API, należy również zapewnić udział osoby lub zespołu, który może wprowadzić wymagane zmiany w testowanej aplikacji.

6. Jakich użytkowników przygotować?

Do pierwszego PoC zazwyczaj nie jest potrzebna duża grupa użytkowników. Zalecane jest wykorzystanie niewielkiej, kontrolowanej grupy kont testowych reprezentujących rzeczywiste scenariusze logowania.

Przed rozpoczęciem testów warto ustalić:

- którzy użytkownicy będą uczestniczyć w PoC,
- jakie typy kont reprezentują,
- z jakich systemów lub grup pochodzą,

- czy posiadają dane wymagane przez wybraną integrację,
- czy mają uprawnienia umożliwiające przetestowanie wszystkich zaplanowanych scenariuszy.

Jeżeli PoC obejmuje synchronizację użytkowników z katalogu, zalecane jest wcześniejsze określenie niewielkiej grupy użytkowników lub grup katalogowych, które mają zostać objęte synchronizacją.

7. Jakie metody MFA mają zostać sprawdzone?

Przed spotkaniem warto określić, które metody uwierzytelniania są istotne z punktu widzenia organizacji i powinny zostać uwzględnione w PoC.

Jeżeli test ma obejmować aplikację Rublon Authenticator, użytkownicy testowi powinni mieć możliwość zainstalowania aplikacji na urządzeniach mobilnych i zarejestrowania jej w Rublon MFA.

Jeżeli jednym z kryteriów PoC jest uwierzytelnianie za pomocą kluczy bezpieczeństwa FIDO2, kluczy dostępu FIDO2, uwierzytelniaczy RFID lub innych fizycznych uwierzytelniaczy, odpowiednie urządzenia powinny być dostępne podczas testów.

Nie wszystkie metody są dostępne dla każdej integracji, dlatego ostateczny zestaw należy dobrać zgodnie z dokumentacją chronionego systemu.

8. Jak przygotować komunikację sieciową?

Przed rozpoczęciem PoC warto sprawdzić wymagania sieciowe, ponieważ blokada komunikacji jest jedną z najprostszych przyczyn opóźnienia testów.

W zależności od integracji należy zapewnić możliwość komunikacji:

- komponentu Rublon MFA z interfejsem Rublon API,
- chronionego systemu z komponentem integracyjnym Rublon MFA,
- komponentu integracyjnego z istniejącym źródłem uwierzytelniania,
- pomiędzy innymi systemami uczestniczącymi w konkretnej ścieżce logowania.

Aplikacje i konektory Rublon MFA wymagają możliwości komunikacji z interfejsem Rublon API przez wychodzący port TCP 443. Jeżeli organizacja stosuje restrykcyjne reguły zapory sieciowej lub listy dozwolonych adresów i domen, należy przygotować odpowiednie reguły przed rozpoczęciem PoC.

Przed PoC należy również ustalić, czy ruch:

- przechodzi przez serwer proxy,
- podlega inspekcji TLS/SSL,
- jest ograniczany przez firewall,
- jest filtrowany przez rozwiązanie antywirusowe lub EDR,
- wymaga wcześniejszego dodania określonych adresów lub usług do list dozwolonych.

Wymagania dotyczące połączenia z interfejsem Rublon API opisują artykuły Jak skonfigurować zaporę sieciową dla usługi Rublon MFA? oraz Z jakich zakresów adresów IP korzysta usługa Rublon MFA?. Wymagania dotyczące komunikacji wewnątrz środowiska, na przykład pomiędzy komponentem Rublon MFA, chronionym systemem i źródłem uwierzytelniania, należy sprawdzić w dokumentacji wybranej integracji.

Warto również przed PoC zweryfikować, czy zabezpieczenia poczty elektronicznej nie blokują wiadomości wysyłanych przez Rublon MFA. Wiadomości e-mail mogą być wykorzystywane między innymi podczas rejestracji użytkowników, uwierzytelniania metodą Link e-mail oraz komunikacji z administratorami. Jeżeli organizacja stosuje restrykcyjne filtry antyspamowe lub listy dozwolonych nadawców, przed rozpoczęciem testów należy dodać do list dozwolonych odpowiednie adresy IP oraz adresy e-mail nadawców Rublon MFA. Informacje na ten temat znajdują się w artykułach Z jakich adresów IP korzysta usługa Rublon MFA do wysyłania e-maili? oraz Z jakich adresów e-mail korzysta Rublon do wysyłania wiadomości?.

9. Jakie zmiany i uprawnienia mogą być potrzebne?

PoC powinien być przeprowadzany w kontrolowanym środowisku testowym lub na wybranych systemach, dla których organizacja zaakceptowała wprowadzanie zmian.

Zależnie od integracji może być wymagane:

- zainstalowanie komponentu Rublon MFA,
- uruchomienie dodatkowej usługi,
- zmodyfikowanie konfiguracji uwierzytelniania chronionego systemu,
- skonfigurowanie protokołu RADIUS, LDAP, SAML, OAuth 2.0, OpenID Connect lub innego mechanizmu integracyjnego,
- wprowadzenie reguły firewall,
- utworzenie konta technicznego z odpowiednimi minimalnymi uprawnieniami,
- wykonanie restartu systemu lub usługi,
- zmiana konfiguracji DNS lub certyfikatów.

Nie wszystkie powyższe działania będą potrzebne w każdym PoC.

Dlatego przed właściwym spotkaniem PoC należy przede wszystkim ustalić, kto po stronie organizacji może wykonać zmiany w systemach objętych testem oraz jak długo trwa uzyskanie wymaganych zgód.

10. Zaplanuj możliwość bezpiecznego wycofania zmian

Przed modyfikacją procesu logowania należy upewnić się, że administratorzy zachowają bezpieczną możliwość odzyskania dostępu lub przywrócenia poprzedniej konfiguracji w przypadku niepowodzenia testu.

Sposób zabezpieczenia zależy od konkretnej integracji. Może obejmować między innymi:

- zachowanie aktywnej sesji administracyjnej,
- ograniczenie pierwszego testu do wybranych użytkowników lub systemów,
- przygotowanie kopii konfiguracji,
- udokumentowanie zmian wykonywanych podczas PoC,
- przygotowanie procedury wycofania konfiguracji,
- pozostawienie alternatywnego, bezpiecznego sposobu dostępu administracyjnego.

W przypadku integracji, których instalacja lub konfiguracja może wpłynąć na dostęp administracyjny do chronionego systemu, warto zachować co najmniej jedną aktywną sesję lub inną bezpieczną ścieżkę dostępu do czasu potwierdzenia poprawnego działania Rublon MFA.

Jeżeli PoC musi zostać przeprowadzony na środowisku produkcyjnym, przed rozpoczęciem testów warto również zapoznać się z artykułem Najlepsze praktyki testowania platformy Rublon MFA na środowisku produkcyjnym.

11. Co przygotowuje organizacja, a w czym pomaga Rublon?

11.1. Po stronie organizacji

Przed rozpoczęciem PoC organizacja powinna:

- określić system lub systemy objęte testem,
- określić scenariusze logowania, które mają zostać sprawdzone,
- przekazać informacje o obecnym sposobie uwierzytelniania,

- przygotować testowe środowisko lub zasób,
- przygotować użytkowników testowych,
- zdecydować, czy PoC obejmuje Directory Sync,
- zapewnić wymagane konta administracyjne i techniczne,
- uzyskać wewnętrzne zgody na wymagane zmiany,
- zapewnić odpowiednią komunikację sieciową,
- przygotować wymagane urządzenia do testowania wybranych metod MFA,
- zapewnić możliwość bezpiecznego wycofania zmian.

11.2. Po stronie Rublon

W ramach przygotowania i realizacji PoC spółka Rublon pomaga:

- dobrać właściwą integrację do wskazanego systemu i scenariusza logowania,
- określić, jakie komponenty będą potrzebne,
- wskazać aktualną dokumentację i wymagania techniczne,
- przejść przez konfigurację organizacji testowej w konsoli Rublon Admin Console,
- skonfigurować wybraną integrację,
- przeprowadzić enrollment użytkowników testowych,
- skonfigurować potrzebne polityki i metody uwierzytelniania,
- zweryfikować przepływ logowania i wynik dodatkowego uwierzytelniania,
- pomóc w analizie problemów ujawnionych podczas PoC,
- wspólnie podsumować wyniki i określić potencjalny zakres kolejnych testów.

12. Lista kontrolna przed spotkaniem technicznym

Przed rozpoczęciem PoC warto przygotować odpowiedzi na poniższe pytania.

Do ustalenia	Status	Komentarze
Wiemy, jaki system lub zasób chcemy zabezpieczyć	☐	
Wiemy, które scenariusze logowania chcemy przetestować	☐	
Wiemy, jaki system obecnie realizuje podstawowe uwierzytelnianie	☐	
Wiemy, czy testowany system korzysta z domeny lub centralnego źródła tożsamości	☐	

Do ustalenia	Status	Komentarze
Zdecydowaliśmy, czy PoC ma obejmować Directory Sync	☐	
Wybraliśmy niewielką grupę użytkowników testowych	☐	
Wiemy, jakie metody MFA chcemy sprawdzić	☐	
Mamy dostęp administracyjny do systemów wymagających zmian	☐	
Sprawdziliśmy wymagania wstępne w aktualnej dokumentacji wybranej integracji	☐	
Wiemy, czy potrzebny będzie dodatkowy komponent Rublon MFA w naszym środowisku	☐	
Jeżeli wybrana integracja wymaga zewnętrznego źródła uwierzytelniania, mamy takie źródło i działa ono poprawnie	☐	
Zweryfikowaliśmy możliwość komunikacji z interfejsem Rublon API i innymi wymaganymi systemami	☐	
Zweryfikowaliśmy, że wymagane wiadomości e-mail wysyłane przez Rublon MFA nie będą blokowane przez zabezpieczenia poczty	☐	
Wiemy, czy firewall, proxy, EDR lub inspekcja TLS mogą wpływać na komunikację	☐	
Uzyskaliśmy lub rozpoczęliśmy proces uzyskiwania wymaganych zgód na zmiany	☐	
Mamy możliwość bezpiecznego wycofania zmian po teście	☐	

13. Czego nie trzeba przygotowywać z góry?

Aby rozpocząć PoC, zazwyczaj nie trzeba od razu przygotowywać docelowej architektury produkcyjnej.

W szczególności:

- dodatkowa maszyna nie jest wymagana dla każdej integracji,
- samo korzystanie z Active Directory nie oznacza konieczności instalowania komponentu Rublon MFA na kontrolerze domeny,
- nie trzeba od razu obejmować testem wszystkich użytkowników,
- nie trzeba testować wszystkich planowanych systemów podczas jednego etapu,
- funkcja Directory Sync może zostać pozostawiona na kolejny etap, jeżeli nie jest wymagana do osiągnięcia celów pierwszego testu,
- podstawowy PoC nie musi od razu uwzględniać docelowego HA, redundancji i wszystkich mechanizmów ciągłości działania, chyba że ich weryfikacja jest jednym z celów PoC.

Najprostszy skuteczny PoC powinien zawierać tylko te elementy, które są potrzebne do potwierdzenia uzgodnionych scenariuszy i kryteriów sukcesu.

14. Co dalej?

Po potwierdzeniu podstawowych scenariuszy zakres PoC można stopniowo rozszerzać o kolejne systemy, grupy użytkowników i elementy infrastruktury.

W zależności od potrzeb kolejne etapy mogą obejmować między innymi:

- dodatkowe aplikacje i systemy,
- Directory Sync,
- kolejne metody uwierzytelniania,
- bardziej szczegółowe polityki dostępu,
- integrację dzienników z systemem SIEM,
- segmentację i bardziej złożone scenariusze sieciowe,
- wysoką dostępność komponentów,
- przygotowanie architektury docelowej,
- rozszerzenie testu na większą grupę użytkowników.

Przy przechodzeniu od PoC do szerszego pilotażu i wdrożenia produkcyjnego warto skorzystać z dokumentu Przewodnik Rublon dotyczący najlepszych praktyk wdrożeniowych, który opisuje między innymi planowanie wdrożenia, etap testowy, przygotowanie organizacji oraz przejście do środowiska produkcyjnego.

Szczegółowe wymagania systemowe, obsługiwane wersje oraz instrukcje instalacji mogą zmieniać się wraz z rozwojem produktów. Dlatego podczas każdego PoC należy korzystać z

aktualnej dokumentacji konkretnej integracji Rublon MFA, zamiast opierać przygotowanie środowiska na statycznej liście wymagań.

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

www.rublon.pl