Poradnik wdrażania uwierzytelniania wieloskładnikowego (MFA)

Rublon sp. z o.o.

ul. Stanisława Wyspiańskiego 11

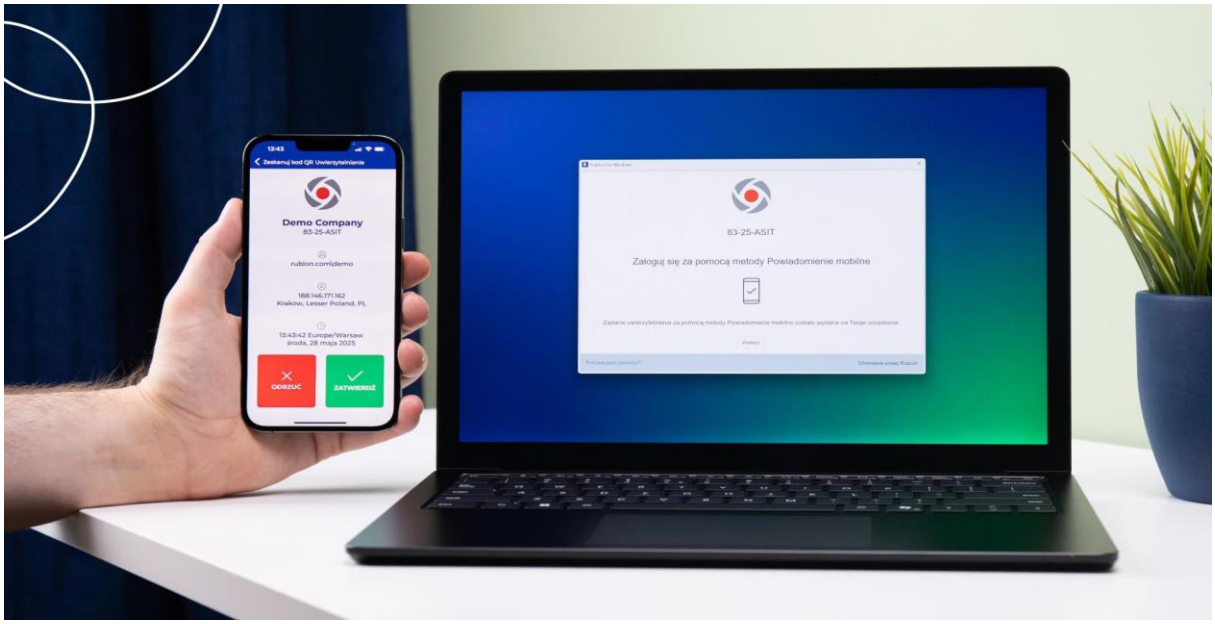
65-036 Zielona Góra

NIP: 9730702133, KRS: 0000003011

www.rublon.pl

Spis treści

Firma **Rublon sp. z o.o.** z siedzibą w Zielonej Górze, ul. Stanisława Wyspiańskiego 11, kod pocztowy 65-036, NIP: 9730702133, KRS: 3011 (dalej „Partner PWCyber"), udziela Ministerstwu Cyfryzacji zgody na wykorzystanie i publikację materiałów przekazanych w ramach Programu PWCyber (zwanych dalej „Materiałami", w szczególności: tekstów, grafik, diagramów, infografik, prezentacji oraz innych treści edukacyjnych. Partner oświadcza, że materiały nie naruszają praw osób trzecich.



Wprowadzenie

Niniejszy dokument to kompleksowy poradnik na temat wdrażania MFA skierowany do administratorów i specjalistów IT w podmiotach administracji publicznej, sektorze prywatnym i innych organizacjach objętych krajowym systemem cyberbezpieczeństwa.

W poradniku znaleźć można odpowiedzi na kluczowe pytania związane z planowaniem i realizacją wdrożenia MFA:

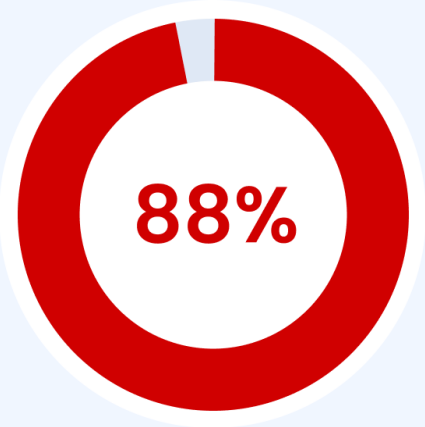
- Jak wybrać dostawcę MFA?
- Jak przygotować organizację do wdrożenia?
- Jak przeprowadzić proces wdrożenia?
- Jak zapewnić ciągłość działania z MFA?

Poradnik zawiera także porównanie zastosowań MFA w środowisku konsumenckim i biznesowym oraz przegląd bezpieczeństwa metod uwierzytelniania. Dodatkowo przedstawiono przykładowy harmonogram wdrożenia, praktyczne listy kontrolne na różnych etapach projektu oraz schematy i tabele podsumowujące najważniejsze informacje.

Co to jest MFA?

Uwierzytelnianie wieloskładnikowe (ang. *multi-factor authentication*, MFA) polega na zastosowaniu co najmniej dwóch niezależnych metod potwierdzania tożsamości użytkownika podczas logowania. Typowo oznacza to połączenie czegoś, co użytkownik **wie** (np. hasło lub PIN), z czymś, co użytkownik **ma** (np. telefon z aplikacją do MFA, klucz sprzętowy) lub czymś, **czym jest** (np. odcisk palca, inna cecha biometryczna). Dzięki temu nawet jeśli jeden składnik uwierzytelnienia (np. hasło) zostanie wykradziony lub złamany, atakujący wciąż nie uzyska dostępu do konta bez drugiego składnika. w praktyce MFA znacząco podnosi poziom bezpieczeństwa dostępu do systemów i danych, dlatego warto włączyć ten sposób weryfikacji tożsamości przy logowaniu.

Więcej o tym, czym jest uwierzytelnianie wieloskładnikowe (MFA), jak działa i dlaczego warto je wdrożyć, przeczytasz w naszym artykule: Co to jest uwierzytelnianie wieloskładnikowe (MFA)?



Dlaczego MFA jest ważne?

Raport Verizon DBIR 2025 podaje, że aż 88% ataków na aplikacje webowe polega na wykorzystaniu skradzionych haseł. Zastosowanie MFA pozwala dodać dodatkową linię obrony, która potrafi powstrzymać do 99% ataków polegających na przejęciu konta, nawet jeśli cyberprzestępca zna hasło.

Specjalny rodzaj MFA zwany „odpornym na phishing" utrudnia także ataki phishingowe, w których ofiara może nieświadomie ujawnić swoje hasło na fałszywej stronie. Krótko mówiąc, wdrożenie MFA jest dziś jedną z najskuteczniejszych metod ochrony przed przejęciem kont i wyciekiem danych w organizacjach.

Porównanie MFA konsumenckiego z biznesowym

Zanim zacznie się myśleć o wdrożeniu MFA, warto zrozumieć różnicę między uwierzytelnianiem wieloskładnikowym stosowanym przez indywidualnych użytkowników (np. przy logowaniu do poczty, mediów społecznościowych czy banku) a wdrożeniem MFA w środowisku firmowym lub instytucjonalnym. Choć zasada działania jest ta sama, kontekst użycia MFA konsumenckiego i biznesowego różni się pod kilkoma względami.

Aspekt	MFA konsumenckie	MFA biznesowe
Inicjatywa wdrożenia	Dobrowolna. Użytkownik chce włączyć MFA, aby podnieść poziom bezpieczeństwa konta.	Odgórna. Organizacja musi wdrożyć MFA, aby podnieść poziom bezpieczeństwa i uzyskać zgodność regulacyjną.
Wymagalność	Zazwyczaj użytkownik sam aktywuje MFA na swoich kontach. Wyjątkiem są banki, gdzie MFA jest obowiązkowe z mocy prawa.	Wymuszane polityką bezpieczeństwa firmy, np. każdy pracownik musi używać MFA przy logowaniu do wybranych systemów.
Metody uwierzytelnienia	Ograniczone do najprostszych: najczęściej SMS, e-mail lub aplikacja mobilna (TOTP). Rzadziej klucze sprzętowe i passkeys.	Szeroki wachlarz metod: od kodów SMS/TOTP, przez powiadomienia push, klucze FIDO i passkeys, po kody QR. Wybór zależy od potrzeb organizacji.
Zarządzanie	Brak centralnego zarządzania. Każdy serwis oferuje własną funkcję MFA, a użytkownik konfiguruje ją oddzielnie dla każdego konta.	Centralne zarządzanie, np. za pomocą konsoli administracyjnej. Wspólne dla wszystkich pracowników i aplikacji w firmie rozwiązanie MFA zintegrowane z katalogiem użytkowników (np. Active Directory), umożliwiające adminom egzekwowanie ustawień i polityk bezpieczeństwa oraz monitorowanie użycia.

Aspekt	MFA konsumenckie	MFA biznesowe
Wsparcie i odzyskiwanie	Ograniczone. w przypadku zgubienia drugiego składnika uwierzytelniania (np. telefonu), użytkownik polega na procedurze danego serwisu (np. kontakt z działem pomocy usługi).	Rozbudowane. Organizacja definiuje procesy odzyskiwania dostępu (np. wydawanie kodów zapasowych, pomoc działu IT organizacji przy utracie telefonu, konta awaryjne dla administratorów, definiowanie więcej niż jednej dozwolonej metody uwierzytelniania).
Skala	Pojedynczy użytkownik zabezpiecza kilka swoich kont.	Skala masowa. Wdrożenie obejmuje dziesiątki, setki, a nawet tysiące kont pracowników i systemów firmowych jednocześnie, co wymaga dokładnego zaplanowania.
Cel i zakres ochrony	Ochrona prywatnych danych użytkownika (e-mail, profile w mediach społecznościowych, finanse) przed przejęciem przez osoby niepowołane.	Ochrona zasobów organizacji (danych w systemach wewnętrznych, aplikacji biznesowych, usług w chmurze) oraz spełnienie wymogów bezpieczeństwa (np. zgodność z normami, rekomendacjami audytowymi). Często MFA jest elementem szerszej strategii podniesienia poziomu bezpieczeństwa w firmie.

Aspekt	MFA konsumenckie	MFA biznesowe
Przykłady wdrożeń	Gmail czy Facebook, gdzie użytkownik sam włącza i konfiguruje MFA na swoim koncie. Dostęp do bankowości elektronicznej to najczęściej MFA w postaci logowania hasłem oraz wpisania jednorazowego kodu SMS.	Dostęp do sieci firmowej wymaga loginu i hasła oraz potwierdzenia w aplikacji mobilnej. Dostęp administratorów do krytycznych serwerów firmy wymaga oprócz hasła również uwierzytelnienia kluczem sprzętowym FIDO. Logowanie pracowników do aplikacji wykorzystywanej w firmie wymaga MFA (kod z telefonu lub powiadomienie push).

Wdrożenie MFA w środowisku biznesowym jest znacznie bardziej złożonym przedsięwzięciem niż prosta konfiguracja MFA przez użytkownika indywidualnego. w organizacji trzeba zadbać o:

- Wybór odpowiedniego rozwiązania technicznego (spełniającego wymagania bezpieczeństwa i integrującego się z istniejącą infrastrukturą IT).
- Proces wdrożenia (etapowy, minimalizujący zakłócenia pracy).
- Utrzymanie i obsługę rozwiązania (obsługę użytkowników, rotację urządzeń, ciągłość działania).

Ten poradnik koncentruje się na zorganizowanym, centralnym wdrożeniu MFA w organizacji.

Dowiedz się, jak Rublon MFA wspiera zgodność z regulacjami, chroni dostęp do danych i integruje się z kluczowymi systemami IT — poznaj konkretne przypadki użycia w różnych środowiskach organizacyjnych.

Wybór dostawcy MFA – na co zwrócić uwagę?

Pierwszym krokiem projektu wdrożenia MFA jest wybór odpowiedniego rozwiązania i dostawcy. Na rynku dostępnych jest wiele platform MFA, więc kluczowe jest wybranie systemu, który spełni wymagania organizacji pod względem bezpieczeństwa, zgodności z przepisami, funkcjonalności oraz użyteczności.

Wybór dostawcy MFA to strategiczna decyzja, ponieważ wybrane rozwiązanie będzie stanowić kluczowy element infrastruktury bezpieczeństwa. z tego powodu warto poświęcić czas na rzetelną ocenę każdego rozwiązania. Nie należy kierować się wyłącznie ceną czy popularnością marki; najważniejsze jest dopasowanie do konkretnych wymogów organizacji. Poniżej omawiamy najważniejsze kryteria wyboru dostawcy MFA.

Bezpieczeństwo i zgodność ze standardami

Należy upewnić się, że rozwiązanie MFA wykorzystuje sprawdzone mechanizmy kryptograficzne do ochrony danych uwierzytelniających (sekretów, kluczy), np. hasła jednorazowe oparte na czasie zgodne ze specyfikacją RFC 6238, klucze prywatne przechowywane w bezpiecznym module itp.

Dostawca powinien zapewniać zgodność z branżowymi standardami takimi jak FIDO2 (nowoczesne uwierzytelnianie odporne na phishing) oraz posiadać certyfikaty zgodności z normami (np. ISO 27001 dla bezpieczeństwa informacji). Warto również sprawdzić, czy rozwiązanie spełnia wymagania poziomu AAL[1]2 oraz AAL3 według wytycznych NIST (wyższe poziomy Authenticator Assurance Level są zalecane dla wrażliwych systemów).

Warto dowiedzieć się, czy dostawca umożliwia wdrożenie uwierzytelniania wieloskładnikowego odpornego na phishing. Metody zgodne ze standardami FIDO U2F oraz FIDO2 są obecnie uznawane za złoty standard bezpieczeństwa. Należy unikać rozwiązań oferujących tylko i wyłącznie przestarzałe lub podatne na ataki metody (np. tylko kody SMS lub tylko kody TOTP). Nie wszystkie formy MFA są równie bezpieczne, np. podstawowe MFA oparte na SMS-ach jest narażone na ataki polegające na podmianie karty SIM (*ang. SIM swap*).

Dowiedz się, jak Rublon MFA pomaga spełnić wymogi bezpieczeństwa i regulacji.

[1] Authenticator Assurance Level - kategoria opisująca poziom bezpieczeństwa procesu uwierzytelniania.

Obsługiwane metody uwierzytelniania

Należy zwrócić uwagę, jakie metody MFA wspiera dany dostawca i czy pokrywają się one z potrzebami organizacji. Minimalny zestaw to zazwyczaj: kody jednorazowe (OTP) w aplikacji mobilnej, kody SMS i powiadomienia push na telefon. Coraz częściej pożądane jest też wsparcie dla kluczy bezpieczeństwa FIDO U2F & FIDO2 (np. YubiKey) oraz sprzętowych lub programowych passkeys zapisywanych na przykład na komputerze pracownika lub na jego koncie w Google Password Manager.

Dobre platformy MFA pozwalają administrować politykami doboru metod. Dzięki takiej funkcjonalności można wymuszać silniejsze metody odporne na phishing podczas logowania administratorów i jednocześnie dopuszczać inne metody dla pracowników logujących się do aplikacji o mniejszym wskaźniku zagrożenia (np. metoda SMS dla pracowników bez smartfonów logujących się do aplikacji, w której nie są przechowywane żadne znaczące dane). Takie podejście pozwala zachować balans między bezpieczeństwem a wygodą użytkowania.

Przykładowo, rozwiązanie Rublon MFA umożliwia jednoczesne wykorzystanie różnych metod - od notyfikacji push, przez logowanie za pomocą kluczy FIDO2, aż po logowanie kodami TOTP - co pozwala dostosować strategię MFA do różnych poziomów ryzyka i typów użytkowników.

Dowiedz się, jakie metody uwierzytelniania obsługuje Rublon MFA.

Elastyczność w doborze metod również jest istotna. Różne scenariusze (logowanie do VPN, do poczty w chmurze, zdalnie do systemów Windows i Linux, itp.) mogą wymagać odmiennych metod uwierzytelniania. Warto sprawdzić czy rozpatrywane rozwiązanie pozwala na taką elastyczność oraz czy pozwala na zarejestrowanie wielu urządzeń dla jednego konta (np. aplikacja na telefon służbowy, na telefon prywatny jako backup oraz klucz FIDO).

Integracja z istniejącą infrastrukturą

Rozwiązanie MFA nie działa w próżni, lecz musi zostać zintegrowane z systemami i aplikacjami, które organizacja chce chronić. Dlatego należy dowiedzieć się, czy dostawca wspiera konkretne technologie wykorzystywane w organizacji, na przykład:

- Import i synchronizacja użytkowników z usług katalogowych pokroju Active Directory i Entra ID.
- Wsparcie dla protokołów SAML, LDAP i RADIUS do zintegrowania aplikacji webowych i sieci VPN.
- Dostępność usługi logowania jednokrotnego (ang. *Single Sign-On, SSO*).
- Natywne konektory dla technologii Microsoft typu Windows Logon, RDP, Remote Desktop Gateway, Remote Desktop Web Access, Remote Desktop Web Client, Outlook Web App (OWA) i Active Directory Federation Services (AD FS).

Im więcej wspieranych technologii, protokołów i natywnych integracji, tym łatwiej będzie wdrożyć MFA w organizacji. Należy też sprawdzić, czy dostawca oferuje interfejsy API oraz gotowe biblioteki SDK. Tego typu narzędzia są przydatne, jeśli organizacja planuje włączyć mechanizmy MFA we własnych aplikacjach biznesowych czy portalach klientów.

Przykładem takiego elastycznego rozwiązania może być rozwiązanie Rublon MFA, które oferuje gotowe konektory do usług Microsoft (m.in. AD FS, OWA, Windows Logon, RDP), integracje SAML i RADIUS, a także REST API umożliwiające wdrożenie MFA we własnych aplikacjach webowych i mobilnych.

Dowiedz się, jak Rublon MFA integruje się z Windows, Active Directory, SAML, LDAP, RADIUS i innymi systemami.

Łatwe zarządzanie użytkownikami i urządzeniami

Jednym z kluczowych aspektów przy wyborze rozwiązania MFA jest łatwość zarządzania cyklem życia użytkowników i ich metod uwierzytelniania. Warto dowiedzieć się, czy rozważana platforma MFA umożliwia automatyczną rejestrację użytkowników, czyli czy mogą być dodawani w platformie od razu przy pierwszym udanym logowaniu do zabezpieczonej technologii. Jeśli dostawca wspiera synchronizację katalogów, warto dopytać czy nowe konta w domenie będą się pojawiać w platformie MFA zaraz po synchronizacji.

Warto też zwrócić uwagę, jak wygląda proces rejestracji nowych urządzeń przez użytkowników (ang. *device enrollment*), czyli czy odbywa się samoobsługowo za pomocą intuicyjnego portalu rejestracji urządzeń, czy wymaga ręcznej pracy administratora. Wysłanie maila do użytkownika z linkiem do rejestracji urządzenia jest wartościową trzecią opcją.

Dowiedz się, jak Rublon automatycznie synchronizuje konta użytkowników z Active Directory i Entra ID (Directory Sync).

Wygoda użytkownika

Uwierzytelnianie wieloskładnikowe dodaje nowy krok do logowania, więc warto upewnić się, że ten dodatkowy etap nie jest zbyt uciążliwy dla pracowników. Warto porównać wygodę korzystania

z różnych proponowanych metod, zadając następujące pytania:

- Czy aplikacja mobilna dostawcy jest przyjazna, w języku polskim i czy działa na popularnych mobilnych systemach operacyjnych?
- Czy powiadomienia push są zatwierdzane jednym dotknięciem oraz czy istnieje możliwość ich dodatkowego zabezpieczenia za pomocą odcisku palca lub skanu twarzy?
- Czy interfejs logowania jest spójny, pozwala spersonalizować komunikaty dla użytkowników oraz oferuje różnorodne metody uwierzytelniania dostosowane do poziomu zaawansowania technicznego, wyposażenia sprzętowego i indywidualnych preferencji użytkowników?

Im prostszy i bardziej zrozumiały dla użytkowników końcowych proces uwierzytelnienia, tym mniej oporu przy wdrożeniu. Warto zapytać dostawcę o materiały edukacyjne dla użytkowników: czy udostępnia dokumentację, przewodniki, samouczki, filmy demo działania MFA. Tego typu materiały ułatwią sprawne wprowadzenie rozwiązania w organizacji.

Dowiedz się, jak funkcja „Zapamiętane urządzenia" w Rublon MFA zwiększa wygodę użytkowników.

Wymagania techniczne i skalowalność

Należy przeanalizować architekturę rozwiązania MFA:

- Czy jest to polski dostawca znający lokalny rynek i potrzeby klientów?
- Czy jest to rozwiązanie lokalne (ang. *on-premise*), czy usługa chmurowa działająca w modelu „oprogramowanie jako usługa" (ang. *Software as a Service*, SaaS)?
- Jeśli to usługa chmurowa, czy dane przechowywane są na terenie Unii Europejskiej? Może mieć to znaczenie dla zgodności regulacyjnej.
- Jakie są wymagania sprzętowe, kompatybilność systemowa oraz czy potrzebne są dodatkowe serwery (np. serwer proxy)?
- Czy rozwiązanie poradzi sobie z przewidywaną liczbą użytkowników i logowań, np. setkami jednoczesnych uwierzytelnień w godzinach szczytu?

- Czy system pozwala łatwo dodać kolejne aplikacje, użytkowników, polityki bezpieczeństwa i metody uwierzytelniania w miarę rozwoju potrzeb organizacji?

Dowiedz się, jakie są wymagania techniczne Rublon MFA.

Audyt i zgodność

Dla organizacji ważne jest mieć podgląd kto, kiedy, gdzie i z jakiego urządzenia loguje się z użyciem MFA. Dlatego warto dowiedzieć się, czy platforma oferuje dzienniki zdarzeń uwierzytelniania, które można wyeksportować w celu dalszego przetwarzania, np. w rozwiązaniach SIEM.

Ponadto, w kontekście zgodności z regulacjami, należy sprawdzić czy rozwiązanie dostawcy wspiera wymogi ogólnych regulacji bezpieczeństwa, takich jak RODO, dyrektywa NIS2, ustawa o KSC, a także bardziej specjalistycznych wytycznych dla konkretnej branży, np. dla instytucji finansowych będzie to rozporządzenie DORA oraz wytyczne Komisji Nadzoru Finansowego (KNF). w sektorze publicznym istotne są rekomendacje krajowych instytucji, np. certyfikacje NASK i listy rekomendowanego oprogramowania. Warto zweryfikować, czy dany produkt MFA jest już stosowany w innych instytucjach.

Dowiedz się, jak działają Dzienniki uwierzytelniania, audytu i telefoniczne w Rublon MFA.

Wsparcie techniczne i koszty

Przy wyborze rozwiązania MFA ważna jest ocena modelu wsparcia oferowanego przez dostawcę. Szybka pomoc i wsparcie w razie problemów czy pytań są nieocenione, dlatego warto zwrócić uwagę, czy wsparcie techniczne jest dostępne w standardowych godzinach pracy w Polsce. Istotne jest też świadczenie wsparcia w języku polskim, ponieważ znacznie ułatwia i przyspiesza to komunikację.

Poza wsparciem technicznym, ważnym aspektem są też koszty rozwiązania. Należy przeanalizować model licencjonowania i koszty oraz porównać je do jakości rozwiązania. Najtańsza opcja nie zawsze jest optymalna. Kluczowe jest dopasowanie rozwiązania do możliwości finansowych. Koszty mogą być naliczane za użytkownika lub za licencję i rozliczane w formie miesięcznych lub rocznych opłat subskrypcyjnych. Czasem dostępne są również licencje wieloletnie, a nawet wieczyste - warto dowiedzieć się, jak to dokładnie działa w przypadku konkretnego dostawcy, którego rozwiązanie jest rozważane.

Należy pamiętać, by podczas analizy uwzględnić również ukryte koszty, na przykład:

- Koszt zakupu dodatkowych urządzeń (klucze FIDO, telefony służbowe).
- Opłaty telekomunikacyjne za metody uwierzytelniania oparte na usługach telefonicznych (np. SMS).
- Koszt utrzymania serwerów on-premise (koszt sprzętu i administrowania).

Dowiedz się, jak działa plan subskrypcji w Rublon MFA.

Wygodna lista kontrolna: Wybór dostawcy MFA

Poniżej znajduje się krótka lista kontrolna najważniejszych pytań, które warto zadać przy wyborze dostawcy MFA. Można ją traktować jako listę kontrolną w trakcie analizy ofert:

- Czy rozwiązanie spełnia wymagane standardy bezpieczeństwa (FIDO2, AAL2/AAL3,, push) i zapewnia odporność na typowe ataki w przestrzeni internetowej (phishing, ransomware, przechwycenie kodów)?
- Jakie metody uwierzytelniania obsługuje dostawca? Czy pokrywają się one z naszymi potrzebami? Czy wspiera klucze sprzętowe FIDO, notyfikacje push, kody w wiadomościach SMS, kody QR, kody offline itp.?
- Czy rozwiązanie integruje się z lokalnym Active Directory, Entra ID, RADIUS, LDAP, SAML, SSO oraz kluczowymi systemami (VPN, poczta, aplikacje biznesowe)? Czy oferuje API/SDK dla niestandardowych integracji?
- Jak wygląda zarządzanie użytkownikami i urządzeniami uwierzytelniającymi? Czy dostępna jest synchronizacja użytkowników, samoobsługowa rejestracja urządzeń, proste procedury resetu i odzyskiwania dostępu?
- Czy interfejs i procesy uwierzytelniania są przyjazne dla użytkowników (aplikacja mobilna, język polski, prostota użycia, wsparcie dla różnych urządzeń użytkownika)?
- Czy architektura rozwiązania pasuje do infrastruktury organizacji? Jakie są wymagania systemowe oraz czy rozwiązanie zapewni wysoką wydajność i dostępność przy konkretnej liczbie użytkowników?
- Jakie możliwości audytowe oferuje dostawca? Czy dzienniki można integrować z rozwiązaniami SIEM? Czy dzięki temu rozwiązaniu można bez problemów spełnić wszystkie wymagania regulacyjne nakładane na organizację?
- Jak wyglądają koszty licencji i utrzymania? Czy w budżecie ujęto wszystkie komponenty (np. zakup kluczy fizycznych, ewentualne koszty SMS)? Jak oceniane jest wsparcie techniczne (dostępność)?
- Czy dostawca i rozwiązanie posiadają pozytywne opinie, szczególnie w sektorze publicznym lub branży podobnej do naszej? Czy inne podmioty KSC już z tego rozwiązania korzystają?

Dowiedz się, dlaczego firmy w Polsce wybierają Rublon MFA jako swoje zaufane rozwiązanie do uwierzytelniania wieloskładnikowego.

Przygotowanie organizacji do wdrożenia MFA

Przygotowania organizacji do wdrożenia MFA dotyczą zarówno strony technicznej, jak i organizacyjnej.

Wdrożenie uwierzytelniania wieloskładnikowego to projekt angażujący zarówno zespół IT, jak i zwykłych pracowników, kierownictwo oraz często również zewnętrznych partnerów i integratorów. Dobre przygotowanie minimalizuje ryzyko przyszłych problemów oraz chaosu podczas pierwszego uruchomienia rozwiązania MFA. Im więcej potencjalnych problemów zostanie rozwiązanych zawczasu, tym płynniej przebiegnie wdrożenie.

Poniżej znajdują się kluczowe kroki do przygotowania organizacji na wdrożenie uwierzytelniania wieloskładnikowego.

Dowiedz się, jakie są najlepsze praktyki wdrażania Rublon MFA.

Uzyskanie wsparcia kierownictwa i ustanowienie polityki bezpieczeństwa

Jeśli jeszcze tego nie zrobiono, należy przedstawić decydentom uzasadnienie biznesowe wdrożenia konkretnego rozwiązania MFA, np.:

- Spełnienie wymogów regulacyjnych.
- Redukcja ryzyka wycieku danych.
- Wskazanie incydentów i rodzajów ataków, którym to rozwiązanie MFA pomoże zapobiec.
- Wskazać zalety tego rozwiązania w porównaniu z innymi.

Poparcie dyrekcji pomoże w egzekwowaniu zmian i późniejszej komunikacji. Równolegle należy opracować lub zaktualizować wewnętrzną politykę bezpieczeństwa określającą zakres stosowania uwierzytelniania wieloskładnikowego:

- Które systemy i zasoby będą objęte MFA?
- Kogo dotyczyć będzie MFA (od razu wszystkich pracowników, czy na początku tylko administrację i działy wrażliwe na ataki hakerskie)?

- Jakie metody powinny być dopuszczalne, a jakie zakazane (np. można ustalić, że metody SMS są tymczasowo akceptowalne, ale długofalowo wymagana będzie migracja na aplikację mobilną lub klucze FIDO)?
- Kiedy ostatecznie zostanie wprowadzone obowiązkowe MFA według powyższych wytycznych?

„Wdrożenie MFA to strategiczna inwestycja w cyberodporność organizacji. Sukces takiego projektu wymaga aktywnego zaangażowania zarządu oraz spójnej, jasno określonej polityki bezpieczeństwa. Bez tych fundamentów nawet najnowocześniejsze technologie nie przełożą się na realne wzmocnienie ochrony danych i usług."

Michał Wendrowski, Prezes zarządu spółki Rublon

Inwentaryzacja systemów i analiza wymagań

Należy sporządzić listę wszystkich systemów, aplikacji i usług, w których planuje się wdrożyć MFA wraz z informacjami jak to zrobić. Na tym etapie wiemy już, że wdrożenie jest możliwe. Teraz musimy zebrać jak najwięcej konkretnych informacji odnośnie dokładnych kroków wdrożenia. Kluczowa jest współpraca z dostawcą MFA lub integratorem, aby zaplanować konfigurację MFA dla wszystkich wymaganych zasobów w organizacji.

Dla każdego zidentyfikowanego obszaru należy ustalić, jak technicznie wdrożyć MFA:

- Czy istnieje dokumentacja integracji na stronie dostawcy?
- Czy wymagana jest integracja przez protokół RADIUS/LDAP/SAML?
- Czy wymagane jest użycie agenta/konektora (np. proxy RADIUS do VPN)?
- Czy wymagana jest instalacja modułu/konektora/pluginu?
- Czy możliwa jest automatyzacja masowego wdrożenia na wielu stacjach roboczych lub serwerach jednocześnie?

Przykład: Jeśli pracownicy łączą się z pulpitami zdalnymi (RDP), należy sprawdzić, w jaki sposób można zabezpieczyć ten dostęp wybranym rozwiązaniem. Czy rozwiązanie MFA oferuje dedykowany konektor do RDP, czy jest to integracja wykonywana w inny sposób? Jeśli w organizacji są systemy legacy nieobsługujące nowoczesnych metod, należy sprawdzić jak rozwiązanie pozwala na ich zabezpieczenie w inny sposób (np. dostęp tylko poprzez VPN zabezpieczony MFA, zamiast bezpośrednio).

Przygotowanie środowiska testowego

Zanim uwierzytelnianie MFA zostanie włączone w środowisku produkcyjnym, warto przygotować środowisko testowe odzwierciedlające kluczowe elementy infrastruktury produkcyjnej. Może to być oddzielna instancja usługi Active Directory z kilkoma kontami testowymi wraz ze sklonowanymi instancjami najważniejszych aplikacji z produkcji. Zainstalowanie i konfiguracja rozwiązania MFA w warunkach kontrolowanych na środowisku testowym pozwoli zweryfikować integrację (np. sprawdzić czy logowanie do VPN działa poprawnie z naszą aktualną konfiguracją), a także oswoić się ze sposobem działania i zarządzania rozwiązaniem.

Jeżeli nie ma możliwości stworzenia oddzielnego środowiska testowego, warto rozważyć przynajmniej testy na ograniczonej grupie rzeczywistych kont (np. dział IT) w trybie nieinwazyjnym. Jeśli wybrane rozwiązanie posiada możliwość włączenia MFA tylko dla wybranych użytkowników w taki sposób, że pozostali użytkownicy logują się tak jak dotąd, bez zauważalnych zmian, to należy wykorzystać ten tryb podczas testów.

Harmonogram wdrożenia

Należy przygotować wstępny harmonogram wdrożenia. Już na etapie przygotowań warto rozrysować sobie wstępnie fazy wdrożenia. Trzeba wyznaczyć czas na pilotaż, na ewentualne dostosowanie konfiguracji, na kampanię komunikacyjną, oraz na wsparcie użytkowników po wdrożeniu.

Ustalone ramy czasowe powinny być realistyczne i uwzględniać m.in. sezonowość (nie powinno się uruchamiać nowego sposobu logowania tuż przed świętami lub w okresie zamknięcia roku budżetowego, gdy dział IT ma inne obciążenia). Jeżeli potrzebne jest wykonanie dłuższej konfiguracji czy wdrożenia (np. instalacja i dostosowanie jakiejś usługi), należy uwzględnić czas na konfigurację i testy. Harmonogram powinien być uzgodniony z najważniejszymi interesariuszami, np. kierownikami działów, których pracownicy będą objęci pilotażem.

Przygotowanie zasobów i narzędzi

Należy upewnić się, że dostępne są wszystkie niezbędne zasoby do realizacji projektu:

- Dostępne są serwery i instancje do zainstalowania komponentów MFA.
- Skonfigurowane są połączenie sieciowe między elementami systemu (np. jeśli używane jest chmurowe MFA, zapory sieciowe muszą przepuszczać ruch do chmury, a konektory muszą swobodnie móc się komunikować z bazą tożsamości użytkowników).
- Urządzenia, takie jak sprzętowe klucze bezpieczeństwa FIDO, muszą zostać zamówione z odpowiednim wyprzedzeniem, aby zdążyły dotrzeć i by można je było rozdysponować pracownikom na czas.
- Pod ręką dostępna jest dokumentacja techniczna rozwiązania. Warto ją przejrzeć jeszcze przed rozpoczęciem wdrożenia i oznaczyć ważne sekcje, aby w trakcie konfiguracji mieć je zawsze pod ręką. w razie jakichkolwiek niepewności warto skonsultować się z dostawcą rozwiązania.

Polityka obsługi wyjątków i sytuacji awaryjnych

Już na etapie planowania warto ustalić, jakie wyjątki od wymogu MFA będą dopuszczalne i w jakich sytuacjach. Należy się również zastanowić, jakie wyjątki od globalnych polityk MFA mogą zaistnieć w organizacji. Przykłady:

- Czy konta usługowe, użytkownicy zewnętrzni i goście powinni zostać objęci MFA? Jeśli tak, to czy w taki sam sposób jak zwykli pracownicy, czy powinno zostać zastosowane inne podejście?
- Czy pozwolić pracownikom nieposiadającym służbowych telefonów na korzystanie z telefonów prywatnych, czy może umożliwić im korzystanie z metod uwierzytelniania niewymagających telefonu?

Warto spisać procedurę awaryjnego dostępu (ang. *break-glass*), tzn. co zrobić, jeśli ktoś utraci dostęp (np. zgubi telefon i nie ma kodów zapasowych) lub gdy system MFA ulegnie awarii. Takie procedury omówione zostaną szerzej w dalszej części poradnika, ale już teraz można zaplanować ich zarys.

Kampania informacyjna i materiały edukacyjne

Wdrożenie MFA dotknie wielu pracowników, dlatego kluczowe jest ich odpowiednie poinformowanie i przeszkolenie. Już na etapie przygotowań warto ustalić, kiedy i jak zostaną zakomunikowane pracownikom nadchodzące zmiany. Można też zapytać dostawcę MFA, czy oferuje gotowe materiały do komunikacji z użytkownikami końcowymi.

Dobrą praktyką jest przygotowanie wewnętrznej listy najczęstszych pytań i odpowiedzi oraz instrukcji dla pracowników, np. prostego poradnika „Jak skonfigurować swoje urządzenie uwierzytelniające do MFA krok po kroku". Być może wystarczą tutaj materiały udostępnione przez dostawcę MFA, ale przygotowanie wewnętrznej instrukcji dostosowanej do konkretnych aplikacji stosowanych w firmie to dobry pomysł.

Można też stworzyć krótkie prezentacje edukacyjne dla pracowników pokazujące, dlaczego organizacja wprowadza MFA (podkreślając istotność ochrony kont pracowników i danych firmy) oraz jak będzie wyglądał nowy proces logowania.

Warto przygotować różne kanały komunikacji z pracownikami: e-mail od działu bezpieczeństwa, ogłoszenie na intranecie, spotkanie lub webinar Q&A dla pracowników, plakaty w biurze, itp. Część materiałów może dostarczyć sam dostawca MFA (warto zapytać o gotowe szablony komunikatów, przewodniki). Wtedy pozostanie tylko dostosować je do wewnętrznych realiów (np. dodać informację, z kim się kontaktować w razie pytań).

Szkolenie zespołu wsparcia IT

Ważne jest przygotowanie działu zespołu wsparcia IT na nadchodzące wdrożenie. Pracownicy IT pierwszej linii muszą znać mechanizmy MFA, aby skutecznie pomagać użytkownikom. Warto zatem zorganizować dla nich dedykowane szkolenie z działania nowego systemu: jak rejestrować użytkowników i ich urządzenia, jak używać konta awaryjnego, jak zweryfikować tożsamość dzwoniącego pracownika, zanim wyłączy mu się MFA (żeby nie powstała luka socjotechniczna).

Dobrą praktyką jest stworzenie procedur obsługi typowych zgłoszeń: *„zgubiłem telefon"*, *„nie mogę się zalogować"*, *„nie dochodzi do mnie SMS z kodem"*, *„aplikacja mobilna pokazuje błędny kod"*, itp.

Dobrą praktyką jest też wyznaczenie kilku osób w firmie (najlepiej z działu IT lub bezpieczeństwa), które będą dodatkowym wsparciem merytorycznym i będą odpowiadać na trudniejsze pytania oraz przyjmować sugestie użytkowników w trakcie wdrożenia.

Dowiedz się, jak zarządzać platformą Rublon MFA w konsoli administracyjnej.

Wygodna lista kontrolna: Przygotowanie organizacji do wdrożenia MFA

Poniżej znajduje się krótka lista kontrolna odnośnie przygotowania organizacji do wdrożenia MFA. Dopiero mając spełnione poniższe punkty, należy przejść do właściwego wdrażania MFA w środowisku produkcyjnym.

- **Polityka MFA i zakres wdrożenia:**
  - Kierownictwo zatwierdziło wdrożenie MFA.
  - Określono które systemy i którzy użytkownicy zostaną objęci MFA.
  - Określono termin wdrożenia MFA.
- **Lista systemów i integracji:**
  - Sporządzono inwentaryzację aplikacji/usług do zabezpieczenia przez MFA.
  - Zweryfikowano techniczne możliwości integracji dla każdej pozycji (w razie braków określono plan alternatyw).
- **Testy:**
  - Przygotowano środowisko testowe do przeprowadzenia próbnej instalacji i konfiguracji MFA.
  - Zaplanowano wstępne testy integracji w kontrolowanych warunkach.
- **Plan projektu i harmonogram:**
  - Ustalono etapy wdrożenia (pilot, komunikacja, migracja etapami, go-live).
  - Oszacowano ramy czasowe i kluczowe daty.
  - Rozdzielono odpowiedzialność za zadania.
- **Zabezpieczenie zasobów technicznych:**
  - Dostępna jest infrastruktura (serwery, oprogramowanie).
  - Zamówiono potrzebne urządzenia (np. klucze sprzętowe).
  - Sprawdzono, że warunki sieciowe i konfiguracja pozwolą na bezproblemowe wdrożenie (np. otwarto porty, dodano wyjątki do zapory).
- **Procedury wyjątków i awaryjne:**
  - Opracowano plan postępowania dla kont uprzywilejowanych, kont serwisowych, sytuacji zgubienia telefonu przez użytkownika.
  - Wyznaczono konta awaryjne dla administratorów.
- **Materiały komunikacyjne i szkoleniowe:**
  - Przygotowano komunikaty do pracowników (maile, ogłoszenia).
  - Stworzono instrukcje dla użytkowników (lub zaadaptowano gotowe od dostawcy) opisujące jak zarejestrować urządzenie uwierzytelniające i jak używać MFA.
- **Przeszkolenie zespołu IT oraz helpdesk:**
  - Przygotowano szkolenie dla zespołu wsparcia z obsługi nowego systemu.

- Materiały referencyjne są dostępne na wyciągnięcie ręki (wewnętrzna baza wiedzy).
- Wyznaczony personel jest gotowy na pytania użytkowników.

Przeprowadzenie wdrożenia MFA – poszczególne etapy i dobre praktyki

Wdrożenie MFA w organizacji powinno być realizowane stopniowo i metodycznie. Poniżej opisany został zalecany przebieg wdrożenia podzielony na etapy, wraz z najlepszymi praktykami dla każdego z nich. Podejście etapowe pozwala na wychwycenie ewentualnych problemów w małej skali (pilot), adaptację konfiguracji, stopniowe przyzwyczajenie użytkowników do nowej formy uwierzytelniania oraz zapewnienie ciągłości działania. Konkretne kroki można dostosować do specyfiki organizacji.

Mała organizacja może część z nich skrócić lub nawet pominąć, ale generalna zasada brzmi: zacznij od małej liczby użytkowników, testuj, wyciągaj wnioski, komunikuj i dopiero potem skaluj na całą firmę.

Przeprowadzenie pilotażu

Pierwszym etapem wdrożenia produkcyjnego powinien być program pilotażowy. Polega on na uruchomieniu MFA dla ograniczonej grupy użytkowników i systemów w celu przetestowania rozwiązania w praktyce, zebrania opinii i wprowadzenia ewentualnych poprawek przed globalnym wdrożeniem.

Pilotaż pozwala dostosować rozwiązanie MFA do realnych warunków użytkowania i wyłapać techniczne niuanse. Dobrze przeprowadzone wdrożenie pilotażowe ułatwi późniejsze wdrożenie właściwe. Wdrożenie pilotażowe wydłuża co prawda ogólny czas wdrożenia, ale czas zwraca się w postaci sprawniejszego wdrożenia na całe przedsiębiorstwo.

Dowiedz się, jak bezpiecznie przetestować Rublon MFA w środowisku produkcyjnym.

„Pilotaż to idealny moment, by zidentyfikować potencjalne problemy już na starcie, zanim wpłyną na całą organizację. Nasze doświadczenie z wdrażania Rublon MFA u setek klientów pokazuje, że starannie zaplanowana faza testowa pozwala precyzyjnie dopasować metody i polityki uwierzytelniania wieloskładnikowego do rzeczywistych potrzeb organizacji.”

Patryk Suchorowski, Architekt rozwiązań IT w Rublon

Oto zalecenia i najlepsze praktyki dotyczące pilotażu:

- **Wybór grupy pilotowej**. Należy starannie dobrać uczestników pilota. Najczęściej zaczyna się od działu IT i bezpieczeństwa, ponieważ pracownicy z wiedzą techniczną mają większą świadomość zagrożeń i dzięki temu bardziej pozytywne podejście do idei wdrożenia MFA w organizacji. Oprócz pracowników z wiedzą techniczną, warto zaangażować przedstawicieli różnych działów (np. po 1-2 osoby z HR, finansów, marketingu). Pozwoli to przetestować uwierzytelnianie wieloskładnikowe w różnych kontekstach pracy. Grupa pilotowa nie powinna być zbyt liczna (np. 5-10% pracowników, w zależności od wielkości firmy), ale na tyle różnorodna, aby dać pełen obraz. Ważne jest, by do pilota dobrowolnie zgłosili się chętni lub byli to pracownicy o pozytywnym nastawieniu do wdrożenia.
- **Ograniczony zakres systemów.** w pilotażu nie trzeba zabezpieczyć od razu wszystkich zasobów. Należy wybrać 2-3 kluczowe systemy i przeprowadzić na nich test MFA. Na przykład, w pilotażu można uwzględnić zabezpieczenie sieci VPN oraz dostępu do komputerów z systemem Windows, ale już zabezpieczenie konkretnych aplikacji używanych w firmie zostawić na później. Mniejszy zakres oznacza łatwiejsze **rozwiązanie ewentualnych problemów i błędów.**
- **Wsparcie i komunikacja podczas pilota**. Uczestnicy pilota powinni mieć zapewnione dedykowane wsparcie, np. bezpośredni kontakt do zespołu wdrożeniowego. Należy ich zachęcać do zgłaszania uwag, problemów i pytań. Dobrą praktyką jest stworzenie grupy dyskusyjnej, gdzie uczestnicy pilota będą mogli dzielić się wrażeniami, a zespół IT szybko zareaguje.
- **Testowanie scenariuszy i zbieranie wyników**. w trakcie pilotażu należy przeprowadzić testy różnych scenariuszy: logowanie z biura, logowanie z domu w przypadku pracy zdalnej, zmiana metody uwierzytelniania, logowanie w trybie offline (jeśli jest wspierane), procedura odzyskiwania dostępu (np. symulacja zgubienia telefonu u jednego z pracowników, by sprawdzić jak szybko helpdesk przywróci mu dostęp). Po zakończeniu pilotażu, warto zebrać opinie uczestników: co im się podobało, co było kłopotem, czy czują się lepiej zabezpieczeni, co by usprawnili.
- **Udoskonalanie konfiguracji**. Na podstawie wyników pilota, należy wprowadzić ewentualne poprawki do ustawień MFA. Może obejmować to zmodyfikowanie polityki bezpieczeństwa, dodanie kolejnej metody uwierzytelniania, czy poprawienie komunikatów wsparcia technicznego do użytkowników. Lepiej wyłapać i poprawić takie szczegóły w pilocie niż dopiero przy masowym wdrożeniu.

Szersze wdrożenie etapowe

Po pomyślnym zakończeniu pilotażu (cele zostały osiągnięte, użytkownicy zaakceptowali rozwiązanie, konfiguracja jest dopracowana), można przystąpić do rozszerzenia wdrożenia MFA na kolejne grupy użytkowników, aplikacje i systemy. Wdrożenie etapowe jest szczególnie zalecane dla większych firm, w których wdrożenie hurtowe mogłoby doprowadzić do przeciążenia działów IT i wsparcia technicznego.

Oto najważniejsze rekomendacje i dobre praktyki związane z wdrożeniem etapowym:

- **Etapy wg podatności**. Warto w pierwszej kolejności wdrożyć MFA dla kont najbardziej narażonych na ataki: administratorów IT, osób z dostępem do krytycznych danych (np. kadra zarządzająca, dział finansowy) oraz pracowników zdalnych. Następnie można stopniowo włączać MFA dla działów i pracowników mniej wrażliwych. Pozwala to skoncentrować wsparcie i przekaz informacyjny na mniejszych grupach, zamiast obciążać helpdesk obsługą wszystkich pracowników naraz.
- **Etapy wg aplikacji**. w niektórych organizacjach bardziej sensowny od podziału wdrożenia na pracowników może być podział na aplikacje. Można wtedy włączać MFA w kolejnych aplikacjach jedna po drugiej. Na przykład, w pierwszej fazie zabezpieczyć logowanie do sieci VPN i aplikacji krytycznych, w drugiej systemy kadrowe i finansowe, a w trzeciej wszystkie pozostałe aplikacje. Ten model sprawdza się, gdy pewne systemy lub aplikacje są bardziej krytyczne od innych i wymagają pierwszeństwa. Jeśli jakieś aplikacje są trudniejsze technicznie do integracji z platformą MFA, można je zostawić na koniec, zdobywając wcześniej doświadczenie na prostszych integracjach. Ważne jest jednak, by nie przeciągać wdrożenia w nieskończoność. Poszczególne etapy powinny następować po sobie w miarę szybko.
- **Monitorowanie postępów**. Podczas wdrożenia etapowego należy stale monitorować metryki: Ilu użytkowników się zarejestrowało? Ilu aktywnie używa MFA? Czy rośnie liczba nieudanych logowań? Warto namierzać pracowników, którzy nadal nie aktywowali MFA. Być może potrzebują indywidualnej pomocy. Na tym etapie wartościowe są okresowe raporty do kierowników działów, np. *„W dziale a już 90% osób korzysta z MFA, a w dziale B tylko 60%, więc prosimy o zachętę z Waszej strony”*. Czasami pracownicy wykonują zadanie dopiero, gdy menedżer powie *„to obowiązek, proszę to zrobić”*.
- **Poszerzanie wdrożenia**. w miarę postępów można dodawać kolejne integracje systemowe, np. po pomyślnym wdrożeniu MFA dla sieci VPN i poczty, warto wprowadzić MFA dla aplikacji chmurowych.

- **Eliminacja mniej bezpiecznych metod**. Jeżeli w początkowych etapach dopuszczaliśmy dla wygody mniej bezpieczne metody (np. SMS), to po pełnym wdrożeniu warto zaplanować zaostrzenie polityki dostępnych metod uwierzytelniania. Takie zmiany należy jednak zakomunikować pracownikom z wyprzedzeniem. Nie powinno się odbierać pracownikom nagle metody, z której korzystają. Najpierw trzeba się upewnić, że mają już działającą alternatywę.

„W sektorze publicznym i regulowanym coraz częściej obserwujemy etapowe wdrożenia MFA, które zaczyna się od kont o krytycznym znaczeniu, a kończy na pełnym pokryciu wszystkich użytkowników i systemów. Taka strategia pozwala ograniczyć ryzyko operacyjne, dając jednocześnie czas na dostosowanie organizacji oraz zapewnienie odpowiedniego wsparcia technicznego."

Przemysław Kucharzewski, Channel Sales Manager w Rublon

Komunikacja i szkolenie użytkowników

Skuteczne wdrożenie MFA zależy w dużej mierze od akceptacji rozwiązania przez pracowników. Dlatego komunikacja i edukacja to krytyczne elementy wdrożenia, które powinny trwać przez cały czas projektu: przed, w trakcie i po wdrożeniu.

Komunikacja to miękki, ale kluczowy element sukcesu wdrożenia. Technologia MFA sama się nie obroni. To ludzie muszą ją zrozumieć i zaakceptować. Włożenie wysiłku w przejrzyste informowanie i szkolenie użytkowników zaowocują mniejszą liczbą problemów i większą skutecznością zabezpieczenia.

Dowiedz się, jak przygotować użytkowników końcowych na wdrożenie Rublon MFA dzięki sprawdzonym szablonom komunikacyjnym.

Oto zalecenia i dobre praktyki dotyczące prowadzenia komunikacji i edukacji pracowników:

- **Wyjaśnienie „dlaczego"**. Warto rozpocząć informowanie pracowników o planach wprowadzenia MFA jak najwcześniej. Ważne jest, aby w pierwszych komunikatach mocno zaakcentować powody i korzyści z wdrożenia MFA, np. „Dbając o bezpieczeństwo naszych systemów i danych klientów, firma wprowadza dodatkowe zabezpieczenie logowania w postaci uwierzytelniania wieloskładnikowego (MFA). Chroni to Was przed skutkami kradzieży haseł. Nawet jeśli ktoś pozna Wasze hasło, nie zaloguje się bez drugiego składnika uwierzytelniania.". Warto przytoczyć proste przykłady (np. „ostatnio wiele firm padło ofiarą ataku, bo złamano hasło pracownika. MFA temu zapobiegnie"), a nawet posłużyć się danymi/statystykami czy rekomendacjami ekspertów (np. „cert.gov.pl radzi stosować MFA wszędzie tam, gdzie to możliwe"). Taki przekaz buduje poczucie sensu u użytkowników.

- **Jasne instrukcje „jak”**. Gdy zbliża się moment wdrożenia, należy zapewnić pracownikom konkretne instrukcje, co będą musieli zrobić. Instrukcja powinna być łatwo dostępna, np. w intranecie, wysłana mailem, wydrukowana jako ulotka. Należy unikać technicznego żargonu i mówić językiem korzyści, np. zamiast: „zarejestruj uwierzytelniacz TOTP” lepiej: „skonfiguruj aplikację generującą kody jednorazowe”. Jeśli to możliwe, warto dodać zrzuty ekranu lub link do krótkiego filmu instruktażowego.
- **Wielokanałowość przekazu**. Ludzie różnie przyswajają informacje, dlatego warto użyć kilku kanałów komunikacji. E-mail to podstawa, ale maili dostaje się dużo, więc maile o MFA powinny się wyróżniać. Przydatne mogą się okazać ogłoszenia na intranetowej stronie głównej, wiadomości na firmowym czacie, drukowane ulotki oraz plakaty na korytarzach z chwytliwym hasłem, np. *„Logowanie 2x bezpieczniejsze – aktywuj MFA do 30 sierpnia!”*.
- **Zaangażowanie kadry kierowniczej**. Warto poprosić menedżerów poszczególnych działów, aby wzmocnili przekaz, np. niech poruszą temat MFA na swoich odprawach zespołów. Często pracownicy uważniej traktują wiadomość od bezpośredniego przełożonego niż ogólnego maila od działu IT. Jeśli w pilotażach brały udział osoby z różnych departamentów, warto to wykorzystać umieszczając na przykład cytaty w komunikacji z pracownikami (*„Pani Kasia z HR: Bałam się, że to skomplikowane, ale instalacja i konfiguracja aplikacji zajęła 2 minuty i czuję się teraz spokojniejsza o swoje konto”*). Taki element ludzki może przemówić do nieprzekonanych jeszcze pracowników.
- **Podkreślenie obowiązkowości i terminów**. O ile na etapie pilotażowym komunikacja z pracownikami powinna być prowadzona językiem dobrowolnej zachęty, o tyle zbliżając się do terminu globalnego wdrożenia, komunikaty powinny już wyraźnie zaznaczać, że od podanego dnia logowanie bez MFA nie będzie już możliwe, a kto nie skonfiguruje MFA, straci dostęp do systemów i będzie musiał skontaktować się z działem pomocy w celu odblokowania konta.

  Takie podejście zmobilizuje pracowników. Trzeba jednak jednocześnie ich zapewnić, że wsparcie jest dostępne. Najgorszy możliwy scenariusz to sytuacja, w której w dniu globalnego wdrożenia MFA znajdą się pracownicy, którzy o niczym nie wiedzą. Aby tego uniknąć, warto wysłać kilka przypomnień.
- **Szkolenia praktyczne.** w niektórych przypadkach, szczególnie gdy pracownicy są mniej techniczni, warto przeprowadzić krótką sesję szkoleniową. Można przygotować film demonstracyjny, na którym pracownik podchodzi z telefonem do pracownika działu IT lub wsparcia i wspólnie instalują i konfigurują aplikację do MFA. Szkolenie można również zrealizować w formie warsztatów online, podczas których zebrana grupa pracowników wykonuje razem z prowadzącym konfigurację krok po kroku.

- **Materiały przypominające zasady bezpieczeństwa**. Po wprowadzeniu MFA, warto przygotować krótkie porady dot. dobrych praktyk bezpieczeństwa. Tego typu komunikaty edukacyjne można rozesłać tuż po wdrożeniu, by utrwalić prawidłowe nawyki. Przykłady:
  - *„Nigdy nie podawaj nikomu swojego kodu jednorazowego - dział IT nigdy Cię o to nie poprosi!"*
  - *„Jeśli dostaniesz na telefon powiadomienie push, którego się nie spodziewasz, NIE akceptuj go, tylko zgłoś incydent do działu IT!"*

Uruchomienie MFA na produkcji

Uruchomienie MFA na produkcji to moment, w którym MFA staje się obowiązkowe dla wszystkich określonych w projekcie użytkowników oraz systemów. Od tego dnia logowanie wymaga dodatkowo przejścia drugiego składnika uwierzytelniania. Jest to kulminacyjny punkt wdrożenia, dlatego wymaga szczególnej uwagi i przygotowania.

Poniżej przedstawiono, jak przeprowadzić produkcyjne uruchomienie MFA, aby zapewnić ciągłość działania i zminimalizować stres zarówno wśród działu IT, jak i pozostałych pracowników.

- **Wdrożenie w dogodnym terminie**. Termin powinien być ściśle dopasowany do specyfiki działania organizacji i przewidywanego czasu przestoju. w dużych firmach zmiany najlepiej przeprowadzać poza standardowymi godzinami pracy (np. nocą lub w weekend), aby zminimalizować wpływ na użytkowników. w mniejszych zespołach można rozważyć wdrożenie w godzinach roboczych, o ile wszyscy kluczowi członkowie zespołu wdrożeniowego są dostępni. Niezbędne jest również sprawdzenie, czy wybrany termin nie pokrywa się z innymi ważnymi wydarzeniami (np. zamknięcie miesiąca, duże wdrożenie innego systemu).
- **Ostatnie przypomnienie**. Na dzień przed globalnym wdrożeniem MFA warto wysłać jeszcze jeden komunikat do wszystkich pracowników, który przypomni, że od jutra MFA będzie wymagane. Należy zawrzeć w nim jeszcze raz wszystkie najważniejsze informacje.
- **Wsparcie w trybie podwyższonej gotowości**. w dniu globalnego uruchomienia MFA warto uruchomić dodatkowe kanały wsparcia, np. specjalny kanał na czacie firmowym czy przedłużony dyżur telefoniczny w IT. Wcześniej przygotowane materiały edukacyjne i pomocnicze dla działu pomocy technicznej również będą przydatne. Jeżeli firma jest duża i rozproszona geograficznie należy zapewnić że w każdej filii ktoś z IT jest przeszkolony i gotów pomóc na miejscu.

- **Monitorowanie systemu**. Tuż po włączeniu wymogu MFA, należy intensywnie monitorować działanie systemu.
  - Czy pojawiają się jakieś błędy w logach uwierzytelnień?
  - Czy infrastruktura jest wydajna (np. serwer nie jest przeciążony, kolejki SMS się nie zapychają)?
  - Czy nie nastąpiły nieprzewidziane problemy?
  - Czy wszyscy użytkownicy mogą zarejestrować swoje urządzenia?
  - Czy istnieją użytkownicy, którzy nie są w stanie się uwierzytelnić?
- **Komunikacja w dniu uruchomienia**. w dniu globalnego uruchomienia MFA wyślij krótką wiadomość do wszystkich pracowników, na przykład: *„MFA zostało pomyślnie włączone.*

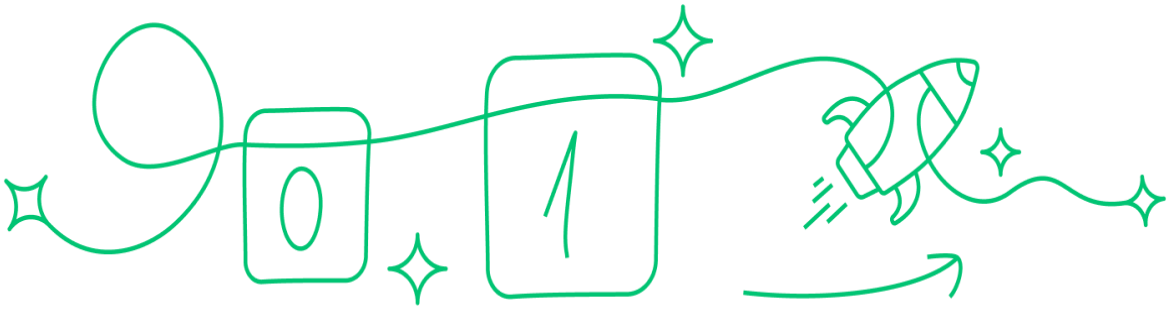
  Przypominamy: od teraz przy logowaniu wymagane będzie potwierdzenie tożsamości metodą X. Jeśli napotkasz trudności, skontaktuj się z …”. Jeżeli pojawiają się jakiekolwiek globalne problemy, natychmiast trzeba poinformować o tym pracowników.
- **Szybkie reagowanie na incydenty**. Pierwsze godziny i dni po uruchomieniu MFA dla wszystkich pracowników to czas, w którym zebrane zostanie większość zgłoszeń. Ważna jest odpowiednia priorytetyzacja tych zgłoszeń. Sytuacje, w których użytkownik nie wie jak coś zrobić są istotne, ale bardziej krytyczne są sytuacje, w których użytkownik w ogóle nie może się zalogować pomimo poprawnego wykonania opisanych kroków i blokuje to dostęp do ważnej usługi. Przypadkom zablokowanego dostępu należy przypisać najwyższy priorytet i reagować na nie w trybie awaryjnym, np. wygenerować awaryjne kody dostępu, które zapewnią ciągłość dostępu do usługi, podczas gdy dział IT będzie pracował nad naprawą napotkanego problemu. Warto prowadzić dziennik wszystkich napotkanych incydentów, by je później na spokojnie przeanalizować i usprawnić na ich podstawie konfigurację.
- **Spotkanie podsumowujące na koniec dnia**. Pod koniec pierwszego dnia globalnego uruchomienia MFA warto zorganizować wewnętrzne spotkanie, na którym zostaną omówione następujące kwestie:
  - Co poszło dobrze?
  - Jakie napotkano problemy?
  - Ile zgłoszeń obsłużono?
  - Czy są jeszcze nierozwiązane kwestie na kolejne dni?
- **Krótkie podsumowanie dla kierownictwa**. Po zakończeniu globalnego uruchomienia MFA, warto przekazać kierownictwu krótką informację na temat

wdrożenia. Wystarczy krótka informacja typu: *„Wdrożenie poszło pomyślnie w X% przypadków, było X problemów, ale wszystkie zostały rozwiązane (lub powstał już plan ich rozwiązania).”*. Można też przekazać pozytywną wiadomość do całej firmy, np. *„Gratulacje, udało nam się wspólnie podnieść poziom bezpieczeństwa w organizacji. Już X% z Was korzysta z MFA. Dziękujemy za współpracę.”*. Taka krótka wiadomość wysłana do pracowników sprawia, że czują się docenieni i zamyka formalnie wdrożenie MFA.

Harmonogram wdrożenia MFA w organizacji

Poniżej znajduje się przykładowy harmonogram działań w okresie globalnego uruchomienia MFA. Jest to przykładowy, orientacyjny harmonogram, który należy dostosować do realiów danej organizacji.

Utworzenie takiego harmonogramu pozwala zrealizować uruchomienie MFA z minimalnym ryzykiem. Należy pamiętać, że celem jest, aby organizacja działała nieprzerwanie: MFA ma zabezpieczać, ale nie paraliżować. Dlatego takie elementy jak kody awaryjne czy gotowość do czasowego obejścia MFA są niezbędne, by organizacja mogła dalej pracować. w idealnym scenariuszu, przy dobrym pilotażu i komunikacji oraz z dobrym rozwiązaniem MFA, dzień globalnego uruchomienia MFA powinien minąć bez poważniejszych incydentów.



Tydzień przed:

- Ostatnia tura komunikacji informująca o zbliżającym się uruchomieniu obowiązkowego MFA.
- Końcowe testy procedur wsparcia i szkolenie zespołów IT i helpdesk z uwierzytelniania wieloskładnikowego.

Uruchomienie MFA – dzień 0 (dzień przed):

- Wysłanie komunikatu informującego, że w następnym dniu roboczym nastąpi uruchomienie MFA.
- Sprawdzenie na kilku kontach testowych, czy wszystko działa zgodnie z planem.

Uruchomienie MFA – dzień 1 (rano):

- Zespół IT oraz wsparcia technicznego w gotowości od rana.
- Włączenie MFA zgodnie z harmonogramem (np. o 10:00).
- Wysłanie pracownikom komunikatu, że MFA jest już aktywne.
- Uruchomienie wzmożonego dyżuru wsparcia.

Uruchomienie MFA – dzień 1 (południe):

- Monitorowanie działania MFA.
- Regularna komunikacja między członkami zespołu (np. co godzinę szybka synchronizacja: ile zgłoszeń, jakie typy problemów)
- Korygowanie drobnych ustawień, jeśli potrzeba.

Uruchomienie MFA – dzień 1 (koniec dnia):

- Zebranie zespołu projektowego.
- Omówienie przebiegu dnia.
- Spisanie zaistniałych problemów i ich rozwiązań.

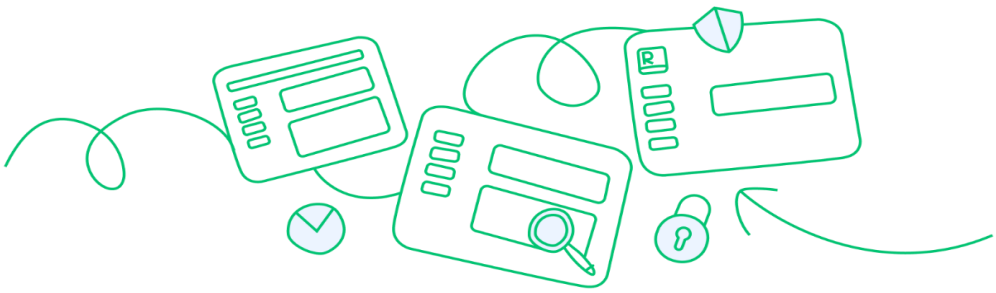
Uruchomienie MFA – kolejne dni:

- Nadal podwyższona gotowość wsparcia.
- Dalsze komunikaty korygujące (jeśli pewna liczba osób wciąż ma problemy z nowym rodzajem uwierzytelniania, warto przygotować oddzielny komunikat z rozwiązaniami).
- Stopniowe przechodzenie do normalnego trybu pracy.

Po wdrożeniu – utrzymanie i doskonalenie

Wdrożenie MFA to nie jednorazowe wydarzenie, ale nowy stan funkcjonowania infrastruktury bezpieczeństwa. Po zakończeniu projektu wdrożenia należy skupić się na utrzymaniu systemu oraz ciągłym doskonaleniu polityk MFA i procesu uwierzytelniania. Oto, o czym warto pamiętać w fazie powdrożeniowej:

- **Monitorowanie bezpieczeństwa i wyciąganie wniosków**. Należy regularnie przeglądać dzienniki uwierzytelniania pod kątem incydentów bezpieczeństwa. Warto zwrócić uwagę na nietypowe godziny logowań (np. o 3 w nocy, gdy nikt z reguły nie pracuje) oraz powtarzające się nieudane próby logowania (dziesiątki odrzuconych prób dla jednego użytkownika). Warto też przeanalizować skuteczność MFA, np. czy od czasu wdrożenia spadła liczba incydentów związanych z kontami.



- **Rotacja urządzeń i aktualizacje**. Należy pamiętać, że środowisko pracy jest dynamiczne: pracownicy wymieniają telefony, nowi członkowie dołączają do zespołu, a dotychczasowi odchodzą.
    - Konieczne jest utworzenie procesu włączania MFA dla nowych pracowników (np. w pierwszym dniu pracy dostają pakiet startowy: *„Oto firmowy komputer, a tu jest link do konfiguracji MFA na koncie. Proszę zrobić to od razu.”*).
    - Trzeba też mieć gotowy proces usunięcia pracownika z systemu MFA po jego odejściu z pracy.
    - Warto poinstruować pracowników, żeby regularnie aktualizowali aplikacje klienckie MFA, jeśli takie istnieją (np. jeśli dostawca MFA oferuje dedykowaną aplikację mobilną, warto zalecić częste aktualizacje, albo włączenie automatycznej aktualizacji).
    - Należy aktualizować również serwery i usługi MFA wdrożone lokalnie, gdy tylko pojawią się ich zaktualizowane wersje. Nowe wersje produktów często zawierają poprawki bezpieczeństwa oraz nowe funkcjonalności, więc regularne aktualizacje są bardzo ważne.
- **Przegląd wyjątków i kont specjalnych**. Jeśli istnieją konta, które nie podlegają MFA (np. konta awaryjne lub serwisowe), należy się upewnić, że są one dobrze zabezpieczone innymi metodami i regularnie audytowane. Hasła do tych kont powinny być wyjątkowo silne i przechowywane w bezpiecznym menedżerze haseł. Warto monitorować czy konta te są używane tylko i wyłącznie w ostateczności oraz okresowo analizować, czy nie powinno się jednak włączyć MFA dla tych kont.
- **Rozszerzenie o kolejne grupy i użytkowników**. Być może po podstawowym wdrożeniu dla pracowników warto objąć MFA także klientów lub partnerów zewnętrznych, którzy mają dostęp do pewnych zasobów organizacji. Wiele rozwiązań MFA na to pozwala (np. integrując się z portalem klienta). Jeśli ma to sens w konkretnym kontekście (np. ochrona dostępu kontrahentów do systemu zamówień), warto rozważyć wykorzystanie istniejącej infrastruktury MFA. Pozwoli to zyskać dodatkową korzyść z raz poniesionej inwestycji.

Podsumowując, wdrożenie MFA to proces ciągły. Po fazie projektu, następuje faza operacyjna, w której trzeba zarządzać MFA podobnie jak każdym innym ważnym systemem bezpieczeństwa. Dobrą wiadomością jest to, że po intensywnej fazie wdrożenia, utrzymanie MFA nie wymaga już dużego nakładu czasu. Nie należy jednak osiadać na laurach. Warto stale monitorować skuteczność rozwiązania i dbać o jego niezawodność. Rozwiązania takie jak Rublon MFA pozwalają monitorować zdarzenia logowania, efektywność wybranych metod MFA oraz poziom aktywności użytkowników, co upraszcza utrzymanie rozwiązania w fazie powdrożeniowej.

Wygodna lista kontrolna: O co zadbać po wdrożeniu MFA

Poniżej znajduje się krótka lista kontrolna najważniejszych aspektów, o które należy zadbać po uruchomieniu MFA w organizacji:

- **Monitoring incydentów MFA**:
  - Należy regularnie analizować dzienniki i zwracać uwagę na podejrzane zdarzenia (wiele błędnych kodów, odrzucane powiadomienia push, logowania z innych krajów itp.).
- **Przegląd polityk dostępu**:
  - Należy okresowo przeglądać polityki MFA i je dostosowywać w miarę potrzeb.
  - Warto rozważyć włączenie nowych opcji uwierzytelniania lub usunięcie starych, jeśli uznane zostaną za niedostatecznie bezpieczne.
- **Aktualizacje systemu**:
  - Należy zaplanować cykliczne aktualizacje serwerów i usług MFA oraz aplikacji klienckich.
  - Dobrze jest zrobić testy aktualizacji w bezpiecznym środowisku testowym przed wdrożeniem produkcyjnym.
- **Zarządzanie tożsamością**:
  - Należy stworzyć procedury uruchamiania MFA dla nowych pracowników oraz usuwania odchodzących z pracy pracowników z platformy MFA.
  - Jeśli istnieją jeszcze jakieś konta bez MFA, konieczne są ich regularne audyty oraz ostatecznie uruchomienie na nich uwierzytelniania wieloskładnikowego, o ile to możliwe.
- **Konta uprzywilejowane i awaryjne**:
  - Konta uprzywilejowane i konta adminów powinny zostać objęte szczególnie silnym uwierzytelnianiem wieloskładnikowym. Preferowane jest MFA odporne na phishing.
  - Konta awaryjne muszą być silnie zabezpieczone i okresowo sprawdzane.

- **Szkolenia utrwalające**: Należy włączyć informacje na temat uwierzytelniania wieloskładnikowego do szkoleń okresowych z bezpieczeństwa dla pracowników. Podczas tego typu szkoleń warto uczyć o bezpiecznym korzystaniu z MFA oraz o rodzajach ataków na tę formę zabezpieczenia, np. o inżynierii społecznej.
- **Plan na wypadek awarii**: Należy mieć sprawdzony (np. testowany raz na pół roku) plan awaryjny na wypadek niedostępności systemu MFA. Konta awaryjne lub konfiguracja dostępu offline muszą być w takiej sytuacji dostępne, a personel musi wiedzieć jak z nich korzystać. Po opanowaniu awarii wszyscy pracownicy ponownie muszą wrócić do korzystania z MFA, tak jak dotychczas.

Zapewnienie ciągłości biznesowej podczas korzystania z MFA

Wdrożenie uwierzytelniania wieloskładnikowego znacząco zwiększa poziom bezpieczeństwa w organizacji, ale jednocześnie dodaje nową warstwę zależności technologicznej. Co się stanie, jeśli system MFA zawiedzie, albo gdy użytkownik utraci wszystkie swoje metody uwierzytelnienia?

Zapewnienie ciągłości biznesowej oznacza przygotowanie się na takie scenariusze, by przerwa w dostępności MFA nie zatrzymała działania organizacji. Poniżej znajdują się środki zapobiegawcze i dobre praktyki, które pozwolą korzystać z MFA bez obaw o paraliż pracy.

Dowiedz się, jak zapewnić nieprzerwane działanie uwierzytelniania MFA dzięki przewodnikowi Rublon dotyczącemu zapewnienia ciągłości biznesowej.

Redundancja i wysoka dostępność systemu MFA

Jeśli rozwiązanie MFA obejmuje lokalne komponenty (ang. *on-premise*), warto zadbać o ich wysoką dostępność (ang. *high availability*). Można to osiągnąć poprzez konfigurację klastra w trybie aktywno-pasywnym lub aktywno-aktywnym, rozmieszczenie serwerów w dwóch lokalizacjach oraz zapewnienie bieżącego backupu bazy danych.

Należy też dobrze przetestować mechanizmy przełączania awaryjnego (failover), aby upewnić się, że zadziałają niezawodnie w przypadku awarii. Przykładowo, warto sprawdzić, czy w razie awarii głównego serwera proxy dodającego MFA, zapasowy od razu przejmie żądania i użytkownicy nawet tego nie odczują.

W przypadku dostawcy MFA oferującego swoją usługę w chmurze, należy sprawdzić umowę o gwarantowanym poziomie świadczenia usług (ang. *Service Level Agreement*, SLA) oraz architekturę rozwiązania.

Kluczowe jest, by jedna awaria nie wyłączyła całego mechanizmu logowania w firmie. Należy testować rozwiązanie MFA pod kątem odporności, na przykład:

- Co się stanie, jeśli utraci się dostęp do Internetu? Czy pracownicy nadal zalogują się na swoje komputery?
- Czy mechanizmy przełączania awaryjnego działają zgodnie z założeniami i przepuszczają lub odrzucają logującego się użytkownika?
- Czy kody awaryjne są dostępne, działają poprawnie i są rotowane po użyciu?

Eliminacja pojedynczych punktów zaporowych

Należy zapewnić użytkownikom alternatywne metody MFA na wypadek problemów z główną metodą. Przykładowo, jeśli pracownicy organizacji używają głównie powiadomień push w aplikacji mobilnej, należy upewnić się, że istnieje także możliwość skorzystania z innej metody uwierzytelniania lub otrzymania kodu awaryjnego w nagłym wypadku.

Jeśli pracownicy korzystają z kluczy FIDO, warto by mieli drugi zapasowy klucz. Jest to szczególnie ważne, jeśli dostęp do krytycznych zasobów może być chroniony tylko i wyłącznie przez klucze bezpieczeństwa zgodne ze standardem FIDO. Warto w takiej sytuacji wydawać pracownikom po 2 klucze bezpieczeństwa: jeden do użytku na co dzień, drugi do schowania w bezpiecznym miejscu na wypadek zgubienia pierwszego.

Wewnętrzna polityka bezpieczeństwa organizacji powinna zachęcać do dodania przynajmniej dwóch odrębnych metod uwierzytelniania do konta.

Procedura odzyskiwania dostępu

Zawsze istnieje ryzyko, że użytkownik utraci dostęp do konta. Musi zatem istnieć formalny proces pozwalający zweryfikować tożsamość użytkownika i przywrócić dostęp. Takie zdarzenie powinno zostać odpowiednio odnotowane i zatwierdzone przez przełożonego, co pomoże uniknąć nadużyć. Typowa procedura przywrócenia dostępu powinna wyglądać następująco:

1. Użytkownik kontaktuje się z wewnętrznym wsparciem technicznym.
2. Operator weryfikuje tożsamość użytkownika na podstawie kilku specyficznych pytań. Muszą one jednoznacznie identyfikować użytkownika i uniemożliwić podszycie się osobie nieupoważnionej.
3. Po pozytywnej weryfikacji operator generuje jednorazowe hasło awaryjne lub wysyła link z możliwością skonfigurowania nowego urządzenia do MFA.

Dowiedz się, jak używać awaryjnych kodów dostępu (Bypass Code) w Rublon MFA.

Konta i ścieżki awaryjne dla administratorów

W zależności od infrastruktury organizacji, konta awaryjnego dostępu mogą być wymagane dla zapewnienia ciągłości działania systemów krytycznych. Te konta powinny służyć tylko do sytuacji awaryjnych, gdy zwykli administratorzy nie mogą się zalogować, bo np. wystąpiła awaria usługi MFA.

Zamiast całkowicie rezygnować z MFA, warto zastosować MFA w trybie offline, np. za pomocą kodów jednorazowych generowanych przez aplikację mobilną. Hasła muszą być nadzwyczajnie silne i odpowiednio chronione (zapieczętowane koperty w sejfie zarządu albo bezpieczny sejf haseł z dostępem tylko dla uprawnionych osób).

W dużych środowiskach warto utworzyć host bastionowy (ang. *bastion host* lub *jump host*), czyli system całkowicie odcięty od internetu i schowany za siecią VPN, który posiada własne konta awaryjne z MFA w trybie offline. Takie podejście pozwala utrzymać zasadę „najbardziej krytyczny dostęp = najsilniejsze MFA", a jednocześnie nie odcina zespołu w razie niedostępności uwierzytelniania wieloskładnikowego.

Scenariusz użycia kont awaryjnych powinien być regularnie testowany. Gdy system MFA nie działa, administrator używa konta awaryjnego, loguje się z dedykowanej stacji PAW i diagnozuje problem. Po każdym użyciu należy odnotować zdarzenie w narzędziu SIEM, zgodnie z kontrolą NIST AC-2(2).

Wykluczenia tymczasowe i mechanizmy „fail-open"

Warto przeanalizować, czy istnieją sytuacje, w których dostęp nie może zależeć wyłącznie od mechanizmów MFA. Przykładem mogą być systemy medyczne działające 24/7, gdzie lekarz musi natychmiast uzyskać dostęp do systemu. Co zrobić, jeśli nie otrzyma kodu uwierzytelniającego na telefon?

W takich przypadkach można rozważyć możliwość logowania jednoskładnikowego w sytuacjach awaryjnych (ang. *fail-open*). Jest to jednak bardzo wrażliwa kwestia, ponieważ niewłaściwe wykorzystanie tego mechanizmu może stanowić lukę bezpieczeństwa.

Alternatywnym podejściem są rozwiązania offline, np. tokeny sprzętowe lub aplikacje mobilne generujące kody OTP bez dostępu do internetu. w sytuacji awaryjnej (np. brak telefonu czy internetu) pracownik może również skorzystać z wydanej mu wcześniej koperty z kodami awaryjnymi.

Kluczowe jest, aby procedury awaryjne były jasno określone i znane wyłącznie uprawnionym osobom. Jednocześnie należy zadbać o odpowiednie zabezpieczenie środków takich jak kody awaryjne, aby nie stały się publicznie dostępną luką w systemie.

Dowiedz się, jak działa tryb awaryjny (Fail Mode) w konektorach Rublon MFA.

Regularne testy DR (Disaster Recovery)

Należy włączyć platformę MFA do planów ciągłości działania i odtwarzania po awarii w organizacji. Jeżeli wykonywane są testy DR (np. symulacja utraty Data Center), to należy uwzględnić scenariusz, w którym niedostępny jest serwer uwierzytelniania MFA. Warto oszacować, jak długo zajmie jego przywrócenie oraz czy pracownicy będą mogli pracować w trybie awaryjnym. Należy również przetestować procedury awaryjne: np. raz na kwartał warto poprosić wybranego administratora by spróbował zalogować się używając konta awaryjnego zgodnie z dokumentacją.

Śledzenie dostępności usług MFA

Warto zasubskrybować stronę informującą o stanie usług dostawcy MFA (ang. *status page*). Pozwala to jednoznacznie stwierdzić, czy problemy z logowaniem wśród pracowników leżą po stronie dostawcy. Strony statusu często zawierają podział całej infrastruktury dostawcy MFA na jej dokładne części składowe. Dzięki temu powiadomienie na temat awarii operatora GSM w regionie na stronie statusu dostawcy MFA jest prostym wytłumaczeniem, dlaczego SMS-y z kodem jednorazowym nie docierają do logujących się pracowników. Mając taką wiedzę, można szybko przełączyć domyślną metodę uwierzytelniania albo powiadomić pracowników o konieczności użycia innej metody uwierzytelniania.

Bezpieczeństwo kluczy i tokenów fizycznych

Jeśli w organizacji używane są klucze sprzętowe lub karty inteligentne (ang. *smart cards*), należy zadbać o politykę ich wymiany i raportowania utraty. Pracownicy powinni wiedzieć, że zgubienie klucza FIDO jest porównywalne do zgubienia klucza do drzwi, i że należy to natychmiast zgłosić, by można było taki klucz unieważnić w systemie. Warto mieć w zapasie pewną pulę nieużywanych kluczy, by szybko móc wydać klucz zamienny, chociaż lepszym rozwiązaniem jest wydawanie pracownikom dwóch kluczy: jednego głównego i drugiego zapasowego. Warto prowadzić ewidencję wydanych urządzeń. w przypadku, gdy tokeny mają ograniczony czas życia (np. certyfikaty na kartach mogą wygasać co 2 lata), należy ustawić przypomnienia o ich odnowieniu z wyprzedzeniem.

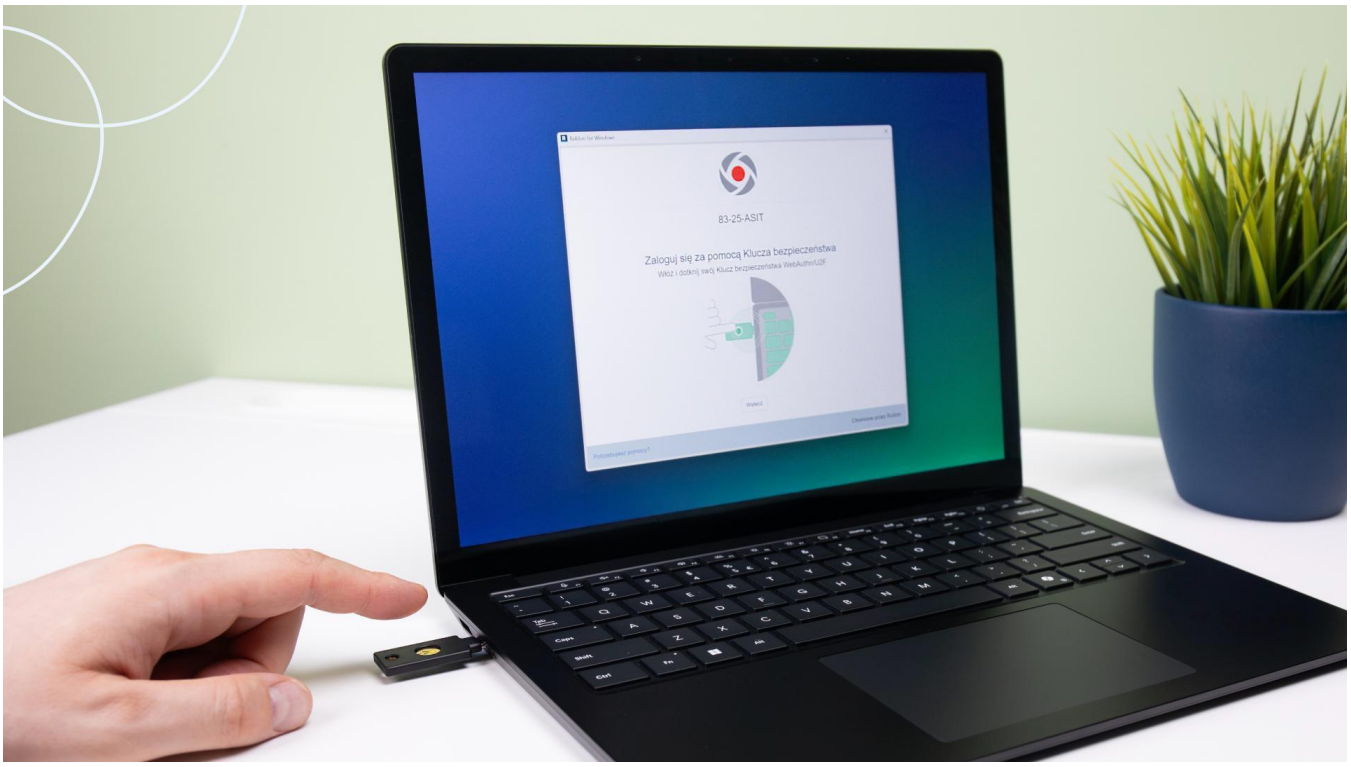
Wygodna lista kontrolna: Zachowanie ciągłości biznesowej

Poniżej znajduje się krótka lista kontrolna odnośnie zachowania ciągłości biznesowej organizacji przy korzystaniu z MFA.

- **Redundancja platformy MFA:**
  - Skonfiguruj klaster aktywno-pasywny / aktywno-aktywny lub instancje w dwóch lokalizacjach.
  - Przetestuj przełączanie (fail-over) – czy zapasowy serwer przejmuje ruch bez przerwy dla użytkownika?
  - Zweryfikuj SLA i architekturę dostawcy chmurowego.
  - Sprawdź, czy logowanie lokalne działa po utracie łącza internetowego.
- **Eliminacja pojedynczych punktów zaporowych:**
  - Wymuszaj minimum dwie różne metody MFA na koncie użytkownika.
  - Zapewnij kody awaryjne lub alternatywną metodę uwierzytelniania dla nagłych wypadków.
- **Procedura odzyskiwania dostępu:**
  - Zdefiniuj kroki weryfikacji tożsamości (pytania kontrolne, kontakt przełożonego).
  - Udokumentuj generowanie hasła jednorazowego lub linku do ponownej rejestracji MFA.
  - Rejestruj każde zdarzenie i poddawaj zatwierdzeniu przez przełożonego.
- **Konta i ścieżki awaryjne dla administratorów:**
  - Utrzymuj 1-2 konta break-glass (hasło + MFA offline).
  - Hasła przechowuj w sejfie, z dostępem tylko dla zarządu/CISO.
  - W dużych środowiskach uruchom bastion host za VPN z własnymi kontami awaryjnymi.
  - Testuj logowanie awaryjne i zmieniaj hasło po każdym użyciu; zdarzenie loguj w SIEM.
- **Wykluczenia tymczasowe & mechanizm „fail-open”:**
  - Przygotuj metody MFA w trybie offline lub koperty z kodami OTP.
  - Ogranicz dostęp do procedury awaryjnej do uprawnionych osób i dokumentuj użycie.
- **Regularne testy DR:**
  - Uwzględnij usługę MFA w planach ciągłości działania.

- Raz na kwartał zasymuluj niedostępność MFA.
- Mierz czas przywracania MFA (RTO) i gotowość pracowników do pracy w trybie awaryjnym.

- **Śledzenie stanu usług MFA:**
  - Subskrybuj stronę statusu dostawcy MFA i włącz powiadomienia o zmianie stanu usług.
  - Skonfiguruj alerty dla kluczowych komponentów.
- **Bezpieczeństwo fizycznych kluczy / tokenów:**
  - Prowadź ewidencję wydanych urządzeń; wymagaj natychmiastowego raportu utraty.
  - Wydawaj dwa klucze na osobę (główny + zapasowy).
  - Ustaw przypomnienia o odnowieniu certyfikatów / kart przed ich wygaśnięciem.



Załącznik 1: Metody uwierzytelniania MFA

Przy doborze metod w organizacji należy kierować się zasadą adekwatności do ryzyka. Dla większości pracowników akceptowalne będą aplikacje mobilne (kody lub push), natomiast dla najbardziej zagrożonych kont trzeba już zastosować klucze sprzętowe FIDO. Należy unikać opierania bezpieczeństwa dostępu na metodach łatwych do obejścia (SMS, e-mail). Takie metody mogą ewentualnie pełnić funkcję awaryjną, ale nie powinny stanowić fundamentu uwierzytelniania.

Warto uwzględnić w dokumentacji wewnętrznej szczegółowy opis typów użytkowników i zasobów wraz z przypisaną do nich wymaganą metodą MFA. Taki dokument pomoże ustandaryzować zasady uwierzytelniania, zapewniając spójność i zgodność z polityką bezpieczeństwa organizacji.

Metoda MFA	Odporność na cyberataki	Najistotniejsze uwagi dotyczące bezpieczeństwa i stosowania
Klucz sprzętowy FIDO2	**Bardzo wysoka** – kryptograficznie powiązany z domeną, odporny na phishing i ataki „man-in-the-middle".	Zalecany dla kont uprzywilejowanych oraz krytycznych systemów. Należy wydać co najmniej dwa klucze (główny + zapasowy) i prowadzić ewidencję sprzętu.
Karta inteligentna (PKI)	**Wysoka** – klucz prywatny chroniony przez kartę + PIN, nie opuszcza urządzenia.	Wymagają pełnej infrastruktury PKI i czytników; powszechne w administracji publicznej (karty PIV) i organizacjach regulowanych.
Passkey	**Wysoka** – odporne na phishing, weryfikacja odbywa się lokalnie (biometria / PIN).	Wygodne dla użytkownika; przy kluczach synchronizowanych klucz prywatny trafia zaszyfrowany do chmury, co wymaga odpowiedniej polityki kont Apple/Google/Microsoft lub ustawień menedżera haseł.
Aplikacja mobilna – powiadomienie push	**Średnia lub Wysoka** – jeśli zastosowano, mechanizm number matching, eliminuje push bombing i przypadkowe akceptacje, zwiększając bezpieczeństwo metody.	Dobry kompromis między wygodą a bezpieczeństwem; wymaga połączenia internetowego w telefonie; wciąż podatne na zaawansowane scenariusze phishingowe.

Metoda MFA	Odporność na cyberataki	Najistotniejsze uwagi dotyczące bezpieczeństwa i stosowania
YubiKey OTP	**Średnia** – kod wpisywany automatycznie po naciśnięciu klucza, lecz wciąż podatny na phishing (atakujący może go natychmiast użyć).	Wygodny, ponieważ nie trzeba wpisywać kodu, ale podatny na phishing; skoro zakupiło się już klucze sprzętowe, zaleca się zamiast YubiKey OTP używać odpornego na phishing uwierzytelniania zgodnego z FIDO2.
Aplikacja mobilna – kod TOTP	**Średnia** – kod można wyłudzić phishingiem, ale zwykle wymaga to dostępu do urządzenia lub złośliwego oprogramowania.	Działa offline; wymaga ręcznego wpisania kodu (potencjalny shoulder surfing). Stosować tylko tam, gdzie bezpieczniejsze metody są niemożliwe.
Sprzętowy token OTP	**Średnia** – kod jednorazowy, ale możliwy do wyłudzenia phishingiem.	Wolny od zależności telefonicznych; wymaga logistyki (wydawanie, baterie). Coraz częściej zastępowany aplikacjami TOTP lub kluczami FIDO.
Aplikacja mobilna – kod QR	**Średnia** – jednorazowy, ale może zostać przechwycony, jeśli ekran jest widoczny publicznie.	Kod powinien wygasać natychmiast po użyciu.
SMS OTP / połączenie głosowe	**Niska** – podatne na phishing, SIM swap i ataki SS7.	Stosować wyłącznie awaryjnie lub dla użytkowników bez smartfona; planować migrację do metod silniejszych.
E-mail OTP	**Niska** – ochrona całkowicie zależna od bezpieczeństwa skrzynki pocztowej.	Używać tylko zapasowo; sama poczta również musi być chroniona przez MFA.
Kody zapasowe / awaryjne	**Zależna od sposobu przechowywania** – papier/plik można wykraść.	Generować tylko na określony czas i określoną liczbę użyć, przekazywać użytkownikom bezpiecznym kanałem i przechowywać offline w chronionym miejscu.

Załącznik 2: Wymogi regulacyjne dotyczące MFA

Poniższa tabela zestawia najważniejsze akty prawne i wytyczne, które wprost nakładają na polskie podmioty publiczne lub nadzorowane obowiązek stosowania uwierzytelniania wieloskładnikowego (MFA) bądź „silnego uwierzytelniania".

Inne regulacje (np. RODO czy rozporządzenie Krajowe Ramy Interoperacyjności) mówią ogólnie o „odpowiednich środkach technicznych" lub „wdrażaniu polityki bezpieczeństwa informacji".

W praktyce organy nadzorcze coraz częściej uznają MFA za środek proporcjonalny do większości ryzyk związanych z dostępem uprzywilejowanym lub zdalnym.

Jurysdykcja / sektor	Akt prawny / dokument	Artykuł / paragraf	Zakres wymogu MFA
UE – podmioty kluczowe i ważne	Dyrektywa (NIS 2) 2022/2555	Art. 21 ust. 2 lit. d, i, j	MFA wspiera bezpieczeństwo łańcucha dostaw, zasobów ludzkich i kontroli dostępu; jest wymagane dla zabezpieczenia komunikacji i systemów awaryjnych, gdzie stosowne.
UE – sektor finansowy	Rozporządzenie (DORA) 2022/2554	Art. 9 ust. 3 lit. b–c; ust. 4 lit. c–d	MFA wspiera realizację polityk bezpieczeństwa ICT przez minimalizację ryzyka nieuprawnionego dostępu, ochronę poufności i integralności danych oraz kontrolę dostępu do zasobów ICT; ponadto stanowi bezpośredni wymóg jako „silny mechanizm uwierzytelniania" zgodny ze standardami.

Jurysdykcja / sektor	Akt prawny / dokument	Artykuł / paragraf	Zakres wymogu MFA
UE – usługi płatnicze	PSD2 (2015/2366), RTS 2018/389	PSD2 (2015/2366) art. 97, RTS 2018/389 art. 4-9	Silne uwierzytelnianie klienta (SCA) jest wymagane przy dostępie do rachunku online, inicjowaniu transakcji elektronicznej oraz każdej czynności zdalnej niosącej ryzyko oszustwa; musi opierać się na ≥ 2 niezależnych elementach z kategorii: wiedza, posiadanie, cechy klienta.

Przykłady wymogów MFA spoza UE

- **USA – NIST SP 800-53 Rev. 5**
  Kontrola IA-2(1)(2): MFA do kont uprzywilejowanych i nieuprzywilejowanych; IA-2 wyznacza techniczne standardy MFA dla systemów federalnych.
- **USA – Executive Order 14028**
  § 3(d) nakazuje wszystkim agencjom federalnym wdrożyć MFA.
- **USA – OMB M-22-09 „Federal Zero Trust Strategy"**
  Wymaga MFA odpornego na phishing dla pracowników i kontraktorów oraz konsolidacji systemów tożsamości.
- **USA – NIST SP 800-171 Rev. 3**
  Wymaga MFA dla wszystkich kont uprzywilejowanych i zwykłych w systemach przetwarzających CUI.

Dlaczego to ważne?

Dynamiczny rozwój regulacji w USA pokazuje kierunek: od „jakiegokolwiek" MFA do obowiązkowych, odpornych na phishing metod (FIDO2, PIV). Podobną ewolucję przewiduje się w UE. Już teraz najnowsze wytyczne ENISA zebrane w dokumencie „NIS2 Technical Implementation Guidance".

Administracja publiczna w Polsce, przygotowując projekty MFA, powinna więc celować od razu w mechanizmy zgodne ze standardem FIDO2, aby uniknąć kosztownych zmian w przyszłości.

Załącznik 3: Słownik pojęć

- **Active Directory (AD)** — usługa katalogowa firmy Microsoft służąca do uwierzytelniania, autoryzacji oraz centralnego zarządzania użytkownikami, komputerami i zasobami w środowisku domenowym systemu Windows.
- **Active Directory Federation Services (AD FS**) — rola systemowa w środowisku Microsoft, umożliwiająca uwierzytelnianie federacyjne i SSO między aplikacjami lokalnymi i chmurowymi. Może być zintegrowana z rozwiązaniami MFA w celu zabezpieczenia logowania.
- **Authenticator Assurance Level (AAL)** — poziom zaufania do mechanizmu uwierzytelniania według klasyfikacji NIST. AAL1 oznacza niski poziom (np. hasło), AAL2 to poziom średni (np. hasło + kod TOTP), a AAL3 to najwyższy poziom (np. hasło + sprzętowy klucz FIDO2).
- **Device enrollment (rejestracja urządzenia)** — proces dodawania urządzenia użytkownika do platformy MFA w celu skonfigurowania metody uwierzytelniania, np. aplikacji mobilnej lub klucza FIDO. Może być przeprowadzany samoobsługowo przez użytkownika lub zarządzany centralnie przez administratora.
- **DORA (Digital Operational Resilience Act)** — rozporządzenie UE 2022/2554 dotyczące odporności operacyjnej instytucji finansowych i dostawców usług ICT. Nakłada obowiązek stosowania silnych metod uwierzytelniania (np. MFA), zarządzania ryzykiem cyfrowym, testów odporności, oraz raportowania incydentów. Dotyczy m.in. banków, firm ubezpieczeniowych, fintech'ów oraz dostawców usług w chmurze.
- **ENISA (European Union Agency for Cybersecurity)** — Agencja Unii Europejskiej ds. Cyberbezpieczeństwa. Publikuje wytyczne, dobre praktyki i raporty dotyczące ochrony systemów IT, w tym rekomendacje w zakresie MFA, tożsamości cyfrowej, zarządzania incydentami oraz wdrażania dyrektywy NIS2. Choć nie pełni formalnej roli interpretacyjnej, jej dokumenty są szeroko uznawane za wiarygodne źródło wsparcia technicznego w zakresie przepisów UE.
- **Entra ID (dawniej Azure AD)** — usługa katalogowa w chmurze Microsoftu, umożliwiająca zarządzanie tożsamościami, dostępem i uwierzytelnianiem użytkowników w środowiskach hybrydowych i chmurowych. Wspiera MFA, SSO i wiele metod logowania.
- **Fail-open** — mechanizm umożliwiający dostęp do systemu w przypadku niedostępności MFA, stosowany tylko w wyjątkowych przypadkach. Wymaga szczegółowych procedur kontrolnych.

- **FIDO2** — otwarty standard nowoczesnego, odpornego na phishing uwierzytelniania, opracowany przez stowarzyszenie FIDO Alliance. Umożliwia logowanie za pomocą kluczy bezpieczeństwa, wbudowanych zabezpieczeń biometrycznych lub passkeys.
- **High Availability (HA)** — architektura systemów informatycznych zapewniająca ich nieprzerwane działanie mimo awarii pojedynczych komponentów.
- **Konto break-glass** — specjalne konto awaryjne z dostępem uprzywilejowanym, przeznaczone wyłącznie do użycia w sytuacjach krytycznych, np. awarii chmurowego systemu MFA. Takie konta powinny być chronione za pomocą offline'owego MFA i regularnie monitorowane.
- **LDAP (Lightweight Directory Access Protocol)** — lekki protokół sieciowy służący do odczytu i modyfikacji informacji przechowywanych w usługach katalogowych, takich jak Active Directory, OpenLDAP czy inne systemy katalogowe. LDAP umożliwia dostęp do danych o użytkownikach, grupach, urządzeniach i innych zasobach w sposób hierarchiczny i zoptymalizowany pod kątem wydajności.
- **Multi-Factor Authentication (MFA)** — rodzaj weryfikacji tożsamości, który wymaga od użytkownika co najmniej dwóch różnych składników uwierzytelniania, aby zdecydować, czy dana osoba jest tym, za kogo się podaje. Te składniki uwierzytelniania to coś, co wiesz (np. hasło lub PIN), coś, co masz (np. klucz bezpieczeństwa lub smartfon) i coś, czym jesteś (np. odcisk palca lub twarz).
- **NIS2 (Network and Information Security Directive 2)** — unijna dyrektywa (2022/2555) dotycząca cyberbezpieczeństwa sieci i systemów informatycznych. Rozszerza zakres podmiotów objętych obowiązkami w zakresie bezpieczeństwa (m.in. administracja publiczna, zdrowie, energia, bankowość, technologie cyfrowe) oraz podnosi wymagania dot. Zarządzania ryzykiem, m.in. przez stosowanie MFA, zarządzanie tożsamością, monitorowanie incydentów i ciągłość działania.
- **Number matching** — mechanizm zwiększający bezpieczeństwo powiadomień push, polegający na konieczności przepisania przez użytkownika liczby wyświetlonej na ekranie logowania do aplikacji mobilnej. Chroni przed atakami typu push bombing i przypadkowymi zatwierdzeniami nieautoryzowanych prób logowania.
- **Odporność na phishing** — cecha metod uwierzytelniania, które zaprojektowane są tak, by nie dało się ich złamać poprzez nakłonienie użytkownika do za pomocą fałszywych stron logowania ani przechwycić danych uwierzytelniających.

- **One-Time Password (OTP)** — hasło jednorazowe używane w celu potwierdzenia tożsamości użytkownika. Najczęściej używane jako drugi składnik uwierzytelniania wieloskładnikowego.
- **Outlook Web App (OWA)** — komponent Microsoft Exchange Server pozwalający na dostęp do poczty przez przeglądarkę internetową. Często wskazywany jako jeden z pierwszych zasobów do objęcia MFA ze względu na zdalny charakter dostępu.
- **Passkey** — nowoczesna metoda uwierzytelniania, która pozwala użytkownikowi logować się bez użycia haseł, wykorzystując parę kluczy kryptograficznych zgodną ze standardem FIDO2.
- **Phishing** — metoda ataku polegająca na podszywaniu się pod zaufany podmiot (np. przez fałszywe e-maile lub strony logowania), w celu wyłudzenia danych uwierzytelniających. MFA odporne na phishing minimalizuje skuteczność takich ataków.
- **Powiadomienie push** — metoda uwierzytelniania, w której użytkownik zatwierdza próbę logowania za pomocą notyfikacji otrzymanej w aplikacji mobilnej. Może być dodatkowo zabezpieczona przez biometrię oraz mechanizm number matching.
- **Push bombing** — technika ataku polegająca na zalewaniu użytkownika powiadomieniami push z prośbą o zatwierdzenie logowania, licząc na jego przypadkową akceptację. Przeciwdziała temu mechanizm „number matching".
- **RADIUS (Remote Authentication Dial-In User Service)** —protokół komunikacyjny służący do uwierzytelniania, autoryzacji i rozliczania dostępu użytkowników do sieci komputerowych. Często wykorzystywany do integracji systemów MFA z sieciami VPN, systemami Wi-Fi oraz serwerami terminalowymi.
- **Remote Desktop Protocol (RDP)** — protokół firmy Microsoft umożliwiający zdalne połączenie z pulpitem innego komputera. w kontekście bezpieczeństwa, połączenia RDP powinny być zabezpieczone MFA ze względu na ich częste wykorzystywanie w atakach zdalnych.
- **REST API (Representational State Transfer Application Programming Interface)** — interfejs programistyczny oparty na architekturze REST, pozwalający systemom na komunikację przez protokoły HTTP. Często wykorzystywany do integracji systemów MFA z aplikacjami własnymi, portalami i usługami chmurowymi.
- **RODO (Rozporządzenie o Ochronie Danych Osobowych)** — rozporządzenie UE 2016/679 dotyczące ochrony danych osobowych. Wymaga od administratorów i podmiotów przetwarzających wdrożenia „odpowiednich środków technicznych i organizacyjnych" dla ochrony danych. Choć MFA nie jest wymienione wprost, jest powszechnie uznawane za środek proporcjonalny w kontekście ochrony dostępu do danych osobowych.

- **SAML (Security Assertion Markup Language)** — standard wymiany informacji o uwierzytelnieniu i autoryzacji pomiędzy dostawcą tożsamości (IdP) a usługodawcą (SP).

  Powszechnie stosowany do integracji logowania jednokrotnego (SSO) i systemów MFA w środowiskach korporacyjnych.
- **SIEM (Security Information and Event Management)** — system do centralnego zbierania, korelacji i analizy logów oraz zdarzeń bezpieczeństwa. Integracja platformy MFA z narzędziem SIEM pozwala na prostsze audytowanie logowań i wykrywanie nieprawidłowości.
- **Single Sign-On (SSO)** — mechanizm logowania jednokrotnego, w którym użytkownik loguje się tylko raz i uzyskuje dostęp do wielu aplikacji bez ponownego podawania danych uwierzytelniających.
- **Time-Based One-Time Password (TOTP)** — metoda generowania jednorazowych kodów oparta na czasie, zgodna ze standardem RFC 6238. Kody zmieniają się co 30 sekund i są generowane lokalnie w aplikacji (np. Google Authenticator, Rublon Authenticator).
- **Windows Logon (logowanie do systemu Windows)** — proces uwierzytelniania użytkownika przy logowaniu do lokalnego systemu operacyjnego Windows. Domyślnie nie obsługuje MFA, ale może być zabezpieczony za pomocą dodatkowych rozwiązań takich jak Rublon MFA.
- **Zero Trust** — model bezpieczeństwa, w którym żadna tożsamość ani urządzenie nie jest automatycznie uznawane za zaufane, nawet jeśli znajduje się w sieci wewnętrznej. MFA stanowi kluczowy komponent architektury Zero Trust, zapewniając silne uwierzytelnianie użytkowników.

Rublon sp. z o.o.

ul. Stanisława Wyspiańskiego 11 65-036 Zielona Góra

www.rublon.pl