

MFA to minimum, nie zabezpieczenie - czas to przyznac

Dlaczego uwierzytelnianie wieloskładnikowe nie wystarczy i co naprawdę chroni firme w 2026 roku

Piotr Załuski · 26.10.2026

Trzy lata temu siedziałem na post-mortem po incydencie bezpieczeństwa w jednej z firm portfelowych funduszu, w którym pracowałem. Atakujący przejął konto administratora w Google Workspace. Firma miała MFA włączone dla wszystkich. Hasła były silne. Polityka bezpieczeństwa liczyła 14 stron. I nic z tego nie pomogło, bo jeden pracownik kliknął w fałszywy ekran logowania, który wyludził od niego jednorazowy kod SMS w czasie rzeczywistym. Atak trwał może 90 sekund.

To był mój pierwszy poważny kontakt z tym, co branża nazywa MFA fatigue lub real-time phishing proxy. I od tamtej chwili mam poważny problem z tym, jak większość firm podchodzi do tematu uwierzytelniania wieloskładnikowego.

Jak MFA stało się checkboxem w prezentacji dla zarządu

Nie twierdzę, że MFA jest bezużyteczne. Twierdzę, że stało się symbolem - i to jest jego największy problem. Kiedy dyrektor IT może wpisać w slajdzie "MFA wdrożone dla 100% pracowników", wszyscy odetchną z ulgą. Zarząd kiwa głową. Audytor odznacza punkt. Ubezpieczyciel cybernetyczny obniża składkę o 15%.

Tymczasem w praktyce to wdrożenie często wygląda tak: SMS jako drugi składnik, brak polityki dostępu warunkowego, zero monitoringu anomalii logowania i aplikacje legacy obsługiwane przez konta serwisowe bez żadnego MFA. Czyli checkbox zaznaczony, bezpieczeństwo - iluzoryczne.

W 2026 roku ataki omijające MFA to już nie niszowa technika zaawansowanych grup APT. To gotowe narzędzia dostępne na forach za kilkaset dolarów. Evilginx, Modlishka, Muraena - frameworki do ataków typu adversary-in-the-middle działają na zasadzie reverse proxy i przechwytują sesje użytkownika już po udanym uwierzytelnieniu, łącznie z tokenem sesji. Kod SMS czy TOTP z aplikacji? Nieistotny. Sesja już przejęta.

Cztery błędy, które widzę najczściej

Przez ostatnie lata - najpierw w funduszu, potem przy własnych projektach - miałem okazję przyglądać się temu, jak firmy od 20 do 2000 pracowników wdrażają MFA. Wzorce są zadziwiająco powtarzalne.

SMS jako drugi składnik

SMS-y są podatne na SIM swapping. To atak, w którym przestępca przekonuje operatora telekomunikacyjnego do przeniesienia numeru ofiary na nową kartę SIM. W Polsce w 2025 roku odnotowano kilkadziesiąt udokumentowanych przypadków SIM swappingu wymierzonych w przedsiębiorców - liczba rzeczywista jest wielokrotnie wyższa, bo większość nie trafia do raportów. Jeśli twoja firma używa SMS-ów jako MFA dla dostępu do systemów

finansowych lub CRM z danymi klientow, to masz problem, który tylko czeka na realizację.

Brak wyjątków od reguły wyjątków

To brzmi jak lamigłowa, ale chodzi o coś prostego. Firmy wdrażają MFA, a potem tworzą wyjątki: "dla prezesa bo mu niewygodnie", "dla systemu legacy bo nie obsługuje", "dla konta serwisowego bo nie ma gdzie wpisać kodu". Każdy wyjątek to dziura. Atakujący nie szturmują frontu - szukają właśnie tych wyjątków.

MFA bez dostępu warunkowego

MFA samo w sobie nie wie, czy logujesz się z biura w Warszawie czy z serwera w Singapurze o 3:00 w nocy. Dostęp warunkowy (Conditional Access w Microsoft Entra ID, Context-Aware Access w Google Workspace) pozwala uzależnić wymagania uwierzytelnienia od kontekstu: lokalizacji, urządzenia, godziny, ryzyka sesji. Bez tego MFA to zamek na drzwiach, do których ktoś zostawił klucz pod wycieraczką.

Brak monitoringu po uwierzytelnieniu

Nawet jeśli atakujący nie ominie MFA, może zalogować się legalnie - przez phishing danych uwierzytelniających w połączeniu z wyludzoną kłódką. Co wtedy? Jeśli nie masz SIEM-u, alertów na anomalie behawioralne ani choćby podstawowego logowania zdarzeń, to nie wiesz, że ktoś jest w środku. Odkrycie incydentu następuje średnio po 197 dniach - to dane IBM Cost of a Data Breach z 2024 roku i nic nie wskazuje, żeby w 2026 było lepiej.

Co naprawdę działa - hierarchia skuteczności

Zanim przejdę do konkretnych, jedno zastrzeżenie: nie ma srebrnej kuli. Bezpieczeństwo to proces, nie produkt. Ale są rozwiązania, które statystycznie redukcją ryzyko o rząd wielkości więcej niż klasyczny MFA z SMS-em.

Odpowiedź na pytanie "co działa" jest więc dość prosta: FIDO2 i passkeys. Standard FIDO2 jest z definicji odporny na phishing proxy, bo klucz kryptograficzny jest powiązany z konkretną domeną. Nawet jeśli użytkownik wejdzie na fałszywą stronę wyglądającą identycznie jak prawdziwa, klucz po prostu nie zadziała - bo domena się nie zgadza. To nie jest kwestia czujności użytkownika. To kwestia matematyki.

Google ogłosiło w 2023 roku, że po wdrożeniu kluczy sprzętowych dla wszystkich pracowników nie odnotowało ani jednego udanego przejęcia konta przez phishing. Zero. Przy skali operacji Google to liczba, która powinna skłonić do refleksji każdego CISO.

Passkeys w praktyce - 2026 to już realna opcja

Jeszcze dwa lata temu passkeys były ciekawostką dla entuzjastów. Dzisiaj obsługują je: Windows Hello, macOS/iOS Face ID i Touch ID, Android, a po stronie serwisów - GitHub, Google, Microsoft, Dropbox, 1Password i dziesiątki innych. Dla firm korzystających z Microsoft Entra ID lub Okta wdrożenie passkeys dla pracowników to kwestia kilku godzin konfiguracji, nie tygodni projektu.

Koszt? Klucze sprzętowe YubiKey 5 NFC kosztują około 60-80 dolarów za sztukę. Dla

50-osobowej firmy to jednorazowy wydatek rzędu 3000-4000 dolarów. Porównaj to z medianą kosztu naruszenia danych dla małej firmy - według Verizon DBIR 2025 to ponad 30 000 dolarów, nie licząc kosztów reputacyjnych i prawnych.

Moje doświadczenie z wdrożeniem w startupie

Kiedy budowałem jeden z moich startupów, przeszliśmy przez dokładnie te ewolucje, która opisuje. Zaczeliśmy od Google Workspace z SMS-ami jako MFA - bo szybko i wszyscy to znają. Po pierwszym audycie bezpieczeństwa (który sami zainicjowaliśmy przed rozmowami z inwestorami) okazało się, że mamy trzy konta serwisowe bez jakiegokolwiek MFA, dwóch pracowników z wyjątkami "bo im nie działa aplikacja" i zero dostępu warunkowego.

Przejdźcie na TOTP zajęło tydzień. Wdrożenie dostępu warunkowego - dwa dni. Likwidacja kont serwisowych na rzecz service accounts z ograniczonymi uprawnieniami - dwa tygodnie, bo wymagało refaktoryzacji kilku integracji. Najtrudniejsza była zmiana kulturowa: przekonanie zespołu, że to nie jest biurokracja dla biurokracji, tylko realna ochrona ich pracy i danych klientów.

Bezpieczeństwo, które nie jest używane, nie istnieje. Możesz mieć najlepsze narzędzia na świecie - jeśli ludzie będą je omijać, bo są za trudne, to masz security theater, nie security.

To zdanie usłyszałem od CISO jednej z większych polskich firm fintech podczas konferencji w Krakowie i wryło mi się w pamięć. Wdrożenie MFA, które ludzie omijają przez udostępnianie kont albo używanie prostych haseł bo "i tak jest MFA", jest gorsze niż brak MFA - bo daje fałszywe poczucie bezpieczeństwa.

Co zrobić w tym tygodniu - konkretna lista

Jeśli prowadzisz firmę lub odpowiadasz za IT, oto lista działań, które mają sens niezależnie od skali organizacji:

- Audyt wyjątków MFA - sprawdź, ile kont w twoim środowisku ma wyłączone MFA lub używa SMS-ów. Zacznij od kont uprzywilejowanych (admini, finanse, HR).
- Włącz dostęp warunkowy - jeśli używasz Microsoft Entra ID lub Google Workspace, masz to dostępne bez dodatkowych kosztów w wyższych planach. Blokuj logowania z nieznanych krajów i urządzeń niezarządzanych.
- Pilotuj FIDO2/passkeys - zacznij od 5-10 osób z dostępem do krytycznych systemów. YubiKey lub wbudowane rozwiązania platformowe (Windows Hello, Touch ID).
- Monitoruj anomalie logowania - nawet podstawowe alerty na logowanie z nowego kraju lub o nietypowej godzinie. W Google Workspace to kwestia kliknięcia w ustawieniach alertów.
- Szkolenie z phishingu - nie jednorazowe, cykliczne. Narzędzia jak KnowBe4 czy Proofpoint Security Awareness Training pozwalają symulować ataki i mierzyć postęp.

MFA to nie jest cel. To punkt startowy. Firmy, które traktują go jako meta, są dokładnie tam, gdzie chcą je widzieć atakujący - zadowolone z siebie i nieprzygotowane na to, co naprawdę nadchodzi.

Gdzie jesteśmy i dokąd zmierzamy

W 2026 roku rozmawiamy już o podejściu zero trust jako nowym standardzie - nie jako

buzzwordzie z prezentacji Gartnera, ale jako realnej architekturze, która wdrażają firmy różnej wielkości. Zero trust zakłada, że żadne urządzenie, żaden użytkownik i żadna sieć nie są z definicji zaufane. Każde zadanie dostępu jest weryfikowane w czasie rzeczywistym, z uwzględnieniem kontekstu, zachowania i ryzyka.

W tym modelu MFA jest jednym z wielu sygnałów, a nie bramą. To fundamentalna zmiana perspektywy. Zamiast pytać "czy użytkownik podał właściwy kod?", system pyta "czy całość zachowania tego użytkownika w tej chwili jest spójna z tym, co wiemy o nim historycznie?".

Brzmi skomplikowanie i drogo? Dla małej firmy wdrożenie pełnego zero trust to rzeczywiście projekt na lata. Ale pierwsze kroki - dostęp warunkowy, FIDO2, monitoring anomalii - są dostępne dziś, w ramach narzędzi, za które prawdopodobnie już płacisz.

Jedyne, czego potrzebujesz, to przestać traktować MFA jako meta i zacząć traktować je jako punkt startowy. Bo nim właśnie jest.