Case Study

Kompleksowa transformacja tożsamości i automatyzacja w Ministerstwie Aktywów Państwowych

Ministerstwo Aktywów Państwowych

Wyzwanie

Głównym celem była modernizacja zarządzania dostępem oraz podniesienie poziomu bezpieczeństwa przy jednoczesnym odciążeniu działu IT z manualnych zadań administracyjnych.

- **Zarządzanie cyklem życia (JML):** Potrzeba automatyzacji procesów zatrudniania, zmian stanowisk i zwolnień (Joiner, Mover, Leaver).
- **Bezpieczeństwo dostępu zdalnego:** Konieczność silnego uwierzytelniania do kluczowych zasobów, w tym VPN.
- **Świadomość zagrożeń:** Chęć powiązania dostępu do systemów z edukacją w zakresie cyberbezpieczeństwa.

Ministerstwo Aktywów Państwowych (MAP) – instytucja rządowa odpowiedzialna za nadzór nad mieniem państwowym. Organizacja o wysokich wymaganiach w zakresie bezpieczeństwa i zgodności (compliance), zatrudniająca kilkuset pracowników, operująca w modelu hybrydowym.

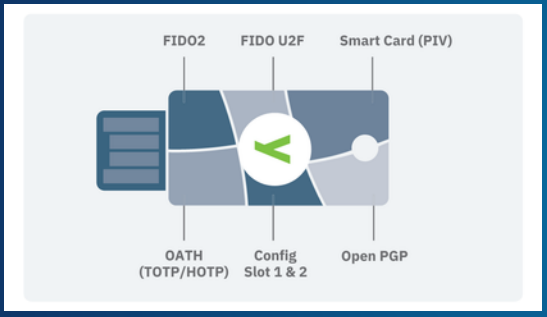
Rozwiązanie I architektura

Wdrożenie zostało podzielone na etapy, ewoluując od podstawowego zabezpieczenia do zaawansowanej ochrony opartej na analizie ryzyka. Fundamentem rozwiązania jest platforma **Okta** zintegrowana z kluczami sprzętowymi **YubiKey**.

Faza 1: Fundamenty i automatyzacja

W pierwszej fazie wdrożono kluczowe moduły Okta Identity Cloud:

- **Single Sign-On (SSO):** Centralizacja dostępu do aplikacji.
- **Universal Directory (UD):** Stworzenie jednego widoku tożsamości użytkownika.
- **Lifecycle Management (LCM):** Automatyzacja procesów JML. Źródłem prawdy (Source of Truth) pozostaje On-prem Active Directory, natomiast Okta przejmuje rolę silnika orkiestracji zmian w systemach docelowych.
- **Adaptive MFA:** Wdrożenie uwierzytelniania wieloskładnikowego, m.in. dla Palo Alto VPN.



Komponent sprzętowy (Yubico):

Wdrożono klucze YubiKey jako podstawowy, odporny na phishing składnik MFA. Dystrybucję połączono z obowiązkowymi szkoleniami z bezpieczeństwa (Security Awareness), budując kulturę "security first".

Faza 2: Rozszerzenie (Po 12 miesiącach)

Po roku system rozbudowano o zaawansowane funkcje ochrony i zarządzania dostępem:

- **Identity Threat Protection:** Wprowadzenie ciągłej oceny ryzyka sesji i użytkownika (User Risk), pozwalające na dynamiczne reagowanie na anomalie.
- **Device Access (Desktop MFA):** Zabezpieczenie logowania do stacji roboczych (Windows/macOS) wymogiem MFA, co chroni przed fizycznym dostępem osób niepowołanych.
- **Okta Workflows:** Rozwój w kierunku "Identity Governance" – tworzenie zaawansowanych ścieżek akceptacji i niestandardowych automatyzacji procesów biznesowych.

Wyniki i Korzyści

- **Pełna automatyzacja JML:** Wyeliminowanie błędów ludzkich i opóźnień w nadawaniu/odbieraniu uprawnień – dostęp jest gotowy w "Dniu 1" i natychmiast odbierany po ustaniu zatrudnienia.
- **Zero Trust:** Wdrożenie modelu "nie ufaj nikomu, weryfikuj zawsze" zarówno na poziomie sieci (VPN), jak i urządzenia (Desktop MFA).
- **Kultura bezpieczeństwa:** Fizyczne klucze YubiKey w połączeniu ze szkoleniami realnie podniosły odporność organizacji na ataki socjotechniczne.