

Case Study

Wdrożenie uwierzytelniania FIDO2 na Uniwersytecie Wrocławskim



Uniwersytet
Wrocławski

Wyzwanie

Uczelnia stanęła przed koniecznością znaczącego podniesienia poziomu bezpieczeństwa cyfrowego. Kluczowe czynniki decyzyjne obejmowały:

- Incydenty bezpieczeństwa: Rejestrowano próby nieautoryzowanego dostępu oraz incydenty związane z utratą służbowych urządzeń przez pracowników.
- Ochrona infrastruktury: Konieczność silnego zabezpieczenia dostępu do zasobów wewnętrznych realizowanego zdalnie (VPN).
- Czynniki ludzkie: Potrzeba podniesienia świadomości użytkowników ("something you have" zamiast tylko "something you know") oraz wyeliminowanie słabych haseł.

Uniwersytet Wrocławski –

jedna z najstarszych i największych uczelni w Europie Środkowej. Instytucja zarządza rozproszoną infrastrukturą oraz dostępem dla tysięcy pracowników naukowych i administracyjnych.



Rozwiązanie

Zdecydowano się na wdrożenie sprzętowych kluczy bezpieczeństwa w standardzie FIDO2/WebAuthn, uznawanym obecnie za standard odporny na phishing.

- **Wolumen:** 4 000 sztuk urządzeń.
- **Modele:** YubiKey 5 NFC oraz YubiKey 5C NFC (zapewnienie kompatybilności z portami USB-A, USB-C oraz urządzeniami mobilnymi).
- **Ekosystem tożsamości:** Microsoft Entra ID (dawniej Azure AD).
- **Bramka VPN:** Palo Alto Networks (GlobalProtect).

Architektura i integracja

Wdrożenie oparło się na nowoczesnym modelu uwierzytelniania federacyjnego:

1. **VPN (Palo Alto):** Skonfigurowany do używania protokołu SAML 2.0 do uwierzytelniania użytkowników.
2. **IdP (Entra ID):** Pełni rolę dostawcy tożsamości. Użytkownik logujący się do VPN jest przekierowywany do Entra ID.
3. **MFA (FIDO2):** Entra ID wymusza użycie klucza YubiKey jako silnego składnika uwierzytelniania (Passwordless lub 2FA). Klucz weryfikowany jest lokalnie przez PIN oraz dotyk (User Presence).

Proces wdrożenia i logistyka (YubiEnroll)

Kluczowym wyzwaniem przy skali 4000 użytkowników była dystrybucja i rejestracja kluczy. Zastosowano model **"Pre-enrollment"**:

- **Centralny zakup:** Uczelnia zakupiła pulę urządzeń na własność.
- **Masowa rejestracja (YubiEnroll):** Dział IT, wykorzystując oprogramowanie YubiEnroll, zarejestrował klucze w imieniu użytkowników bezpośrednio w Entra ID.
- **Konfiguracja:** Podczas rejestracji kluczom nadano tymczasowe, losowe kody PIN.
- **Dystrybucja:** Wstępnie skonfigurowane klucze zostały przekazane do poszczególnych działów/jednostek, a następnie wręczone użytkownikom końcowym.
- **Onboarding:** Użytkownik otrzymywał klucz gotowy do pracy, co drastycznie skróciło czas potrzebny na samodzielną konfigurację po stronie pracownika.



Wyniki i Korzyści

- **Szybkość:** Logowanie do VPN jest szybsze (dotknięcie klucza vs. przepisywanie kodów OTP).
- **Bezpieczeństwo:** Wyeliminowano ryzyko phishingu poświadczeń VPN oraz przejęcia dostępu w przypadku kradzieży samego laptopa (brak klucza sprzętowego uniemożliwia dostęp).
- **Skalowalność:** Model pre-rejestracji pozwolił na sprawne wdrożenie w dużej organizacji bez paraliżu helpdesku.

