SECFENSE

User Access Security Broker

Jak wyeliminować wszystkie ataki związane z hasłami?

Czy jesteś gotowy na rewolucję FIDO2? Dowiedz się, jak wprowadzić już dziś uwierzytelnianie odporne na phishing w całej organizacji.

81% ataków wynika z kradzieży lub słabych haseł.

63% udanych ataków pochodzi ze źródeł wewnętrznych.

33% ataków dotyczy socjotechniki.

> **Wyeliminuj te ataki, dodając odporne na phishing biometryczne MFA. Daj się namówić również na passwordless i zrezygnuj całkowicie z wykorzystywania haseł!**

MFA odporne na phishing

Uwierzytelnianie wieloskładnikowe (MFA) jest dziś absolutnym standardem bezpieczeństwa uwierzytelniania, a nie tylko dodatkiem służącym zabezpieczeniu najbardziej istotnych programów w organizacji. Polityki związane z hasłami przestają mieć już znaczenie. Zastępują je metody MFA, które skutecznie chronią przed phishingiem i socjotechniką, nawet jeśli hasła zostaną złamane.

Najwygodniejszym i najbezpieczniejszym sposobem uwierzytelniania jest obecnie FIDO2. I choć nazwa ta może nie brzmieć znajomo, to ten sposób uwierzytelniania jest powszechnie stosowany przez każdego, kto odblokowuje swój telefon odciskiem palca lub spoglądając w jego w kamerę.

Dlaczego więc tak łatwy i bezpieczny sposób uwierzytelniania nie jest wykorzystywany do uwierzytelniania we wszystkich programach, z których korzystamy w pracy i w życiu prywatnym?

Trudna implementacja

MFA jest trudne do wdrożenia. Instalacja wymaga zaangażowania programistów, modyfikowania kodu chronionych aplikacji, a co za tym idzie prowadzi często do problemów z ciągłością pracy, nieplanowanymi kosztami i licznymi komplikacjami. W wypadku dużych organizacji, mających złożoną i rozbudowywaną przez lata infrastrukturę IT, implementacja MFA może być wręcz niemożliwa.

Secfense – łatwa i szybka implementacja

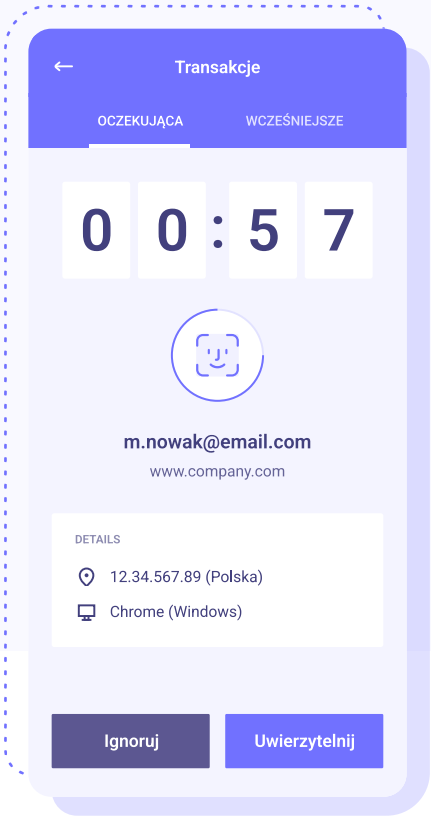
Secfense opracował technologię User Access Security Broker, dzięki której można wdrożyć dowolną metodę MFA (zarówno nowoczesne FIDO2, jak również każdą inną metodę) na dowolnej liczbie aplikacji bez żadnego kodowania.
Firmy wykorzystujące Secfense mogą:

- Całkowicie wyeliminować ryzyko związane z phishingiem i socjotechniką
- Zabezpieczyć wszystkie, a nie jedynie wybrane aplikacje
- Wdrożyć MFA w całej organizacji dla wszystkich użytkowników
- Wdrożyć i wyskalować najnowsze, jak również już używane metody MFA
- Wyeliminować koszty programistyczne implementacji (wdrożenie no-code)

Secfense Authenticator

Chcesz wdrożyć biometryczne, odporne na phishing uwierzytelnianie FIDO2 w całej organizacji, ale nie chcesz inwestować w klucze sprzętowe U2F/FIDO2?

Aplikacja Secfense Authenticator pozwala do silnego uwierzytelniania w sieci wykorzystać telefon. Dzięki aplikacji Secfense Authenticator wszyscy pracownicy Twojej organizacji, którzy mają smartfon, będą mogli kryptograficznie potwierdzać swoją tożsamość w sieci. Dokładnie w taki sam bezpieczny sposób, w jaki do tej pory robili to, wykorzystując fizyczne klucze sprzętowe U2F / FIDO2.



Umów się na rozmowę tutaj:
secfense.com/pl/kontakt