SECFENSE

Jak, już dzisiaj, wyeliminować wszystkie ataki związane z hasłami?

Czy jesteś gotowy na rewolucję FIDO2? Dowiedz się jak wprowadzić silne uwierzytelnianie w całej organizacji.

81% ataków wynika z kradzieży lub słabych haseł.

63% udanych ataków pochodzi ze źródeł wewnętrznych.

33% ataków dotyczy socjotechniki.

> **Teraz wyobraź sobie, że możesz całkowicie wyeliminować tego rodzaju ataki po prostu rezygnując z wykorzystywania haseł!**

Silne uwierzytelnianie

Silne uwierzytelnianie - czyli logowanie wykorzystujące kilka różnych składników uwierzytelniania - nie jest już jedynie dodatkiem służącym zabezpieczeniu najbardziej istotnych programów w organizacji. Silne uwierzytelnianie staje się już standadrem bezpieczeństwa. A coraz lepsze i wygodniejsze metody uwierzytelniania powodują, że hasła stają się już zbędne i wręcz szkodzą bezpieczeństwu organizacji.

Istnieje wiele alternatywnych dla haseł sposobów uwierzytelniania. Większość z nas korzystała już kiedyś z haseł jednorazowych lub powiadomień push w skrzynce elektronicznej. Do najlepszych sposobów zebezpieczenia należy uwierzytelnianie FIDO2. Choć nazwa nie brzmi znajomo to jednak uwierzytelnianie to jest wszystkim znane. Dzięki niemu bowiem możemy odblokować smartfon odciskiem palca lub spoglądając w kamerę telefonu. Dlaczego więc tak łatwy i bezpieczny sposób uwierzytelniania nie jest wykorzystywany do uwierzytelniania we wszystkich programach, z których korzystamy?

Problemem jest trudna implementacja

Silne uwierzytelnianie jest trudne do wdrożenia. Instalacja wymaga zaangażowania programistów, modyfikowania kodu chronionych aplikacji,
a co za tym idzie może prowadzić do problemów z ciągłością pracy, wysokich kosztów i wielu komplikacji. W wypadku dużych organizacji, w których infrastruktura informatyczna rozbudowywana była przez lata przez różne zespoły specjalistów wykorzystujących różne technologie i języki programowania, implementacja silnego uwierzytelniania może być wręcz niemożliwa do zrealizowania.

Rozwiązaniem jest implementacja bez ingerencji w kod chronionych aplikacji

A co gdyby można było wdrożyć silne uwierzytelnianie za pomocą zaledwie kilku kliknięć? Bez kodowania? Bez zatrudniania programistów? A wszystko to na ogromną skalę, silne uwierzytelnianie wprowadzone nie na jednym lecz na setkach lub tysiącach programów jednocześnie?

User Access Security Broker umożliwia globalne użycie silnego uwierzytelniania i zabezpieczenie wszystkich programów w organizacji.

Secfense zbudował rozwiązanie User Access Security Broker dzięki któremu możliwym jest wdrożenie silnego uwierzytelniania w dowolnej liczbie aplikacji i bez żadnego kodowania.

A co z hasłami?

Na koniec wisieńka na torcie. Jeśli Twoja organizacja jest gotowa na przejście na uwierzytelnianie bez haseł, czyli tak zwane passwordless, i chciałaby całkowicie zrezygnować z haseł, możemy Ci w tym pomóc.

Zapytaj nas, jak pomogliśmy bankowi wejść na ścieżkę do uwierzytelniania bez haseł wykorzystując obecnie wykorzystywaną technologię bezhasłowego uwierzytelniania stacji roboczych i przeniesienia tego mechanizmu na całą organizację. Podczas krótkiej rozmowy opowiemy jak wyglądało to wdrożenie i jakie efekty przyniosło, jak również pomożemy Ci zdecydować jaki jest najlepszy sposób na zabezpieczenie twojej organizacji.

Umów się na rozmowę tutaj:

https://secfense.com/contact