SECFENSE

Bezpieczeństwo Twoich użytkowników na nowym poziomie

Co jest nie tak z dwuskładnikowym uwierzytelnianiem (2FA) ?

Phishing, man-in-the-middle, replay czy malware to przykłady popularnych i skutecznych ataków na konta użytkowników. Od dawna znane jest także remedium na te ataki - dobre dwuskładnikowe uwierzytelnianie, czyli dodatkowy element, którym użytkownik legitymuje się podczas logowania. Czasem jest to klucz kryptograficzny, czasem cecha biometryczna, a innym razem jednorazowe hasło wygenerowane w aplikacji mobilnej.

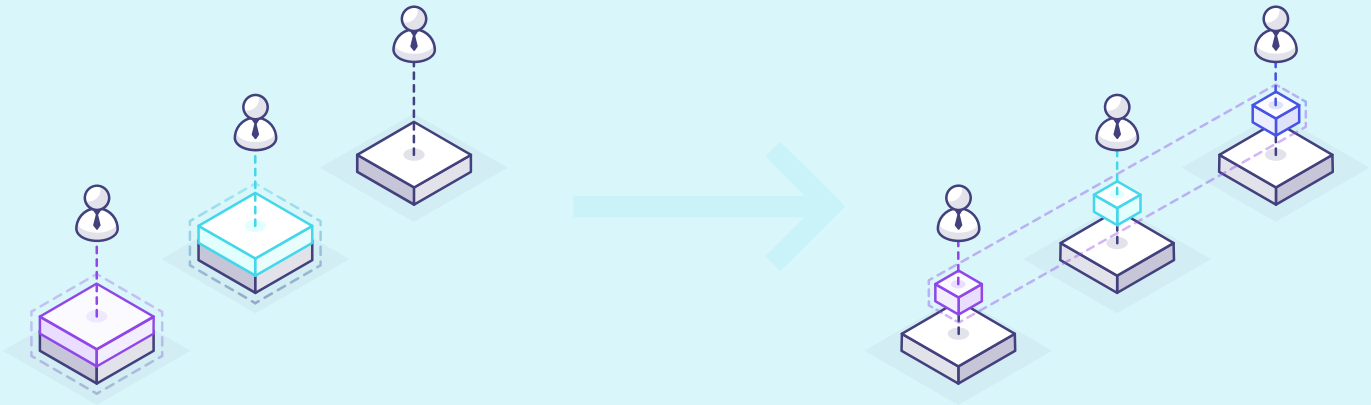
Standardowym rozwiązaniem wciąż jednak pozostaje statyczne hasło - jedyna przeszkoda, jaką musi pokonać atakujący, aby przejąć konto ofiary. Wyjście poza standard wiąże się z ingerencją w oprogramowanie docelowej aplikacji i “przyszycie” do niej danej metody 2FA. Proceder ten ma swoje konsekwencje:

- wysokie koszty implementacji i utrzymania
- wpuszczenie obcego kodu do aplikacji
- potencjalny vendor-lock, a w konsekwencji wysokie koszty i brak rozwoju
- związanie się z metodą nieskuteczną lub złamaną (vide SMS token)
- metoda wdrożona w jednej aplikacji nie daje ochrony (nie portuje się) w innych

PROBLEMEM NIE JEST 2FA, A SPOSÓB JEGO IMPLEMENTACJI

SECFENSE

Poznaj Secfense.
2FA przeniesione na zupełnie nowy poziom



2FA bez Secfense

Ochroną objęci wybrani użytkownicy w wybranych aplikacjach przy użyciu zadeklarowanej metody.

2FA z Secfense

Ochroną objęci wszyscy użytkownicy we wszystkich aplikacjach przy użyciu dowolnej metody.

Pomyśl o wirtualizacji. Wprowadzenie abstrakcji pomiędzy fizycznym sprzętem a wyższymi warstwami zmieniła świat IT nieodwracalnie. Podobną ścieżką podążyliśmy w Secfense. Secfense powoduje, że 2FA przestaje być domeną świata software'u, a staje się częścią elastycznej infrastruktury. Budowanie na tej infrastrukturze odbywa się bez ingerencji w warstwę poniżej, czyli chronione aplikacje i bazy danych.

Niezależność

Ochrona aplikacji bez konieczności znajomości ich struktury

Elastyczność

Możliwość zaaplikowania dowolnej metody 2FA dla dowolnej aplikacji

Skalowalność

Ochrona dostępna dla całej organizacji, niezależnie od lokalizacji aplikacji (cloud / on-premises)

SECFENSE JEST DLA 2FA TYM, CZYM WIRTUALIZACJA DLA INFRASTRUKTURY IT.

SECFENSE

Secfense w praktyce - jak to działa?

Krok 1

Secfense implementowany jest w organizacji. Występuje w roli fizycznego albo wirtualnego klastra umieszczanego przed albo za load-balancerem chronionych aplikacji

Krok 2

Ruch do chronionej aplikacji przepływa swobodnie przez Secfense. W zależności od umiejscowienia, Secfense może terminować ruch SSL/TLS.

Krok 3

Secfense wprowadzony w tryb uczenia analizuje charakterystykę ruchu sieciowego na linii użytkownik-aplikacja i buduje profil aplikacji.

Krok 4

Znalezione wzorce zostają zaaplikowane. Skutkuje to kształtowaniem ruchu sieciowego w taki sposób, że od logujących się użytkowników wymagane jest 2FA

Kroki następne

Budowane są polityki, zgodnie z którymi dla zadanych warunków aktywowana jest wybrana metoda 2FA. Rekomendowana jest metoda U2F oparta na fizycznych kluczach kryptograficznych oraz metoda TOTP oparta na Google Authenticator. Wszystkie dostępne teraz i w przyszłości metody 2FA zostaną dostarczone z Secfense. W ramach usługi maintenance dostępność metod 2FA nie jest niczym ograniczona.