SECFENSE + Sandis

Case Study

Wdrożenie User Access Security Broker w grupie WAGAS

Sandis wybrał i wdrożył w Grupie WAGAS rozwiązanie Secfense, by szybko zabezpieczyć 27 różnych aplikacji i ponad 5000 użytkowników oraz zrealizować rekomendacje Komisji Nadzoru Finansowego i wprowadzić w życie wymagania rozporządzenia DORA.

Sandis to integrator i dostawca oprogramowania dla branży ubezpieczeniowej. Oferuje oprogramowanie do dystrybucji produktów ubezpieczeniowych, a także świadczy usługi w zakresie zarządzania infrastrukturą i rozwojem aplikacji. Z aplikacji Sandis codziennie korzystają tysiące sprzedawców produktów ubezpieczeniowych, a oferowane rozwiązania wspierają obsługę wielu kontaktów o zasięgu ogólnopolskim.

Jednym z filarów strategii firmy jest zapewnienie odbiorcom wysokiego standardu bezpieczeństwa danych, które przetwarzają. To dlatego Sandis poświęca wiele uwagi nowym wymagania w zakresie cyberbezpieczeństwa, w szczególności tym nakładanym na całą branżę.

Rekomendacje KNF i rozporządzenie DORA a silne uwierzytelnianie

19 października 2022 roku opublikowane zostało stanowisko Urzędu Komisji Nadzoru Finansowego w sprawie działań zakładów ubezpieczeń i reasekuracji w zakresie cyberbezpieczeństwa. Urząd Komisji zaznacza w nim, że „w obliczu zintensyfikowanych działań cyberprzestępców, brak stosowania silnego, wieloskładnikowego uwierzytelnienia klientów jest nieakceptowalnym ryzykiem”.

Dodatkowo 16 stycznia 2022 roku w życie weszło rozporządzenie DORA (Digital Operational Resilience Act), stanowiące część strategii cyberbezpieczeństwa Unii Europejskiej. Firmy i instytucje mają czas do 17 stycznia 2025 roku na dostosowanie się do nowych przepisów. A przepisy te, obejmujące także zewnętrznych dostawców usług ICT dla podmiotów działających w branży finansowej, wymagają wdrożenia polityk i protokołów dotyczących silnych mechanizmów uwierzytelniania w ramach zarządzania ryzykiem ICT.

Sytuacja Sandis przed wdrożeniem

W związku z tymi wymaganiami Sandis w ramach współpracy z grupą WAGAS stanął przed wyzwaniem zabezpieczenia zarówno oferowanych przez siebie aplikacji, jak i aplikacji zewnętrznych dostawców. Sandis zdecydował się na wprowadzenie dodatkowej ochrony w postaci mechanizmów uwierzytelniania wieloskładnikowego opartego na FIDO, by użytkownicy aplikacji mogli się do nich bezpiecznie logować, unikając popularnych cyberzagrożeń – phishingu, przejęcia konta oraz kradzieży danych swoich i klientów. Projekt utrudniała mnogość systemów, różnorodność technologii i wiek niektórych aplikacji. W ramach analizy przedwdrożeniowej firma zweryfikowała, że użytkownicy korzystają z bardzo różnych platform klienckich: komputerów stacjonarnych, laptopów, tabletów, smartfonów i tradycyjnych telefonów komórkowych. Każde z tych urządzeń różni się zaawansowaniem technologicznym i funkcjami, a także poziomem zabezpieczeń.

Rozwiązania udostępniane tysiącom użytkowników w Grupie WAGAS hostowane są w trzech centrach danych. A korzysta z nich wiele tysięcy użytkowników:

3
Centra Danych

+27
Aplikacji

- **DA 1:** 14 aplikacji
- **DA 2:** 4 aplikacje
- **DA 3:** 9 aplikacji

Główne wyzwania:

- różnorodne technologie
- wielu dostawców
- aplikacje na różnym etapie cyklu rozwoju, aktualnie rozwijane i utrzymywane,
- wygaszane i te “na emeryturze”
- dostarczenie rozwiązania MFA, które zapewniałoby standaryzowany 'look and feel".

Wybór rozwiązania

Sandis wziął pod uwagę dwa różne scenariusze działania – wdrożenie mechanizmów MFA w ramach poszczególnych aplikacji oraz wykorzystanie scentralizowanego, zunifikowanego rozwiązania, jakim jest Secfense.

Secfense dostarcza rozwiązanie User Access Security Broker, które pozwala szybko objąć silnym uwierzytelnianiem dowolny system i aplikację, bez ingerencji w ich kod.

Sandis dokonał wyboru, analizując TOC – Total Cost of Ownership, czyli pełny obraz kosztów **„od zakupu do wycofania”**. Do kluczowych analizowanych elementów należą:

- CAPEX – nakłady
- OPEX – utrzymanie, rozwój
- koszty ukryte: przestoje, utrata produktywności, pomoc koleżeńska

Firma wzięła pod uwagę między innymi:

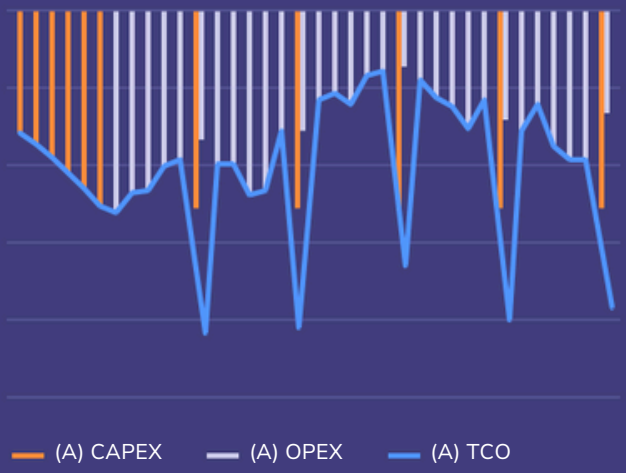
- development inicjalny
- development w cyklu życia
- utrzymanie
- administrację
- koszty braku spójności (szkolenia, obsługę call center, obsługę helpdesk)

Porównanie kosztów obu scenariuszy (scenariusz A – wdrożenie organiczne oraz scenariusz B – wdrożenie User Access Security Broker) nie pozostawiło żadnych wątpliwości co do większej opłacalności skorzystania z rozwiązania Secfense. Wdrożenie zabezpieczeń MFA na poziomie każdej aplikacji z osobna byłoby zbyt kosztowne, długotrwałe i trudne w utrzymaniu.

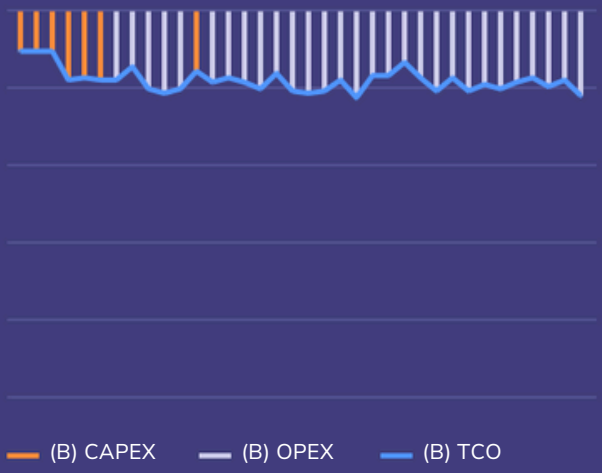
Analiza scenariuszowa

Sandis

A



B



Inne istotne cechy rozwiązania Secfense

Sandis zwrócił uwagę także na inne cechy User Access Security Broker:

- pozwala wdrożyć mechanizmy silnego uwierzytelniania na wielu aplikacjach
- w kilka tygodni
- nie wymaga ingerencji w kod
- umożliwia zastosowanie dowolnego drugiego składnika uwierzytelniania

Sandis obok FIDO, dedykowanej aplikacji mobilnej oraz haseł jednorazowych generowanych przez aplikacje typu Authenticator pozostawił także możliwość uwierzytelniania za pomocą dostępnych na wszystkich urządzeniach klienckich kodów wysyłanych przez SMS-y czy e-maile.

Przebieg wdrożenia

Sandis już w pierwszym etapie wdrożenia zabezpieczył 11 oferowanych przez siebie aplikacji, aby docelowo udostępnić zabezpieczenia dla 27 aplikacji hostowanych w trzech różnych centrach danych.
Szybkość i łatwość wdrożenia User Access Security Broker sprawiła, że Sandis
pominął etap Proof of Concept. Zespół firmy uznał, że prosta implementacja
i sposób licencjonowania bazujący na subskrypcji zawierającej m.in. wsparcie
pozwalają od razu przejść do etapu wdrożenia i działania produkcyjnego.

Efekt wdrożenia User Access Security Broker

Sandis bardzo szybko zapewnił nowoczesną ochronę ponad 5000 użytkowników. I jest dziś w pełni przygotowany do tego, by zabezpieczać kolejne aplikacje i zapewniać zgodność z regulacjami Unii Europejskiej oraz rekomendacjami Komisji Nadzoru Finansowego.