CASE STUDY

PASSUS AMBIENCE ANALIZUJE RUCH HTTP NA POTRZEBY DZIAŁÓW BIZNESOWYCH I BEZPIECZEŃSTWA IT W INSTYTUCJI FINANSOWEJ

KLIENT

Prezentowane studium przypadku opisuje projekt realizowany w jednej z instytucji wchodzących w skład międzynarodowej grupy finansowej. Klient ten świadczy usługi m.in. z zakresu bankowości dla blisko 4 mln klientów w Polsce zarówno osób prywatnych jak i przedsiębiorstw. Z bankowej aplikacji mobilnej korzysta obecnie blisko 1 milion klientów.

PRZED WDROŻENIEM

Kluczowe aplikacje bankowości elektronicznej banku zostały zainstalowane w dwóch niezależnych lokalizacjach geograficznych. W obu lokalizacjach zastosowano load balancery, które odpowiadały m.in. za deszyfrowanie ruchu https na http. Do uwierzytelniania i autoryzacji użytkowników i urządzeń wykorzystywano usługę Active Directory.

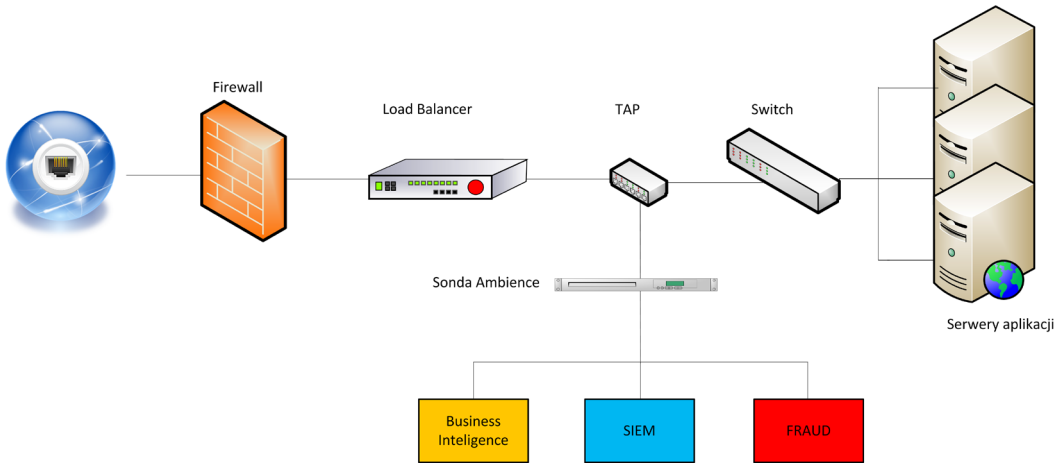
KLUCZOWE OCZEKIWANIA KLIENTA

Dział IT otrzymał zadanie wdrożenia rozwiązania, które będzie monitorować ruch http w czasie rzeczywistym. Wybrane dane miały być następnie przekazywane do systemu klasy Business Intelligence operującego na zbiorach Big Data w celu dalszej ich analizy. Ze względu na dynamicznie zmieniające się potrzeby analityczne jak i planowany rozwój aplikacji, ważnym kryterium wyboru rozwiązania była jego elastyczność. W szczególności system powinien umożliwiać zmianę parametrów poszczególnych analizatorów jak i algorytmów ich działania. Użytkownik powinien mieć m.in możliwość definiowania czym jest sesja (w rozumieniu systemu transakcyjnego, nie połączenia sieciowego) oraz powiązania wybranych zdarzeń lub ich sekwencji w oparciu o login podany przez użytkownika w momencie logowania. Ważnym kryterium było też spełnienie restrykcyjnych wymogów polityki bezpieczeństwa Banku obejmujących m.in. anonimizację danych wrażliwych, wielostopniowe procedury akceptacji konfiguracji systemu, a także udokumentowane metody przetwarzania pozyskanych informacji. Wśród dodatkowych wymagań wymieniono skalowalność, geolokalizację, filtrowanie ruchu na poziomie warstwy 7 oraz monitorowanie procedur logowania do systemu. Zapotrzebowanie działów biznesowych zostało uzupełnione o wymagania działu bezpieczeństwa IT. System powinien umożliwić wyodrębnienie incydentów niosących znamiona fraudu i przekazywać dane związane z tymi zdarzeniami do specjalistycznych narzędzi umożliwiających ich analizę.

ROZWIĄZANIE

Analiza ruchu http i integracja z systemem Business Analytics

Ruch między użytkownikami i aplikacjami internetowymi Klienta jest monitorowany za pośrednictwem sond Passus Ambience. Urządzenie działa pasywnie - podłączone do portu load balancera F5 Networks w czasie rzeczywistym przechwytuje kopię strumienia bez dodatkowego obciążenia sieci.



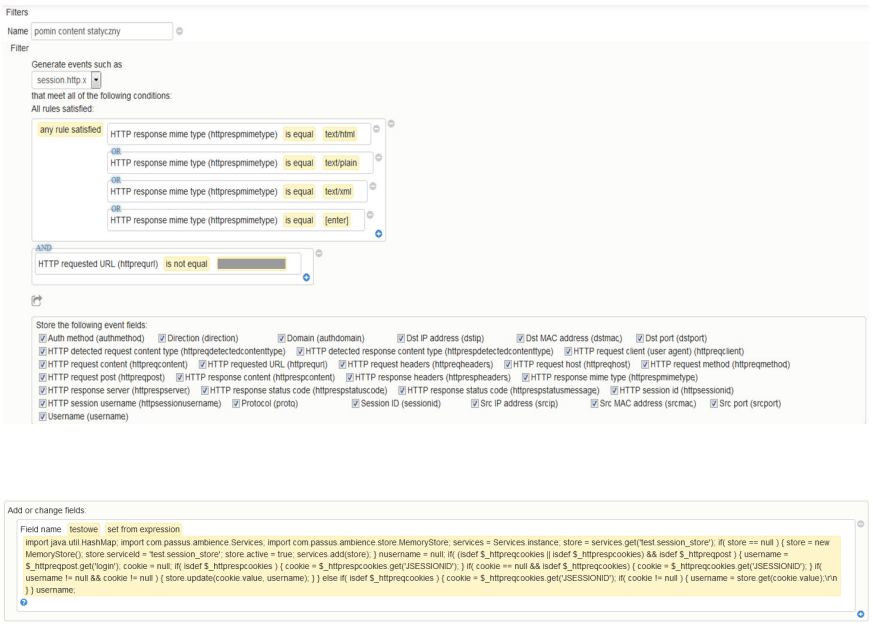
Rys. 1 Schemat sieci z wykorzystaniem sondy Passus Ambience

Analizator zainstalowany na sondzie łączy odpowiedzi z zapytaniami, a filtry korelacyjne działające na poziomie warstwy 7 pozwalają precyzyjnie wyselekcjonować ruch, który jest istotny z punktu widzenia działów biznesowych. Dzięki temu, nieistotne zdarzenia odrzucane są już na poziomie sondy Ambience. System np. nie loguje tych zapytań, których wynikiem jest wyświetlenie zawartości statycznej, np. grafiki, js, css. Dane spełniające kryteria zdefiniowane przez użytkownika biznesowego jako istotne są przesyłane do rozwiązania Business Intelligence korzystającego z technologii Hadoop. Selekcja danych na poziomie sondy odciąża sieć i zmniejsza obciążenie systemu Business Inteligence, co ma także istotny wpływ na koszty licencji.

Definiowanie warunków, które muszą spełnić określone pola, aby event w ogóle był zgłoszony przez analizator. W tym wypadku założono dwa filtry: przekazujący jedynie eventy, których odpowiedź była określonego typu: html, plain, xml lub pusta i wywoływany adres był inny niż bank/test.html.

Określenie pól, które będą opisywać dany event poprzez ich wybór z predefiniowanej listy.

Definiowanie nowych pól użytkownika z wykorzystaniem wbudowanych skryptów w tym wypadku języka MVEL.



Rys. 2 Przykład definiowania analizatorów Passus Ambience.

Pozyskane za pomocą Passus Ambience dane wykorzystywane są m.in. do personalizacji treści strony w oparciu o zachowanie użytkownika w trakcie sesji, a także do prowadzenia zaawansowanych analiz i segmentacji użytkowników serwisów www.

Analiza ruchu http pod kątem fraudów. Zgodność z polityką Compliance

Równolegle z analizą zdarzeń biznesowych, Passus Ambience monitoruje ruch http pod kątem ewentualnych ataków lub nadużyć. Analizowany jest m.in. ruch z wybranych źródeł np. określonych adresów, czas przebywania na poszczególnych stronach, sekwencja zdarzeń wskazująca na anomalie w bezpieczeństwie np. pominięcie niezbędnych kroków w procesie. Informacje o zdarzeniach noszących znamiona fraudu przekazywane są do systemu SIEM. Passus Ambience dostosowano także do restrykcyjnych wymagań polityki Compliance. Procesy uwierzytelniania i autoryzacji administratorów rozwiązania Passus Ambience zintegrowano z usługą Active Directory. Część danych wrażliwych, nieprzydatnych w dalszych analizach jest trwale usuwana bezpośrednio przez analizator na sondzie. Dane wrażliwe (np. niezbędne do identyfikacji uczestnika sesji) są anonimizowane, aby uniemożliwić ich odczyt przez osoby nieupoważnione. System monitoruje i rejestruje wszelkie zmiany w konfiguracji analizatorów. System akceptacji zmian w konfiguracji minimalizuje ryzyko błędów lub nadużyć ze strony osób administrujących systemem.

PO WDROŻENIU – PODSUMOWANIE

Rozwiązanie Ambience dostarcza w czasie rzeczywistym dane o zachowaniu użytkowników aplikacji webowych, w tym bankowości elektronicznej. Informacje te są wykorzystywane zarówno w aspekcie biznesowym, jak i pod kątem ewentualnych ataków. Wdrożenie systemu zajęło kilka godzin - a dostępność podczas wdrożenia zespołu programistów producenta pozwoliła szybko dostosować wybrane funkcje do indywidualnych oczekiwań Klienta. Dzięki temu, iż system działa w sposób pasywny i umożliwia filtrowanie danych na poziomie sondy, jego działanie nie ma wpływu na wydajność środowiska IT. Możliwość samodzielnego modyfikowania parametrów i algorytmów, wg których działają poszczególne analizatory pozwola szybko dostosowywać ich działanie do zmieniających się potrzeb w przyszłości. Zaawansowane rozwiązania do anonimizacji i wbudowane mechanizmy kontroli zmian w konfiguracji systemu spełniły restrykcyjne wymagania polityki compliance instytucji finansowej.

Passus Spółka Akcyjna jest polskim integratorem i dostawcą wysoko specjalizowanych rozwiązań informatycznych obejmujących w szczególności:

- rozwiązania do monitorowania i rozwiązywania problemów z wydajnością sieci oraz aplikacji;
- rozwiązania z zakresu bezpieczeństwa IT m.in. do wykrywania podatności, zabezpieczenia sieci, aplikacji oraz danych przed zaawansowanymi atakami oraz zagrożeniami wskutek nadużyć lub zaniedbań wewnętrznych;
- rozwiązania do projektowania, budowy i modernizacji wydajnych sieci WiFi w tym realizacji specjalistycznych projektów „pod klucz" (m.in. captive portal, lokalizacja zasobów, dostęp WiFi w środkach komunikacji i transportu).

Tym, co wyróżnia Passus SA spośród firm integracyjnych, jest elastyczność i koncentracja na rzeczywistych potrzebach Klienta. Płaska i przejrzysta struktura organizacyjna spółki oraz ograniczone do niezbędnego minimum procedury pozwalają szybko i skutecznie reagować na oczekiwania Klienta. Ponad 20 lat współpracy z firmami oraz instytucjami z Polski i z zagranicy zaowocowało znajomością uwarunkowań biznesowych i technicznych tych organizacji. Do grona Klientów w Polsce należą tak wymagający partnerzy, jak m.in. Ministerstwo Obrony Narodowej, T-Mobile, Narodowy Bank Polski, Grupa Enea, Centrum Onkologii w Gliwicach, Komisja Nadzoru Finansowego, Orange, PGE, Swedwood, PKO BP, PZU, Volkswagen Polska, Politechnika Rzeszowska, Orlen, Grupa PKP SA, Wojskowy Instytut Medyczny.

Bazując na własnych produktach i usługach oraz technologiach uznanych światowych producentów, Passus SA tworzy i wdraża rozwiązania, precyzyjnie dostosowane do wymagań klienta. Spółka zapewnia klientom kompleksową obsługę, począwszy od analizy potrzeb, przez planowanie, usługi wdrożeniowe, szkolenia pracowników, aż po opiekę serwisową oraz posprzedażną. Oferowane rozwiązania są przygotowywane w oparciu o produkty własne jak i uznanych światowych dostawców. Firma jest partnerem takich producentów jak: Riverbed (Riverbed Premier Partner), Core Security (wyłączny dystrybutor w Polsce), GD Fidelis (rekomendowany Partner w Polsce), Fluke Networks (Premier Advantage Partner Plus), Cisco (Premier Partner) Invea-Tech (Platinium Partner) oraz Qualys. Passus posiada także własny zespołów programistów i inżynierów realizujących projekty na indywidualne zamówienie. Na bazie zebranych doświadczeń, w maju 2014 roku, zespół ten przygotował unikalne w skali światowej rozwiązanie umożliwiające identyfikację nadużyć i incydentów w oparciu o analizę ruchu sieciowego – Passus Security Anomaly Detector.

Firma Passus SA powstała w wyniku wydzielenia Działu Sieci i Bezpieczeństwa IT z Passus sp. z o.o., działającej w branży IT od 1992 roku. Zatrudnia blisko 30 wykwalifikowanych pracowników – inżynierów, programistów i specjalistów. Potwierdzeniem kompetencji zespołu, obok wielu udanych wdrożeń, jest blisko 40 indywidualnych certyfikatów m.in.: poświadczenie bezpieczeństwa osobowego do klauzuli „Tajne" oraz „NATO Secret", CISA, CISSP, Riverbed Certified Solutions Professional, Cisco Associate oraz Professional w zakresie R&S (routing & switching), Security oraz Wireless, Core Impact Certified Professional, Audytor wiodący ISO 27001, Riverbed Network and Application Performance Management Qualified Trainer oraz Fluke Networks Application Performance Appliance Certified Trainer.