# AUDYT BEZPIECZEŃSTWA APLIKACJI I STRON WEBOWYCH

## W CELU ZMINIMALIZOWANIA RYZYKA UTRATY DANYCH PRZEZ SŁABE PUNKTY APLIKACJI I STRON WEBOWYCH ZALECAMY CYKLICZNE WYKONYWANIE AUDYTÓW BEZPIECZEŃSTWA

W bankach mamy do czynienia z aplikacjami webowymi, które mają dostarczać Klientom pełnej informacji na temat produktów banku i z aplikacjami, dzięki którym Klient wykonuje operacje w ramach bankowości internetowej.

Ze względu na wzrost zagrożenia cyberprzestępstwami wyłudzającymi dane Klientów, a także próbami włamań do aplikacji webowych zalecamy cykliczne wykonywanie testów podatności tych aplikacji. W czasie standardowego audytu bezpieczeństwa informacji wykonujemy audyt aplikacji internetowych na zasadzie testów white box. Testy te z reguły potwierdzają zabezpieczenie tych aplikacji na zadowalającym poziomie.

Szczególnie zalecamy wykonanie analiz aplikacji webowych w środowiskach testowych, które jednoznacznie potwierdzą stan ich bezpieczeństwa.

Należy pamiętać, że przy stale rozwijającym się ruchu sieciowym przy wykorzystaniu urządzeń mobilnych, stale wzrasta zapotrzebowanie Klientów na sprawne aplikacje, które zapewnią bezawaryjną i bezpieczną obsługę aplikacji bankowych.

Należy uświadomić sobie, że ataki na aplikacje odbywają się przez 24 godziny na dobę i nie uwzględniają dni świątecznych – wolnych od pracy. Stosowane standardowe zabezpieczenia jak zapory ogniowe, systemy wykrywania włamań i inne produkty zabezpieczające sieć, mogą nie powstrzymać zagrożeń pochodzących z internetu co może skutkować przestojami w pracy, kradzieżami danych, naruszeniem bezpieczeństwa.

Jednym ze sposobów analizy bezpieczeństwa są testy koncentrujące się na ocenie bezpieczeństwa aplikacji pod kątem słabych punktów, wad technologicznych, luk w zabezpieczeniach i podatności, które mogą być furtką do ataku na aplikacje. Audyt kończy się wygenerowaniem raportu, w którym zdefiniowane są wszystkie słabe punkty aplikacji, jej podatności i braki technologiczne. Zawsze staramy się wskazać Klientowi najprostsze rozwiązanie, które szybko wyeliminuje stwierdzone luki w systemie.



Servus Comp Sp. z o.o. Sp. K.
30-019 Kraków ul. Mazowiecka 25/502
tel. 12 631-91-22 biuro@servus-comp.pl
www.premiumbank.zadbajobezpieczenstwo.pl

Analiza podatności aplikacji i stron webowych prowadzona jest przy pomocy m.in.:

- narzędzi technologicznych wykorzystujących narzędzia open source jak i narzędzia komercyjne
- wykonywanie testów ręcznie – mapowanie aplikacji i testowanie logiczne. Aplikacje dzielone są na podstawowe moduły i obszary funkcjonalne. Następuje dogłębna analiza każdego modułu w celu identyfikacji plików, folderów i istniejących parametrów. Odbywa się mapowanie przepływu danych między komponentami wraz z ich relacjami logicznymi. Następnie symulowane są scenariusze potencjalnych podatności.

Skorelowanie i powiązanie tworzonej listy podatności następuje po zestawieniu danych z przeprowadzonych testów wykonanych ręcznie i automatycznie. Następnie, na dostępnej bazie występujących podatności, zostają opracowane odpowiednie profile zagrożeń. Następnie odbywa się kolejna analiza wsteczna prowadzona przez ekspertów, którzy ponownie analizują ewentualne słabe obszary, których nie wykryto podczas analizy automatycznej.

Specjaliści zestawiają ręcznie opisy, dowody, referencje i specyficzne podatności dotyczące testowanych aplikacji.

Jak działamy:

- automatycznie - wykorzystując skanery do badania podatności, problemów technicznych
- weryfikacja ręczna – brak fałszywych alarmów
- wykorzystujemy specjalistyczne narzędzia w zależności od infrastruktury docelowej
- wykorzystanie narzędzi komercyjnych oraz open source
- korelacja danych z wielu narzędzi i źródeł
- OWAPS top 10
- SANS TOP 20
- testowanie założeń koncepcyjnych
- zestawienie informacji dla poszczególnych aplikacji
- zestawienie dokładnych dowodów wraz z eksploracją
- przedstawienie rozwiązania problemu i zalecenia dotyczące zastanego środowiska



Servus Comp Sp. z o.o. Sp. K.
30-019 Kraków ul. Mazowiecka 25/502
tel. 12 631-91-22 biuro@servus-comp.pl
www.premiumbank.zadbajobezpieczenstwo.pl

W celu uzyskania pełnej informacji w omawianych zakresach zapraszamy do kontaktu:

**Andrzej Popiołek**
Audytor Wiodący SZBI, Członek IIA Polska
+48 602 220 749 andrzej.popiolek@servus-comp.pl

**Ewa Niesiołowska**
Audytor Wiodący SZBI, Członek IIA Polska
+48 531 364 287 ewa.niesiolowska@servus-comp.pl

**Anna Stręk**
Audytor Wiodący SZBI, Członek IIA Polska
+48 781 555 025 anna.strek@servus-comp.pl

**Anna Kramarczyk**
Kierownik ds. projektów IT
+48 794 671 787 anna.kramarczyk@servus-comp.pl

**Servus Comp Sp. z o.o. Sp.k.**
ul. Mazowiecka 25/502, 30-019 Kraków
Sąd Rejonowy dla Krakowa – Śródmieście,
XI Wydział Gospodarczy Krajowego Rejestru Sądowego
NIP: 6772394344 | Regon: 362815411 | KRS: 0000582481
https://zadbajobezpieczenstwo.pl
https://premiumbank.zadbajobezpieczenstwo.pl