LIFE IS FOR SHARING.

Kontakt

Zespół Cybersecurity
e-mail: B2B_Security_Squad@t-mobile.pl

Badanie bezpieczeństwa i zabezpieczeń aplikacji WEB

Ocena wrażliwości bezpieczeństwa aplikacji WEB

Aplikacje WEB-owe to częsty cel działania cyberprzestępców ze względu na fakt, że na ogół wystawione są w sieci Internet jako interfejs komunikacyjny dla użytkownika zewnętrznego. Poza standardową konfiguracją na etapie wdrożenia i utrzymania rzadko mają dodatkowe warstwy ochrony, pozwalające na detekcję oraz zabezpieczenie przed zagrożeniami. Podatności i błędy aplikacji WEB-owych to jedna z podstawowych przyczyn występowania incydentów zagrożenia bezpieczeństwa teleinformatycznego, związanych z kompromitacją serwisów, wyciek danych klientów, pracowników, której skutkiem jest uzyskanie punktu dostępowego do zasobów organizacji, a następnie traktowanie go jako pośrednika komunikacyjnego do dalszych działań cyberprzestępczych.

Autorska metodyka badania wrażliwości

Dokonaj oceny wrażliwości na zagrożenia, badając stan i poziom zabezpieczeń aplikacji WEB-owych oraz systemów ochronnych WAF.

Badanie to ma na celu:

- Aktywne sprawdzanie podatności aplikacji WEB-owych pod kątem znanych podatności.
- Ocenę skuteczności WAF w zakresie wykrywania i blokady zagrożeń.
- Dynamiczną analizę kodu źródłowego aplikacji w celu identyfikacji błędów programistycznych.
- Identyfikację złośliwego oprogramowania i treści, które mogą być osadzone w serwisach WEB-owych.

Wynikiem przeprowadzonego badania będzie raport zawierający:

- Ocenę stanu zabezpieczeń, błędów konfiguracyjnych i podatności.
- Informację o wykrytych zagrożeniach.
- Wytyczenie odnośnie do kierunku rozwoju oraz zmian koniecznych, aby zwiększyć poziom bezpieczeństwa organizacji.
- Rekomendację działań naprawczych.

Dlaczego Twoja firma potrzebuje takiego badania?

- Wzrost poziomu cyberbezpieczeństwa w organizacji.
- Podniesienie poziomu ochrony danych klientów i pracowników.
- Normy i regulacje (np. ustawa o prawie telekomunikacyjnym, KNF-D, dyrektywa NIS – ustawa o krajowym systemie cyberbezpieczeństwa).
- Audyt (wewnętrzy, zewnętrzny).
- Usprawnienie czynności związanych z procesem zarządzania incydentami zagrażającymi cyberbezpieczeństwu.