Załącznik nr 1 do Umowy – Opis przedmiotu zamówienia

OGÓLNE ZASADY

- Zamawiający ma prawo do zlecenia audytu bezpieczeństwa Systemu firmie zewnętrznej zgodnie z ustalonym harmonogramem. Termin ten nie może być dłuższy niż 30 dni od dnia poinformowania Usługodawcy. Podczas audytu przerwa w pracy użytkowników nie może być dłuższa niż 5 dni roboczych.
- Audyt będzie przeprowadzony przez firmę zewnętrzną z zachowaniem pełnej współpracy na styku Zamawiający-Wykonawca-Usługodawca.
- Usługodawca nie może odmówić przeprowadzenia audytu bezpieczeństwa Systemu.
- Audytowi bezpieczeństwa podlegać będą wszystkie elementy składające się na całość rozwiązania Systemu tj. serwery aplikacyjne, bazy danych, moduły wewnętrzne aplikacji oraz aplikacje klienckie.

WYMAGANY ZAKRES PRAC ZWIĄZANYCH Z AUDYTEM BEZPIECZEŃSTWA OBEJMUJE:

I. Weryfikacja realizacji przez Wykonawcę systemu wymogów bezpieczeństwa.

II. Weryfikacja bezpieczeństwa elementów architektury audytowanego systemu, w tym bezpieczeństwo punktów styku Systemu z wewnętrznymi i zewnętrznymi serwisami, bazami danych oraz serwisami centralnymi (np. Węzeł Identyfikacji Elektronicznej, ePUAP lub inne wykorzystane w danym projekcie)

III. Standardowe czynności związane z audytem bezpieczeństwa aplikacji:

1. Przeprowadzenie testów penetracyjnych typu blackbox i greybox.

2. Badanie aplikacji pod kątem odporności na ataki w zakresie:

- autoryzacji, uwierzytelniania i kontroli dostępu,

- zarządzania sesją,

- walidacji wejścia,

- mechanizmów kryptograficznych oraz danych wrażliwych,

- konfiguracji systemu,

- logowania,

3. Analizę podatności i zagrożeń,

4. Badanie bezpieczeństwa API, w tym identyfikacja luk w autoryzacji, manipulacje danymi, itp.

5. Analizę konfiguracji (serwery, systemy operacyjne, bazy danych, usługi, porty),

6. Podczas testów szukane będą podatności w oparciu o OWASP TOP 10:

A01. Błędy kontroli dostępu- (Broken Access Control)

A02. Błędy kryptograficzne- (Cryptographic Failures)

A03. Wstrzyknięcia- (Injection)

A04. Błędy w konstrukcji systemu- (Insecure Design)

A05. Błędna konfiguracja zabezpieczeń- (Security Misconfiguration)

A06.Wrażliwe i podatne komponenty- (Vulnerable and Outdated Components)

A07. Błędy w identyfikacji i uwierzytelnianiu- (Identification and Authentification Failures)

A08. Błędy oprogramowania i integralności danych- (Software and Data Integrity Failures).

A09. Awarie logowania i monitorowania bezpieczeństwa- (Security Loggin and Monitoring Failures)

A10. Fałszowanie żądań po stronie serwera- (Server-Side Request Forgery (SSRF)

7. Dodatkowo powinny być analizowane takie elementy aplikacji webowych jak:

- Nagłówki wysyłane przez serwer

- Pliki cookie

- Skrypty javascript

- Elementy RIA aplikacji webowych (pliki SWF, aplety java)

- Czasy odpowiedzi serwera przy poszczególnych operacjach

- Reakcja na dane wejściowe w zapytaniach (nagłówki, agent przeglądarki, wadliwe zapytania protokołu HTTP)

- Próby aplikacyjnych ataków DoS/ DDoS

- Mechanizm HTTP Strict Transport Security

- Aktualność wtyczek i bibliotek

- Enumeracje haseł i loginów

- XSS (Skrypty między witrynami)

Testy zakładają również badanie pod kątem bezpieczeństwa zachowania logiki aplikacji. W tej części testów osoby audytujące utworzą szereg scenariuszy, które następnie będą przetestowane. Scenariusze są opracowywane pod kątem logiki działania danego systemu.

Dodatkowo przeprowadzone testy będą symulowały próby przeprowadzenia ataków na aplikację ze strony:

- Użytkownika niezalogowanego

- Klienta aplikacji

9. Prace powinny być wykonywane z uwzględnieniem najlepszych praktyk oraz metodyk takich jak OSSTMM v3, ISSAF oraz OWASP TOP 10.

10. Testy penetracyjne zostaną powtórzone nie później niż dwa miesiące po przekazaniu i omówieniu wyników i raportów testów właściwych.

11. Testy penetracyjne zakończą się prezentacją i omówieniem metodyki Audytu dla 10 osób wskazanych przez Zamawiającego

Zamówienie w ramach Zamówienia Podstawowego

System 1:

Audyt oraz re-audyt bezpieczeństwa systemu informatycznego wraz z prezentacją i omówieniem metodyki Audytu dla maksymalnie 10 osób wskazanych przez Zamawiającego

System informatyczny składający się z:

aplikacji webowej w której w skład wchodzi:

- **maksymalnie 4 adresy https://**
- **maksymalnie 12 serwerów** (w tym możliwość wskazania serwerów w różnych środowiskach- testowe oraz produkcyjne)
- **maksymalnie 3 bazy danych** (w tym możliwość wskazania baz danych w różnych środowiskach- testowe oraz produkcyjne)

System 2:

Audyt oraz re-audyt bezpieczeństwa systemu informatycznego wraz z prezentacją i omówieniem metodyki Audytu dla maksymalnie 10 osób wskazanych przez Zamawiającego

System informatyczny składający się z:

aplikacji webowej w której w skład wchodzi:

- **maksymalnie 1 adres https://**
- **maksymalnie 3 serwery** (w tym możliwość wskazania serwerów w różnych środowiskach- testowe oraz produkcyjne)
- **maksymalnie 2 bazy danych** (w tym możliwość wskazania baz danych w różnych środowiskach- testowe oraz produkcyjne)

Szkolenia:

Szkolenia w formie warsztatu z zakresu:

- SQL Injection - XSS - ataki CSRF - XXE - path traversal

Zamówienie w ramach Prawa Opcji

WARIANT nr 1:

Audyt oraz re-audyt bezpieczeństwa systemu informatycznego wraz z prezentacją i omówieniem metodyki Audytu dla maksymalnie 10 osób wskazanych przez Zamawiającego

System informatyczny składający się z:

aplikacji webowej w której w skład wchodzi:

- **maksymalnie 4 adresy https://**
- **maksymalnie 12 serwerów** (w tym możliwość wskazania serwerów w różnych środowiskach- testowe oraz produkcyjne)
- **maksymalnie 3 bazy danych** (w tym możliwość wskazania baz danych w różnych środowiskach- testowe oraz produkcyjne)

WARIANT nr 2:

Audyt oraz re-audyt bezpieczeństwa systemu informatycznego wraz z prezentacją i omówieniem metodyki Audytu dla maksymalnie 10 osób wskazanych przez Zamawiającego

System informatyczny składający się z:

aplikacji webowej w której w skład wchodzi:

- **maksymalnie 2 adresy https://**
- **maksymalnie 6 serwerów** (w tym możliwość wskazania serwerów w różnych środowiskach- testowe oraz produkcyjne)
- **maksymalnie 3 bazy danych** (w tym możliwość wskazania baz danych w różnych środowiskach- testowe oraz produkcyjne)

WARIANT nr 3:

Audyt oraz re-audyt bezpieczeństwa systemu informatycznego wraz z prezentacją i omówieniem metodyki Audytu dla maksymalnie 10 osób wskazanych przez Zamawiającego

System informatyczny składający się z:

aplikacji webowej w której w skład wchodzi:

- **maksymalnie 1 adres https://**
- **maksymalnie 3 serwery** (w tym możliwość wskazania serwerów w różnych środowiskach- testowe oraz produkcyjne)
- **maksymalnie 2 bazy danych** (w tym możliwość wskazania baz danych w różnych środowiskach- testowe oraz produkcyjne)