Załącznik nr 1 do SIWZ

Opis Przedmiotu Zamówienia

1. W ramach Zamówienia, Wykonawca będzie zobowiązany do świadczenia usług polegających na wykonywaniu:
   a. audytów bezpieczeństwa oraz testów penetracyjnych systemów IT,
   b. audytów kodu źródłowego,
   c. audytów bezpieczeństwa oraz testów penetracyjnych infrastruktury,
2. Przedmiot Umowy obejmuje dwa tryby zamówień: audyt pełny i audyty ad hoc
   a. Raz w roku kalendarzowym Wykonawca zobowiązuje się do wykonania pełnego audytu aplikacji i infrastruktury, co oznacza usługi wymienione w pkt 1 a) i 1) c powyżej w zakresie całej infrastruktury i wszystkich systemów Zamawiającego określonych poniżej w tabeli Wykaz systemów Zamawiającego
   b. Ilość zamówień na w trybie ad hoc audytów wybranych systemów lub aplikacji, lub ich części oraz bezpieczeństwa elementów infrastruktury, nie przekroczy w czasie trwania Umowy ilości 14 zamówień, przy czym rocznie będzie to maksymalnie 7.
3. Testy bezpieczeństwa i audyty kodu obejmować będą co najmniej następujące elementy:

Lp.	Nazwa usługi	Zakres
1	Audyt kodu aplikacji webowej	• Określenie powierzchni ataku • Określenie obszarów podwyższonego ryzyka • ~~Określenie zgodności ze standardami organizacji~~ • Identyfikacja klas podatności • Weryfikacja wdrożonych zaleceń
2	Test penetracyjny aplikacji	• Testy penetracyjne serwera WWW • Testy penetracyjne serwera aplikacyjnego • Testy penetracyjne aplikacji (komponenty dostępne publicznie) • Testy penetracyjne aplikacji po uwierzytelnieniu) • Testy penetracyjne interfejsów bazy danych • Testy penetracyjne bazy danych z poziomu użytkownika
3	Test penetracyjny sieci lokalnej	• Testy penetracyjne punktu styku z Internetem • Kontrolowana próba obejścia zabezpieczeń • Testy uwierzytelniania sieciowego • Testy szczelności VLANów i poufności przesyłanych informacji • Testy penetracyjne systemów operacyjnych

4. W ramach realizacji Przedmiotu Umowy zostaną wykonane następujące badania bezpieczeństwa, zgodnie z poniższym opisem

a. Ocena podatności - identyfikacja podatności występujących w systemach informatycznych, przy pomocy automatycznych narzędzi testujących. W przypadku tego typu badania nie występuje próba wykorzystania wykrytych podatności, w celu uzyskania dostępu do testowanych systemów.
b. Test penetracyjny - określenie faktycznego stanu bezpieczeństwa polegające na symulacji prób złamania lub ominięcia zabezpieczeń. W trakcie testów stosowane są metody i narzędzia, którymi zwykle posługują się potencjalni napastnicy. Zidentyfikowane podatności są wykorzystywane do przejęcia kontroli nad testowanymi systemami oraz do dalszych prób eskalacji ataku. Umożliwia to określenie potencjalnej skali naruszenia bezpieczeństwa, która wystąpi, jeśli te podatności zostaną wykorzystane przez hackerów.
c. Testy realizowane jako testy penetracyjne funkcjonalności dostępnych z zewnątrz oraz jako ocena podatności infrastruktury w obszarze funkcji dostępnych z sieci wewnętrznej.

5. Badania obejmą co najmniej podatności co najmniej na podatności wymienione w OWASP Top 10 Most Critical Web Application Security Risks
6. W ramach testów zostaną wykorzystane dwa rodzaje testów penetracyjnych: black box (z minimalną wiedzą o audytowanej aplikacji) oraz crystal box (z pełną wiedzą i kontem użytkownika w audytowanej aplikacji).
7. Testom bezpieczeństwa i audytom podlegać będą systemy informatyczne i aplikacje użytkowane przez Zamawiającego, zarówno zewnętrzne jak i wewnętrzne, funkcjonujące w określonym środowisku Zamawiającego.
8. Testom bezpieczeństwa podlegać będą systemy w przeważającej większości oparte o technologie: PHP, JSP/Java, Ruby on Rails, Python, Perl, ASP/ASP.NET.
9. Testy aplikacji w większości będą przeprowadzane na instancjach przeznaczonych do testowania (nieprodukcyjnych).
10. Testy mogą wymagać obecności Wykonawcy w siedzibie Zamawiającego.
11. W przypadku środowisk utrzymywanych w centrach danych partnerów zewnętrznych, Zamawiający każdorazowo zapewni zgodę operatora centrum danych na wykonanie testów.

Wykaz systemów Zamawiającego

Lp.	*Rodzaj audytu*	*Obszar*
1	Testy penetracyjne i ocena podatności oraz Audyt kodu aplikacji	Lokalny System Informatyczny – aplikacja do naboru i obsługi wniosków o dofinansowanie
2	Testy penetracyjne i ocena podatności	aplikacja „System do rejestrowania umów i przychodów z projektów”
3	Testy penetracyjne i ocena podatności	aplikacja ”Portal rejestracyjny dla ekspertów”
4	Testy penetracyjne i ocena podatności	witryna www
5	Testy penetracyjne i ocena podatności	aplikacja ”Portal ankiet”
6	Testy penetracyjne i ocena podatności	aplikacja ”System do naboru wniosków w konkursach międzynarodowych”
7	Testy penetracyjne i ocena podatności	system kadry-płace-finanse-księgowość
8	Testy penetracyjne i ocena podatności	system samoobsługi pracowniczej
9	Testy penetracyjne i ocena podatności	EZD - Elektroniczne Zarządzanie Dokumentacją
10	Testy penetracyjne i ocena podatności	infrastruktura Intranet
11	Testy penetracyjne i ocena podatności	styk z siecią Internet – OwnCloud
12	Testy penetracyjne i ocena podatności	styk z siecią Internet - Poczta e-mail – usługi MS Exchange Server plus OWA
13	Testy penetracyjne i ocena podatności	styk z siecią Internet
14	Ocena podatności	infrastruktura teleinformatyczna
15	Testy penetracyjne i ocena podatności	wskazane fragmenty sieci wewnętrznej
~~16~~	~~Raport z testów~~	~~udokumentowane wyniki prowadzonych badań audytowych~~
~~17~~	~~Retesty zakończone Raportem z retestów~~	~~ponowne testy całości badanego środowiska i aplikacji/systemów przeprowadzane po wprowadzeniu zmian, także tych wiążących się z wdrożeniem zaleceń poaudytowych~~