

OPIS PRZEDMIOTU ZAMÓWIENIA

Zakup usługi eksperckiej - testy penetracyjne

Przedmiotem zamówienia jest usługa wykonania testów penetracyjnych systemów informatycznych Szpitala w ramach projektu Rozwój usług cyfrowych w Samodzielnym Publicznym Zakładzie Opieki Zdrowotnej Wojewódzkim Szpitalu Specjalistycznym nr 3 w Rybniku w ramach KPO na lata 2021-2026 DZIAŁANIE 1.1.2 „Przyspieszenie procesów transformacji cyfrowej ochrony zdrowia poprzez dalszy rozwój usług cyfrowych w ochronie zdrowia” będąca elementem komponentu D „Efektywność, dostępność i jakość systemu ochrony zdrowia”.

Zakres usługi oraz warunki realizacji zostały opisane poniżej.

Przeprowadzane testy mają wykazać na jakim poziomie są systemy teleinformatyczne Szpitala.

Wynik testów będzie wsadem do audytu cyberbezpieczeństwa.

Zakres usługi:

Testy penetracyjne infrastruktury IT

1. Wprowadzenie

- 1.1. Przedmiotem zamówienia jest wykonanie usług testów penetracyjnych infrastruktury IT Zamawiającego zgodnie z obowiązującymi standardami bezpieczeństwa informacji i najlepszymi praktykami branżowymi.
- 1.2. Usługi obejmują identyfikację podatności, próbę ich eksploatacji oraz raport z rekomendacjami naprawczymi.

2. Cel zamówienia

Celem zamówienia jest

- 2.1. kompleksowa ocena bezpieczeństwa infrastruktury IT;
- 2.2. identyfikacja podatności i luk w zabezpieczeniach;
- 2.3. dostarczenie Zamawiającemu rzetelnego raportu z wnioskami i rekomendacjami;
- 2.4. weryfikacja skuteczności zastosowanych mechanizmów ochronnych.

3. Zakres usług

Testy penetracyjne infrastruktury IT obejmują:

Usługa powinna objąć co najmniej:

- 3.1. Testy zewnętrzne – symulacja ataków z internetu;
- 3.2. Testy wewnętrzne – symulacja ataku z sieci wewnętrznej;
- 3.3. Testy infrastruktury sieciowej – analiza routerów, switchy, zapór, IDS/IPS, VPN;
- 3.4. Testy systemów serwerowych – analiza serwerów Windows/Linux, usług katalogowych, usług sieciowych;

- 3.5. Testy usług i aplikacji – analiza systemów webowych, usług dostępnych w ramach infrastruktury;
- 3.6. Testy konfiguracji i polityk bezpieczeństwa – analiza konfiguracji bazowej i polityk dostępu;
- 3.7. Ocena podatności na ataki socjotechniczne (opcjonalnie) – phishing, vishing (jeśli Zamawiający to przewiduje).

4. Metodyka i standardy

Wykonawca przeprowadzi testy zgodnie z uznanymi standardami i metodykami, takimi jak:

- 4.1. OWASP Testing Guide;
- 4.2. OSSTMM;
- 4.3. PTES (Penetration Testing Execution Standard);
- 4.4. NIST SP 800-115.

lub metodyki równoważne.

Testy powinny być przeprowadzone z zachowaniem zasad bezpieczeństwa, minimalizując wpływ na środowisko produkcyjne.

5. Etapy realizacji

5.1. Etap I – Analiza wstępna i planowanie

- 5.1.1. zebranie informacji o środowisku, zasobach i celach testów;
- 5.1.2. opracowanie harmonogramu i scenariuszy testowych;
- 5.1.3. uzyskanie akceptacji od Zamawiającego.

5.2. Etap II – Testowanie penetracyjne

- 5.2.1. przeprowadzenie testów zgodnie z zaakceptowanym planem;
- 5.2.2. dokumentowanie przebiegu testów;
- 5.2.3. rejestrowanie wykrytych podatności.

5.3. Etap III – Raportowanie

- 5.3.1. przygotowanie **Raportu częściowego roboczego** dla Zamawiającego;
- 5.3.2. przygotowanie **Raportu końcowego** zawierającego szczegółowe wyniki, opisy podatności i rekomendacje;
- 5.3.3. prezentacja wyników Zamawiającemu.

6. Wymagania dotyczące raportów

Raporty powinny zawierać co najmniej:

- 6.1. opis środowiska testowanego;
- 6.2. wykaz wykonanych testów i metodyki;
- 6.3. wykryte słabości i podatności;
- 6.4. poziomy ryzyka (np. CVSS lub inna metodyka oceny ryzyka);
- 6.5. rekomendacje naprawcze;
- 6.6. listę artefaktów (np. logi, zrzuty ekranowe, dowody eksploatacji).

Raport ma być sporządzony w języku polskim (opcjonalnie wersja angielska, jeśli Zamawiający wymaga).

7. Wymagania minimalne wobec Wykonawcy

Wykonawca musi:

- 7.1. posiadać udokumentowane doświadczenie w realizacji usług testów penetracyjnych infrastruktury IT;
- 7.2. dysponować specjalistami posiadającymi odpowiednie certyfikaty (np. OSCP, CEH, CISSP – opcjonalnie wskazane);
- 7.3. zapewnić poufność i bezpieczeństwo informacji zgodnie z umową;
- 7.4. posiadać procedury bezpieczeństwa i ochrony danych.

8. Warunki techniczne i organizacyjne

- 8.1. Zamawiający udostępni Wykonawcy niezbędne informacje, adresy IP, zakresy, dane konfiguracyjne i dokumentację do przeprowadzenia testów.
- 8.2. Testy powinny być wykonywane w sposób kontrolowany, z uprzednim powiadomieniem wyznaczonych osób Zamawiającego.

9. Poufność

Wykonawca zobowiązuje się do:

- 9.1. zachowania poufności wszelkich informacji uzyskanych w związku z realizacją testów;
- 9.2. podpisania umowy o poufności (NDA) przed rozpoczęciem prac;
- 9.3. zastosowania środków ochrony danych zgodnych z RODO i wewnętrznymi wymaganiami Zamawiającego.

10. Kryteria oceny wykonania zamówienia

- 10.1. Poprawność i kompletność przeprowadzonych testów.
- 10.2. Jakość raportów, czytelność i adekwatność rekomendacji.
- 10.3. Zgodność realizacji z przyjętymi standardami.

Termin realizacji zadania - do dnia 26.06.2026 r.

UWAGA:

1. W przypadku zastosowania przez Zamawiającego w opisie przedmiotu zamówienia odniesień lub nazw specyfikacji technicznych, aprobat, technologii, funkcjonalności lub norm, Zamawiający dopuszcza zaoferowanie rozwiązań co najmniej równoważnych z opisywanymi. Wykonawca, który w celu realizacji Zamówienia powołuje się na rozwiązania co najmniej równoważne z opisywanym przez Zamawiającego, jest obowiązany wykazać, że oferowane przez Wykonawcę rozwiązania spełniają wymagania określone przez Zamawiającego.

2. Jeżeli w jakimkolwiek dokumencie postępowania znajduje się jakikolwiek znak towarowy, znak handlowy jakiegoś wyrobu, nazwa własna (handlowa), patent czy pochodzenie – należy przyjąć, że Zamawiający podał taki opis ze wskazaniem na typ i dopuszcza zastosowanie materiałów, urządzeń, sprzętu i wyposażenia o co

najmniej równoważnych parametrach technicznych w odniesieniu do parametrów podanych pod pojęciem typu. Wykonawca, który w celu realizacji Zamówienia powołuje się na rozwiązania co najmniej równoważne, jest obowiązany wykazać, że oferowane przez Wykonawcę rozwiązania spełniają wymagania określone przez Zamawiającego.

Potwierdzam spełnienie opisanych powyżej wymogów.

..... dnia
(miejscowość)

.....
(podpis(y) osoby (osób) upoważnionej do
występowania w imieniu Wykonawcy