

## **Szczegółowy Opis Przedmiotu Zamówienia**

**Nazwa: „Zakup usługi wykonania testów bezpieczeństwa infrastruktury sieciowej na rzecz KPRM”**

Przedmiotem zamówienia jest wykonanie usługi przeprowadzenia testów bezpieczeństwa sieciowej infrastruktury zewnętrznej (w tym publicznie dostępne usługi i systemy) i wewnętrznej (w tym infrastruktura sieciowa, systemy aplikacyjne i urządzenia dostępne w sieci wewnętrznej) na rzecz Kancelarii Prezesa Rady Ministrów.

### **I. Zakres prac**

#### **1. Testy zewnętrzne (External Penetration Tests)**

- 1) Identyfikacja usług sieciowych wystawionych do sieci publicznej,
- 2) Testy bezpieczeństwa serwerów, urządzeń brzegowych (firewalle, routery, VPN), aplikacji webowych i portali udostępnianych użytkownikom zewnętrznym,
- 3) Próby obejścia mechanizmów uwierzytelniania i autoryzacji,
- 4) Analiza podatności na ataki powszechnie znane (np. SQLi, XSS, RCE, CSRF, Directory Traversal, SSRF),
- 5) Weryfikacja aktualności i konfiguracji certyfikatów SSL/TLS,

#### **2. Testy wewnętrzne (Internal Penetration Tests)**

- 1) Analiza segmentacji sieci i poprawności separacji środowisk,
- 2) Ocena bezpieczeństwa kontrolerów domeny, serwerów plików, systemów pocztowych i bazodanowych,
- 3) Testy uprawnień użytkowników i mechanizmów uwierzytelniania (Active Directory, LDAP),
- 4) Próby eskalacji uprawnień w systemach wewnętrznych,
- 5) Analiza zabezpieczeń stacji roboczych i konfiguracji systemów operacyjnych,

#### **3. Testy aplikacji krytycznych**

- 1) Przegląd bezpieczeństwa wybranych aplikacji wskazanych przez Zamawiającego,
- 2) Testy zgodnie z metodologią OWASP.

### **II. Warunki realizacji zamówienia**

#### **1. Warunki techniczne przeprowadzania testów:**

- 1) Testy zostaną przeprowadzone dla infrastruktury zewnętrznej oraz wewnętrznej Zamawiającego,
- 2) Testy wewnętrzne zostaną przeprowadzone w dwóch scenariuszach:
  - bez uwierzytelnienia (symulacja podłączenia nieautoryzowanego urządzenia do sieci),
  - z wykorzystaniem konta domenowego zwykłego użytkownika (AD);
- 3) Infrastruktura wewnętrzna objęta testami obejmuje około 900 stacji roboczych i 120 serwerów,
- 4) Brak aplikacji webowych, usług klient-serwer oraz brak systemów wystawionych do Internetu, za wyjątkiem serwera VPN,

- 5) Cała infrastruktura znajduje się w jednej podsieci (wspólna maska IP), bez fizycznej segmentacji sieciowej,
  - 6) Segmentacja i kontrola dostępu realizowane są – jeśli w ogóle – wyłącznie na poziomie konfiguracji poszczególnych hostów (host-based firewall, reguły lokalne),
  - 7) W ramach testów zostanie udostępniony zdalny dostęp do specjalnie przygotowanej maszyny (Linux) umieszczonej wewnątrz sieci KPRM, z której prowadzone będą wszystkie działania testowe.
  - 8) Maszyna testowa musi mieć pełną łączność sieciową z pozostałymi hostami w podsieci.
2. Wymagania ogólne przeprowadzania testów:
- 1) Testy prowadzone będą w godzinach ustalonych z Zamawiającym, z uwzględnieniem minimalizacji wpływu na dostępność usług,
  - 2) Testy będą realizowane w środowisku produkcyjnym, przy zachowaniu zasad bezpieczeństwa i akceptacji ryzyka przez Zamawiającego,
  - 3) Wszystkie informacje uzyskane w trakcie prac mają charakter poufny i nie mogą być wykorzystywane przez Wykonawcę poza realizacją zamówienia,
  - 4) Prawa autorskie do Raportu Końcowego i wyników testów zostaną przekazane Zamawiającemu,
  - 5) Szczegółowy Raport Końcowy, zawierający m.in. wyniki przeprowadzonych testów Raport musi zostać objęty klauzulą „Zastrzeżone”, jeśli spełnione zostaną przesłanki wyrażone w art. 5 ust. 4 ustawy o ochronie informacji niejawnych.
3. Wykonawca przestrzega zasad równości szans i niedyskryminacji oraz zasady równości kobiet i mężczyzn, jako zasad horyzontalnych obowiązujących przy realizacji zamówienia współfinansowanego ze środków unijnych w ramach programu „Inwestycja C3.1.1. Konkurs Grantowy - Cyberbezpieczny Rząd”, określonych w Wytycznych dotyczących realizacji zasad równościowych w ramach funduszy unijnych na lata 2021-2027, dostępnych na stronie Portalu Funduszy Europejskich (pod adresem <https://www.funduszeuropejskie.gov.pl/strony/o-funduszach/dokumenty/wytyczne-dotyczace-realizacji-zasad-rownosciowych-w-ramach-funduszy-unijnych-na-lata-2021-2027-1/>).
4. Wykonawca zapewni, że wszystkie czynności związane z realizacją przedmiotu zamówienia będą planowane i wykonywane w sposób zapewniający dostępność oraz niedyskryminację wobec jakiegokolwiek grupy osób, w tym osób z niepełnosprawnościami.
  5. Wykonawca uwzględni w swojej ofercie i w realizacji zamówienia wymagania odnoszące się do dostępności produktów i usług (np. zgodność z tzw. „Standardami dostępności” określonymi w Wytycznych – o ile dotyczy) oraz usługi wdrożeniowe (szkolenia, dokumentacja) muszą być dostępne dla osób z niepełnosprawnościami.
  6. W swojej ofercie Wykonawca załączy oświadczenie o spełnieniu powyższych zasad oraz opis działań i mechanizmów jakie przewiduje w celu ich zapewnienia (np. zapewnienie dostępności sprzętu/oprogramowania, usługi szkoleniowe dostępne dla osób z niepełnosprawnościami, równy dostęp do zasobów w projekcie etc.).
  7. Zamawiający zastrzega sobie prawo kontroli w zakresie spełniania powyższych zasad równościowych – Wykonawca musi umożliwić audyt, inspekcję lub przekazać dokumentację potwierdzającą zgodność z wytycznymi.

### **III. Termin realizacji**

Wykonawca zrealizuje przedmiot umowy, o którym mowa w ust. 2, w terminie do 65 dni kalendarzowych, licząc od dnia podpisania Umowy.

1. Przygotowanie i planowanie harmonogramu testów w uzgodnieniu z Zamawiającym,
2. Przeprowadzenie testów zewnętrzne i wewnętrzne, w terminie uzgodnionym z Zamawiającym za pośrednictwem poczty elektronicznej,
3. Analiza wyników i opracowanie raportu (zwanego dalej „Raportem Końcowym”),
4. Prezentacja wyników i przekazanie Raportu Końcowego.

### **IV. Wymagania wobec wykonawcy**

1. Doświadczenie w realizacji co najmniej 3 usług testów penetracyjnych w jednostkach administracji publicznej lub instytucjach o podobnym poziomie złożoności, w ciągu ostatnich 3 lat.
2. Dysponowanie zespołem posiadającym certyfikaty branżowe potwierdzające kompetencje w obszarze testów bezpieczeństwa, np.:
  - 1) OSCP (Offensive Security Certified Professional),
  - 2) CISSP, CISA (dla nadzoru merytorycznego),
  - 3) Stosowanie uznanych metodyk testowania, np. OWASP, PTES, NIST,
  - 4) Zapewnienie pełnej poufności i ochrony informacji uzyskanych w trakcie realizacji usługi,
  - 5) OSCE.
3. Wykonawca musi prowadzić działalność zgodną z zasadami zrównoważonego rozwoju oraz nie może być wykluczony z możliwości realizacji projektów finansowanych ze środków KPO.
4. Wykonawca musi mieć zdolność do przetwarzania informacji niejawnych oznaczonych klauzulą „zastrzeżone” w rozumieniu ustawy o ochronie informacji niejawnych, a w szczególności:
  - 1) posiadać pełnomocnika ds. ochrony informacji niejawnych,
  - 2) posiadać pracowników zdolnych merytorycznie sporządzić raport oraz legitymujących się:
    - aktualnym poświadczeniem bezpieczeństwa upoważniającym do dostępu do krajowych informacji niejawnych lub aktualnym upoważnieniem kierownika jednostki organizacyjnej do dostępu do informacji niejawnych o klauzuli „zastrzeżone”,
    - aktualnym zaświadczeniem o odbyciu szkolenia w zakresie ochrony informacji niejawnych,
  - 3) posiadać akredytowany system teleinformatyczny, aby zgodnie z przepisami wytworzyć raport, o którym mowa w cz. II, ust. 2, pkt. 5. W przypadku braku spełnienia tego wymogu Zamawiający dopuszcza wytworzenie raportu w siedzibie Zamawiającego, przy użyciu akredytowanych systemów teleinformatycznych KPRM.