Załącznik nr 1 do zapytania ofertowego

OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest przeprowadzenie testów bezpieczeństwa (pentestów) systemów informatycznych Starostwa Powiatowego, obejmujących:

1. Pentest wewnętrzny infrastruktury oraz sieci teleinformatycznej Starostwa Powiatowego,
2. Pentest zewnętrzny aplikacji mapowej udostępnianej publicznie (test z perspektywy Internetu).

Celem zamówienia jest identyfikacja podatności bezpieczeństwa, ocena odporności systemów na potencjalne ataki oraz wskazanie rekomendacji naprawczych w celu podniesienia poziomu cyberbezpieczeństwa.

Zadanie jest dofinansowane przez Unię Europejską w ramach Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) „Cyberbezpieczny samorząd"; Priorytet II: Zaawansowane usługi cyfrowe; Działanie 2.2 – Wzmocnienie krajowego systemu cyberbezpieczeństwa. Umowa o powierzenie grantu o numerze FERC.02.02-CS.01-001/23/0891/FERC.02.02-CS.01-001/23/2024.

1. Zakres zamówienia

1.1. Pentest wewnętrzny sieci i infrastruktury Starostwa Powiatowego

Pentest wewnętrzny obejmuje symulację działań atakującego posiadającego dostęp do sieci lokalnej Starostwa (np. pracownik, osoba nieuprawniona po uzyskaniu dostępu fizycznego lub logicznego).

Zakres testów obejmuje w szczególności:

- infrastrukturę sieciową (LAN, VLAN, routing, segmentację sieci),
- serwery fizyczne i wirtualne,
- systemy operacyjne serwerowe i stacje robocze (w zakresie uzgodnionym),
- usługi sieciowe (AD, DNS, DHCP, LDAP, SMB, RDP, HTTP/HTTPS itp.),
- mechanizmy uwierzytelniania i autoryzacji (w tym Active Directory),
- polityki haseł i uprawnień,
- konfigurację zabezpieczeń,
- możliwość eskalacji uprawnień,
- podatności wynikające z błędnej konfiguracji,
- możliwość ruchu bocznego (lateral movement),
- wykrywanie znanych podatności (CVE) oraz błędów logicznych
- Wykrywanie podatności w dostępie do aplikacji dziedzinowych

Pentest powinien być realizowany w modelu grey-box lub black-box (do wyboru przez Zamawiającego), z wykorzystaniem uzgodnionych danych dostępowych lub bez nich.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

1.2. Pentest zewnętrzny aplikacji mapowej

Pentest zewnętrzny dotyczy publicznie dostępnej aplikacji mapowej, udostępnianej przez Starostwo Powiatowe, dostępnej z sieci Internet.

Zakres testów obejmuje w szczególności:

- testy bezpieczeństwa aplikacji webowej,
- testy podatności OWASP Top 10 (aktualna wersja),
- testy uwierzytelniania i autoryzacji (jeżeli występują),
- testy odporności na ataki:
  - SQL Injection,
  - XSS (Stored / Reflected / DOM),
  - CSRF,
  - IDOR,
  - SSRF,
  - LFI / RFI,
  - deserializacja,
  - błędy logiki biznesowej,
- analizę nagłówków bezpieczeństwa,
- analizę konfiguracji HTTPS / TLS,
- testy dostępności nieudokumentowanych funkcji i endpointów API,
- testy bezpieczeństwa danych przetwarzanych przez aplikację.

Pentest realizowany w modelu black-box, bez dostępu do kodu źródłowego.

2. Metodyka realizacji

Testy bezpieczeństwa muszą być przeprowadzone zgodnie z uznanymi standardami, w szczególności:

- OWASP Testing Guide,
- PTES (Penetration Testing Execution Standard),
- NIST SP 800-115,
- ISO/IEC 27001 oraz ISO/IEC 27002 (w zakresie adekwatnym).

Testy muszą być realizowane manualnie, z wykorzystaniem narzędzi automatycznych wyłącznie jako wsparcia, a nie jedynej metody badania.

3. Produkty końcowe (rezultaty)

Wykonawca zobowiązany jest do dostarczenia odrębnych raportów dla każdego pentestu:

3.1. Raport z pentestu wewnętrznego

3.2. Raport z pentestu zewnętrznego aplikacji mapowej

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

Każdy raport powinien zawierać co najmniej:

- opis zakresu i metodyki testów,
- podsumowanie zarządcze (Executive Summary),
- szczegółowy opis wykrytych podatności,
- klasyfikację ryzyka (np. krytyczne / wysokie / średnie / niskie),
- scenariusze potencjalnych ataków,
- dowody techniczne (np. zrzuty ekranu, logi, payloady),
- rekomendacje naprawcze (techniczne i organizacyjne),
- wskazanie podatności zgodnie z CVE / OWASP,
- ocenę ogólnego poziomu bezpieczeństwa.

Raporty muszą być dostarczone w języku **polskim**, w formie elektronicznej (PDF).

4. Testy ponowne (retest)

Zamówienie obejmuje możliwość przeprowadzenia jednorazowego retestu wykrytych podatności po ich usunięciu, w terminie uzgodnionym z Zamawiającym, bez dodatkowych kosztów.

5. Wymagania wobec Wykonawcy

Wykonawca musi:

- posiadać doświadczenie w realizacji pentestów dla podmiotów publicznych publicznych,
- dysponować zespołem specjalistów ds. bezpieczeństwa IT,
- zapewnić poufność przetwarzanych informacji,
- podpisać umowę NDA,
- realizować testy w sposób niezakłócający pracy systemów produkcyjnych**.**

6. Terminy realizacji

- Rozpoczęcie realizacji: do 14 dni od podpisania umowy,
- Czas realizacji pentestów: maksymalnie 14 dni roboczych**,**
- Dostarczenie raportów: do 7 dni od zakończenia testów.

7. Warunki dodatkowe

- Testy muszą być prowadzone wyłącznie w uzgodnionych godzinach,
- Zakres testów oraz adresy IP zostaną przekazane Wykonawcy przed rozpoczęciem realizacji,
- Wszelkie wykryte incydenty krytyczne muszą być niezwłocznie zgłaszane Zamawiającemu.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa