*Załącznik nr 1 do Zapytania Ofertowego*

**OPIS PRZEDMIOTU ZAMÓWIENIA**

w postępowaniu o udzielenie zamówienia publicznego w trybie Zapytania Ofertowego, pod nazwą:

**Przeprowadzenie audytu bezpieczeństwa** **i testów penetracyjnych**

realizowanego w ramach projektu

**Cyberbezpieczny Samorząd Gmina Rabka Zdrój**

**Zamawiający**: Gmina Rabka Zdrój, ul. Parkowa 2, 34-700 Rabka Zdrój

Projekt finansowany ze środków Funduszy Europejskich na Rozwój Cyfrowy (FERC) 2021-2027 Priorytet II „Zaawansowane usługi cyfrowe” Działanie 2.2 „Wzmocnienie krajowego systemu cyberbezpieczeństwa”

1. **Wymagania dotyczące Audytu bezpieczeństwa i Testów penetracyjnych**
2. Audyt bezpieczeństwa musi być zgodny z wymaganiami Ustawy z dnia 5 lipca 2018 roku o Krajowym Systemie Cyberbezpieczeństwa, Rozporządzeniem Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych oraz z aktualnymi wymaganiami normy PN ISO IEC 27001 lub równoważnej.
3. W ramach wykonywania testów penetracyjnych aplikacji wymagane jest wykorzystanie obowiązujących standardów bezpieczeństwa udostępnianych przez organizację OWASP (Open Web Application Security Project) lub równoważnych.
4. Testy penetracyjne powinny być wykonane zgodnie ze standardami określonymi przez:
5. OWASP Application Security Verification Standard (ASVS) w wersji 4.0.1 lub 4.0.2 <https://owasp.org/www-project-application-security-verification-standard/>
6. OWASP Web Security Testing Guide (WSTG) w wersji 4.2 <https://owasp.org/www-project-web-security-testing-guide/v42/>
7. Penetration Testing Execution Standard (PTES)
8. Proces testowania musi zapewnić, że każdorazowe badanie z uwzględnieniem metodyki zawartej w normach branżowych, będzie składało się z następujących, wyróżnionych etapów:
9. przeprowadzenie badań i testów;
10. opracowanie oceny eksperckiej;
11. przedstawienie wiążącego stanowiska;
12. przedstawienie rekomendacji zmian.
13. Zakres audytu bezpieczeństwa i testów penetracyjnych
14. Audyt konfiguracji systemów operacyjnych, obejmujący sprawdzenie:
15. uruchomionych usług sieciowych,
16. kont systemowych,
17. mechanizmów uwierzytelniania i autoryzacji,
18. wdrożonych mechanizmów dostępu do zasobów,
19. uprawnień do zasobów,
20. wdrożonych mechanizmów instalacji aktualizacji,
21. wdrożonych mechanizmów tworzenia kopii zapasowych,
22. wdrożonych mechanizmów logowania zdarzeń,
23. wdrożonych mechanizmów administracji zdalnej,
24. wdrożonych mechanizmów zabezpieczenia systemu w fazie boot,
25. wdrożonych mechanizmów zarządzania systemem,
26. wdrożonych dodatkowych metod ochrony,
27. Audyt konfiguracji baz danych, obejmujący:
28. sprawdzenie wdrożenia podstawowych zasad hardeningowych bazy (np.: dostępność domyślnych użytkowników guest, partycjonowanie bazy, składowanie logów, logowanie nietypowych zdarzeń, dostępność wybranych niebezpiecznych procedur /funkcji składowanych);
29. sprawdzenie komunikacji z klientem bazodanowym - wykorzystanie mechanizmów kryptograficznych (logowanie się klienta oraz transfer danych);
30. ogólną recenzję architektury bazy (wykorzystane mechanizmy autoryzacji oraz uwierzytelniania segmentacja uprawnień, wykorzystanie widoków; wykorzystanie procedur składowanych);
31. weryfikację sposobu wykonywania kopii zapasowych oraz ich odtwarzania;
32. analizę sposobu udostępnienia zarządzania bazą danych na poziomie sieciowym.
33. Audyt bezpieczeństwa aplikacji, obejmujący
34. sprawdzenie architektury sieciowej i serwerowej; pod kątem bezpieczeństwa;
35. sprawdzenie procedur zarządzania serwerami;
36. sprawdzenie podatności komponentów aplikacji (w tym serwerów aplikacyjnych i baz danych);
37. weryfikację sposobu instalacji aplikacji i procedur stosowanych przy wdrażaniu nowych aplikacji;
38. weryfikację mechanizmów uwierzytelniania / autoryzacji;
39. Przeprowadzenie testów szczegółowych:

* sprawdzenie zabezpieczeń panelu administracyjnego przed nieupoważnionym dostępem,
* próba uzyskania dostępu do panelu administracyjnego za pomocą kont zwykłych użytkowników min. przez: wykorzystanie bieżącej sesji, podniesienie uprawnień,
* próba uzyskania większych uprawnień,
* próba uzyskania nieautoryzowanego dostępu do danych znajdujących się w systemie,
* próba uzyskania nieautoryzowanego dostępu do plików znajdujących się na serwerze,
* analiza możliwości enumeracji użytkowników,
* próba ataków typowych dla aplikacji webowych i web services, m.in.: SQL Injection, Cross Site Scripting, IMAP/SMTP Injection, LDAP Injection, ORM Injection, XML Injection, XPath Injection, Code Injection, Command Injection, HTTP Splitting,
* funkcja przekierowujących pod kątem walidacji wprowadzanych danych,
* analiza polityki haseł w aplikacji,
* próba ominięcia mechanizmu uwierzytelniania za pomocą min. analizy identyfikatorów sesji, manipulacji parametrami, bezpośredniego dostępu do widoku aplikacji,
* próba ominięcia mechanizmu autoryzacji min. przez uzyskanie bezpośredniego dostępu do zasobów, manipulacje parametrami, uzyskanie wyższych uprawnień,
* analiza wykorzystywanego przez aplikację szyfrowania przesyłanych danych, pod kątem dostępnych/wykorzystywanych algorytmów,
* analiza mechanizmu logowania pod kątem możliwości ominięcia uwierzytelniania i możliwości podsłuchu przesyłanych danych,
* analiza mechanizmu zakończenia sesji użytkownika pod kątem skuteczności i możliwości przeprowadzenia ataku Denial of Service,
* analiza zabezpieczenia plików Cookie,
* analiza zabezpieczenia serwera przed niebezpiecznymi metodami http,
* analiza przesyłanego kodu pod kątem zawartości zbędnych informacji o aplikacji,
* analiza nagłówków http pod kątem bezpieczeństwa,
* analiza błędów aplikacji pod kątem ujawniania informacji,
* analiza możliwości zapamiętywania przez przeglądarkę informacji klientów,
* próba odnalezienia wcześniejszych wersji kodu źródłowego i plików kopii zapasowych na serwerze.

1. Audyt bezpieczeństwa infrastruktury, obejmujący:
2. audyt architektury bezpieczeństwa infrastruktury IT;
3. audyt konfiguracji urządzeń sieciowych
4. testy penetracyjne zewnętrzne:

* identyfikacje dostępnych serwisów sieciowych, określenie oraz weryfikacja ich podatności;
* penetracja systemu za pomocą skanerów TCP i UDP;
* bezpieczeństwo aplikacji oraz usług dostępnych z zewnątrz;
* analiza topologii sieci widzianej z zewnątrz;
* możliwość uzyskania nieautoryzowanego dostępu do danych;
* badanie podatności związanych atakami typu DDoS;
* konfiguracja komunikacji z usługami (np. konfiguracja SSL/TSL, IPsec);
* weryfikacja procedur zarządzania siecią WAN.

1. testy penetracyjne wewnętrzne:

* bezpieczeństwo urządzeń sieciowych;
* bezpieczeństwo protokołów trasowania;
* analiza topologii sieci i logiki jej segmentacji;
* bezpieczeństwo maszyn zlokalizowanych w obrębie sieci (serwery, stacje robocze);
* bezpieczeństwo usług zlokalizowanych na każdym z dostępnych w sieci urządzeniu oraz maszynie, Istnienie nieautoryzowanych urządzeń (np. nieautoryzowanego urządzenia bezprzewodowego wpiętego do sieci);
* filtrowanie komunikacji wewnętrznej (np. konfiguracja firewall, IDS/IPS, WAF, separacja pomiędzy kluczowymi podsieciami);
* konfiguracja komunikacji z zasobami (np. konfiguracja SSL/TLS dla kluczowych aplikacji);
* możliwość uzyskania nieautoryzowanego dostępu do danych (np. danych wrażliwych);
* przegląd danych dostępnych na udziałach sieciowych – weryfikujemy, czy możliwe jest uzyskanie nieautoryzowanego dostępu do danych na udziałach sieciowych takich jak hasła do systemów, czy też kluczowych dla działania organizacji danych;
* podatność na ataki DDoS;
* weryfikacja zasad bezpieczeństwa na wybranych stacjach roboczych;
* weryfikacja dostępu do Internetu z LAN;
* weryfikacja procedur zarządzania siecią LAN.

1. Bezpieczeństwo urządzeń sieciowych
2. badanie odporności urządzeń na ataki z poziomu Internetu;
3. wskazanie potencjalnych skutków ataku dla znalezionych luk i określenie ich krytyczności;
4. wskazanie potencjalnych, dodatkowych metod ochrony sieci;
5. analiza podatności na ataki;
6. skanowanie portów TCP / UDP;
7. skanowanie hostów aktywnych w danej podsieci;
8. określenie ścieżki sieciowej do urządzenia;
9. próba detekcji typu oraz wersji usług sieciowych działających w systemie;
10. próba detekcji wersji oraz typu oprogramowania systemowego zainstalowanego na urządzeniu;
11. próba komunikacji w obrębie protokołu ICMP;
12. próba generacji pakietów o dużym rozmiarze (np. powiększonych pakietów ICMP echo).
13. Testy bezpieczeństwa VPN (IPsec)
14. badanie poziomu bezpieczeństwa systemów klasy VPN;
15. weryfikacja możliwości użycia systemów klasy VPN jako punkt pośredniego do ataku na infrastrukturę IT;
16. określenie realnego zabezpieczenia komunikacji sieciowej oferowanej przez wdrożoną u Zamawiającego implementację VPN;
17. próba wykrycia aktywności serwera VPN;
18. próba wykrycia rodzaju wykorzystywanego rozwiązania VPN (dostawcy sprzętu);
19. próba inicjowania tunelu z różnymi algorytmami kryptograficznymi (szyfry symetryczne, funkcje skrótu, metoda uwierzytelniania, grupa DH);
20. skanowanie portów oraz podatności na koncentratorze VPN;
21. weryfikacja wykorzystanych trybów połączenia (transport, tunnel, ESP, AH);
22. weryfikacja przyjętych metod uwierzytelniania (np. PKI, hasła jednorazowe);
23. weryfikacja przyjętych polityk bezpieczeństwa dla urządzeń klienckich korzystających z VPN (pod względem możliwości ataku na infrastrukturę VPN - inicjowanych z urządzeń klienckich);
24. podstawowa analiza architektury sieci – pod względem rozmieszczenia komponentów.
25. Audyt procesów zarządczych IT w zakresie serwerów, sieci, infrastruktury, baz danych, aplikacji, obejmujący:
26. podział ról i odpowiedzialności za zarządzanie w badanym obszarze
27. analiza architektury w badanym obszarze
28. procesy zarządzania zmianą
29. procesy obsługi incydentów
30. procesy wdrażania nowych rozwiązań
31. procesy wycofywania
32. procesy utrzymania
33. Audyt na zgodność z krajowymi ramami interoperacyjności, obejmujący:
34. Wymiana informacji w postaci elektronicznej, w tym współpraca z innymi systemami/rejestrami informatycznymi i wspomaganie świadczenia usług drogą elektroniczną

* usługi elektroniczne
* centralne repozytorium wzorów dokumentów elektronicznych
* model usługowy
* współpraca systemów teleinformatycznych z innymi systemami
* obieg dokumentów w urzędzie
* formaty danych udostępniane przez systemy teleinformatyczne

1. system zarządzania bezpieczeństwem informacji w systemach teleinformatycznych

* dokumenty z zakresu bezpieczeństwa informacji, zaangażowanie kierownictwa podmiotu
* analiza zagrożeń związanych z przetwarzaniem informacji
* inwentaryzacja sprzętu i oprogramowania informatycznego
* zarządzanie uprawnieniami do pracy w systemach informatycznych
* szkolenia pracowników zaangażowanych w proces przetwarzania informacji
* praca na odległość i mobilne przetwarzanie danych
* serwis sprzętu informatycznego i oprogramowania
* procedury zgłaszania incydentów naruszenia BI
* audyt wewnętrzny z zakresu bezpieczeństwa informacji
* kopie zapasowe
* projektowanie, wdrażanie i eksploatacja systemów teleinformatycznych
* zabezpieczenia techniczno-organizacyjne dostępu do informacji
* zabezpieczenia techniczno-organizacyjne systemów informatycznych
* rozliczalność działań w systemach teleinformatycznych

1. zapewnienie dostępności informacji zawartych na stronach internetowych urzędów dla osób niepełnosprawnych
2. **Raporty**
3. Wynikiem przeprowadzonych audytów i testów będzie raport poaudytowy zawierający:
4. przedmiot, cel i zakres audytu;
5. datę rozpoczęcia audytu;
6. opis przyjętej metodyki;
7. raport dla kierownictwa obejmujące syntezę wyników audytu i ocenę poziomu spełnienia wymogów KRI / UoKSC regulacji wewnętrznych dot. bezpieczeństwa informacji Zamawiającego oraz ocenę bezpieczeństwa systemu informatycznego w tym podsumowanie zidentyfikowanych słabości / nieprawidłowości, a także główne rekomendacje dotyczące poprawy bezpieczeństwa informacji, danych i systemu informatycznego;
8. raport szczegółowy zawierający dokładny opis zidentyfikowanych nieprawidłowości w szczególności:
9. wskazujący dokładne miejsca, w których występują realne bądź potencjalne problemy z bezpieczeństwem informacji;
10. zawierający wyniki audytów, w tym testów i ich interpretację - każde ustalenie musi odnosić się do konkretnych przypadków słabości/nieprawidłowości popartych zgromadzonymi dowodami audytowymi, które będą stanowiły załącznik do raportu;
11. opisy błędów, informacje jakich narzędzi użyto do odnalezienia błędu, opis warunków, które są konieczne, aby doszło do błędu;
12. plik proof of concept, pozwalający na reprodukcję błędu;
13. zawierający rekomendacje w zakresie eliminacji zidentyfikowanych słabości/nieprawidłowości oraz poprawy poziomu bezpieczeństwa, w tym wskazanie działań korygujących i/lub doskonalących;

Ocena, ustalenia i rekomendacje muszą być ze sobą jasno powiązane i łatwo identyfikowalne.

1. propozycje zmian w treści regulacji wewnętrznych dot. bezpieczeństwa informacji, w tym danych osobowych (dokumentacja SZBI) Zamawiającego wraz z proponowaną treścią nowych (zmienionych lub dodanych) zapisów;
2. datę sporządzenia raportu;
3. imiona i nazwiska audytorów realizujących zadanie oraz ich podpisy.
4. Raport musi zawierać podział podatności ze względu na ryzyko, wpływ wykrytej podatności na poufność, integralność i dostępność informacji (poziom krytyczności), prawdopodobieństwo wykorzystania podatności, złożoność (trudność) wprowadzenia naprawy – usunięcia podatności.
5. Raport z audytu musi być podpisany przez audytora dokonującego audyt systemu bezpieczeństwa informacji wdrożonego w urzędzie JST.
6. Raport w formie edytowalnej i pdf, przesyłany drogą elektroniczną musi być zaszyfrowany przy użyciu algorytmu szyfrującego AES-256 oraz zabezpieczony co najmniej 9-znakowym hasłem jednorazowym (zawierającym małe i duże litery, cyfry i znaki specjalne) przesłanym przez Wykonawcę alternatywny kanał komunikacji w terminie do 14 dni od daty zakończenia audytu w siedzibie Zamawiającego.