zał. numer 2 do zapytania

OPIS PRZEDMIOTU ZAMÓWIENIA

Wymagania dla usługi przeprowadzenia audytów łączonych SZBI oraz KRI & UoKSC (audyt początkowy oraz audyt końcowy) dla UG Piątnica oraz jednostek podległych: Centrum Usług Samorządowych, Ośrodka Pomocy Społecznej w Piątnicy, 7 placówek edukacyjnych (Zespół Szkolno-Przedszkolny w Piątnicy, Szkoła Podstawowa w Kisielnicy, Dobrzyjałowie, Drozdowie, Olszynach, Rakowo-Boginie i Jeziorku)

Zamawiający wymaga, aby audyty zostały przeprowadzone w zgodzie z Krajowymi Ramami Interoperacyjności (KRI) z uwzględnieniem elementów ustawy o Krajowym Systemie Cyberbezpieczeństwa (KSC) w kontekście Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).

Zamawiający wymaga, aby na zespole audytorskim spoczywał obowiązek weryfikacji zgodności z innymi przepisami, w tym:

- zgodność z przepisami dotyczącymi ochrony danych osobowych (np. RODO), w kontekście zarządzania danymi, bezpieczeństwa informacji oraz cyberbezpieczeństwa.
- sprawdzenie zgodności z krajowymi i międzynarodowymi normami oraz standardami związanymi z bezpieczeństwem informacji i cyberbezpieczeństwem.

AUDYT POCZĄTKOWY łączony SZBI oraz KRI & UoKSC stanowi kluczowy element w ramach projektu Cyberbezpieczny Samorząd, a jego celem jest dokonanie wstępnej oceny obecnego stanu bezpieczeństwa informacji u Zamawiającego, w tym identyfikacja wszelkich zagrożeń, słabości, luk w zabezpieczeniach itd. Na podstawie wyników audytu należy zweryfikować braki i obszary wymagające poprawy, co kluczowe jest dla skutecznego wdrożenia działań w ramach projektu. Audyt początkowy niezbędny jest dla Zamawiającego do oceny zgodności z normami i standardami dotyczącymi zarządzania bezpieczeństwem informacji, a jego wyniki stanowią fundament do opracowania dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji.

AUDYT KOŃCOWY łączony SZBI & UoKSC ma wykazać efektywność wdrożonych działań i weryfikację czy zidentyfikowane w audycie początkowym słabości i luki zostały skutecznie zlikwidowane, a także czy nowo wdrożone procedury i mechanizmy działają zgodnie z ich założeniami.
Zamawiający wymaga, aby audyt końcowy stanowił formalną ocenę funkcjonowania Systemu Zarządzania Bezpieczeństwem Informacji i weryfikację jego poprawności, funkcjonowania zgodnie z wymaganiami norm, przepisów prawnych oraz wewnętrznych polityk. Audyt końcowy jest także dla Zamawiającego niezbędny do zapewnienia, że Jednostka jest przygotowana do dalszego funkcjonowania zgodnie z wymogami cyberbezpieczeństwa, a ponadto jego uzasadnienie znajduje się w konieczności formalnego zamknięcia Projektu i jego ocenę.

Zamawiający wymaga, aby w ramach czynności audytowych Wykonawca przeprowadził kompleksowe testy penetracyjne (dwukrotnie, wraz z czynnościami audytowymi) infrastruktury IT Jednostek. Testy penetracyjne mają na celu identyfikację i ocenę nieznanych dotąd podatności. Testy te muszą być wykonane przez wykwalifikowanego pentestera i powinny obejmować szczegółową analizę zarówno zewnętrznych, jak i wewnętrznych komponentów systemu informatycznego.

Zamawiający wymaga, aby zakres testów penetracyjnych obejmował m.in.:

1. **Zewnętrzne testy penetracyjne infrastruktury IT:**
   - analiza topologii sieci na granicy z Internetem - szczegółowe zbadanie struktury sieci na styku z Internetem, z uwzględnieniem istniejących zabezpieczeń;
   - ocena mechanizmów ochronnych - sprawdzenie efektywności systemów zabezpieczeń, takich jak zapory sieciowe, IDS/IPS oraz inne urządzenia na granicy sieci;
   - wykrywanie publicznie dostępnych usług sieciowych - przeprowadzenie skanowania portów oraz usług dostępnych publicznie w celu zidentyfikowania potencjalnych punktów dostępu dla atakujących;
   - identyfikacja wersji i typów publicznie dostępnego oprogramowania - ustalenie wersji oprogramowania, które jest widoczne z sieci publicznej, w celu określenia możliwych luk w zabezpieczeniach;
   - próby wykorzystania wykrytych podatności - testowanie ryzyka poprzez wykorzystanie zidentyfikowanych luk bezpieczeństwa;
   - zalecenia dotyczące wzmocnienia ochrony sieci brzegowej - przygotowanie zaleceń dotyczących wzmocnienia ochrony na granicy sieci lokalnej z Internetem.

2. **Wewnętrzne testy penetracyjne infrastruktury IT:**
   - ocena struktury sieci LAN**: Szczegółowa analiza wewnętrznej topologii sieci LAN, w tym rozmieszczenia urządzeń oraz zastosowanych mechanizmów ochrony;
   - testowanie wewnętrznych zabezpieczeń sieciowych - sprawdzenie izolacji urządzeń, segmentacji sieci oraz innych środków ochronnych stosowanych w sieci wewnętrznej;
   - analiza i monitoring ruchu sieciowego - przeprowadzenie dokładnego monitoringu ruchu sieciowego w poszukiwaniu nietypowych wzorców mogących świadczyć o naruszeniu bezpieczeństwa;
   - skanowanie portów i usług w sieci LAN - identyfikacja usług i aplikacji działających w sieci wewnętrznej poprzez skanowanie portów TCP/UDP;
   - wykrywanie aktywnych urządzeń w sieci - identyfikacja i analiza urządzeń podłączonych do sieci lokalnej w celu oceny potencjalnych zagrożeń;
   - eksploatacja zidentyfikowanych podatności w sieci LAN - przeprowadzenie prób wykorzystania słabości w sieci wewnętrznej w celu oceny ryzyka;
   - ocena procedur tworzenia i odzyskiwania kopii zapasowych - przegląd skuteczności procedur backupu i przywracania danych;
   - rekomendacje dla poprawy bezpieczeństwa wewnętrznej sieci LAN - przygotowanie szczegółowych zaleceń dotyczących zwiększenia poziomu zabezpieczeń sieci lokalnej.

3. **Audyt bezpieczeństwa serwisów WWW:**
   - sprawdzenie aktualności serwera HTTP oraz systemu CMS - ocena zgodności wersji oprogramowania serwerowego oraz systemu CMS z najnowszymi standardami bezpieczeństwa, z naciskiem na wykrywanie znanych luk;

- ocena bezpieczeństwa komunikacji internetowej - analiza stosowanych certyfikatów X.509, wersji protokołu TLS oraz metod kryptograficznych, zapewniających poufność i integralność transmisji danych przez Internet.

4. **Audyt bezpieczeństwa serwisów pocztowych:**
   - analiza mechanizmów SPF, DKIM i DMARC - ocena poprawności implementacji mechanizmów SPF, DKIM oraz DMARC, mających na celu ochronę przed fałszerstwami wiadomości e-mail;
   - ocena zabezpieczeń TLS w komunikacji e-mailowej - sprawdzenie czy mechanizmy szyfrowania TLS zostały poprawnie wdrożone w celu zabezpieczenia komunikacji pocztowej.

5. **Raport z przeprowadzonych testów i audytów:**

- dokumentacja wykonanych prac - szczegółowy raport zawierający opis zastosowanej metodologii, użytych narzędzi oraz zakresu wykonanych testów i analiz;
- analiza wyników testów penetracyjnych - przedstawienie wyników testów, wraz z identyfikacją wykrytych podatności i oceną związanego z nimi ryzyka;
- zalecenia i wnioski - opracowanie rekomendacji dotyczących naprawy wykrytych problemów oraz strategii mających na celu podniesienie poziomu bezpieczeństwa;
- szczegółowa analiza technicznych zabezpieczeń - ocena oraz omówienie stanu zabezpieczeń serwisów WWW, serwisów pocztowych, sieci LAN i połączeń z Internetem, wraz z zaleceniami dotyczącymi utrzymania wysokiego poziomu bezpieczeństwa.

Opracowanie raportu z audytu wskazującego wykryte podatności oraz błędy wraz rekomendacjami działań naprawczych i korygujących oraz uzupełnienie załącznika nr 6 do Regulaminu Konkursu Grantowego pn. „Cyberbezpieczny Samorząd" – ankieta dojrzałości cyberbezpieczeństwa w jednostkach samorządu terytorialnego.

Z kolei wsparcie poaudytowe, które polegać ma m.in. na: udzielanie informacji na temat audytowanych elementów wynikających z raportu. Czas dla klienta na zapoznanie się z raportem i zadawanie pytań odnośnie raportu min. 6 miesięcy od przeprowadzenia audytu i przedstawieniu raportu.

Niniejszy opis przedstawia minimalny zakres wymagań dla przeprowadzenia kompleksowych testów penetracyjnych oraz audytów bezpieczeństwa IT, które mają na celu wszechstronną ocenę stanu bezpieczeństwa informatycznego Jednostek Zamawiającego.

WÓJT
mgr Krzysztof Ryszard Kozicki

Projekt pn. „Cyberbezpieczna Gmina Piątnica" jest finansowany z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd" o numerze FERC.02.02-CS.01-001/23