Załącznik nr 1 do Zapytania ofertowego

BA-WZ.25.13.2020.KR

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

I. PRZEDMIOTU ZAMÓWIENIA:

Przedmiotem zamówienia jest analiza środowiska infrastruktury informatycznej Centrum Unijnych Projektów Transportowych – audyt wybranych obszarów środowiska teleinformatycznego.

II. WYMAGANIA WSTĘPNE PRZED REALIZACJĄ AUDYTU:

Wykonawca przed przystąpieniem do realizacji audytu jest zobowiązany do podpisania klauzuli poufności i jest zobligowany do zachowania w tajemnicy wszelkich informacji pozyskanych w sposób bezpośredni lub pośredni dotyczących Zamawiającego, a w szczególności danych osobowych, technicznych, ekonomicznych lub organizacyjnych. Zobowiązanie do zachowania poufności dotyczy wszelkich informacji udzielonych ustnie, pisemnie, drogą elektroniczną lub w inny sposób w odpowiedzi na zapytania Wykonawcy w trakcie realizacji zadań audytywnych i jest bezterminowe. Dostęp do środowiska informatycznego zamawiającego będzie realizowany wyłączenie z komputerów Zamawiającego.

III. MIEJSCE I OBSZAR PRAC AUDYTOWYCH

1. Lokalizacja realizowanych prac:

1.1 Analiza będzie przeprowadzana w siedzibie zamawiającego tj. plac Europejski 2 Warszawa w Budynku C Warsaw Spire.

1.2 Audyt dotyczy infrastruktury dwóch serwerowni (głównej i zapasowej) oraz czterech sieciowych punktów dystrybucyjnych znajdujących się w odrębnych pomieszczeniach.

2. Orientacyjna skala audytowanego środowiska:

2.1 Audytem zostanie objętych ok. 10 systemów Zamawiającego wykorzystywanych przez ok. 350 pracowników.

2.2 Systemy objęte audytem to m.in. :

a) Active Directory,
b) Exchange,
c) Sharepoint,
d) System wydruku (Safeq)
e) PKI
f) MDM (Workspace One-VMware)
g) OwnCloud
h) System Backupu

IV. SZCZEGÓŁOWY ZAKRES AUDYTU

Audyt wybranych obszarów środowiska teleinformatycznego musi zostać zrealizowany w oparciu o aktualne wymagania Krajowych Ram Interoperacyjności (Dz.U.2017.2247 j.t.) oraz norm ISO 27001, 27002, 27005 w następującym zakresie i obszarach:

1. Zdefiniowanie aktywów infrastruktury teleinformatycznej składających się na serwerownię podstawową oraz zapasową oraz czterech sieciowych punktów dystrybucyjnych znajdujących się w odrębnych pomieszczeniach.
2. Określenie ryzyk związanych z dalszym funkcjonowaniem powyższych aktywów w kontekście integralności, poufności i dostępności przetwarzanych informacji oraz zachowania ciągłości działania obejmującego audyt w zakresie:

   1.1 Weryfikacji stanu dokumentacji (zakres oraz aktualność) w odniesieniu do wymogów norm. Weryfikacji podlegać będą m.in.: zakres merytoryczny dokumentów i ich aktualność w tym określenie zakresu koniecznych zmian związanych z wymogami norm. W ramach zadnia przeanalizowane mają być, m.in.: aktualnie stosowane polityki, procedury i inne dokumenty związane z bezpieczeństwem (np. Polityka Bezpieczeństwa Informacji, Plany Zachowania Ciągłości Działania w obszarze IT itp.).

   1.2 Weryfikacji treści umów serwisowych oraz gwarancji dostawców badanej infrastruktury.

   1.3 Zestawienia zastanej architektury z wymaganiami norm i aktualnymi trendami rynkowymi oraz najlepszymi praktykami w poszczególnych obszarach (transmisja danych, zasoby serwerowe, wirtualizacja, zasoby dyskowe, backupy wraz z zarządzaniem kopiami itd.)

   1.4 Zidentyfikowania potencjalnych podatności ze szczególnym uwzględnieniem urządzeń i systemów wykorzystywanych przez pracowników organizacji do pracy zdalnej (notebooki, telefony komórkowe, aplikacje) – na podstawie aktualnych konfiguracji urządzeń i ich rodzajów (bez testów penetracyjnych).

   1.5 Analiza urządzeń i wykorzystywanej infrastruktury sieciowej oraz urządzeń typu Firewall w zakresie stosowanych zabezpieczeń przed nieautoryzowanym dostępem do infrastruktury i danych Zamawiającego – na podstawie aktualnych konfiguracji urządzeń i ich rodzajów (bez testów penetracyjnych).

V. OPRACOWANIE RAPORTU KOŃCOWEGO

Wykonawca zobowiązany będzie do przedstawienia szczegółowego raportu z wykonanych prac. Raport zawierać musi informacje o przebiegu badania, znalezionych błędach oraz zalecenia po audytowe. Raport obejmować musi przynajmniej informacje wymienione poniżej:

1. Przygotowanie planów/rekomendacji postępowania z rozpoznanymi ryzykami z powyższych obszarów, mającymi na celu ich redukcję bądź transfer.
2. Poziom istotności znalezionych nieprawidłowości (błędów) według zaproponowanej przez Wykonawcą i uzgodnionej z Zamawiającym klasyfikacji,
3. Wpływ na bezpieczeństwo systemu (lub inne systemy) –tzw. impact
4. Rekomendacje dalszych działań i koniecznych zmian odnoszących się do zapewnienia zgodności z wymaganiami norm, KRI i najlepszymi praktykami w poszczególnych obszarach (transmisja danych, zasoby serwerowe, wirtualizacja, zasoby dyskowe, backupy wraz z zarządzaniem kopiami itd.).
5. Rekomendacje w zakresie modernizacji i rozbudowy infrastruktury IT do poziomu spełniającego wymagania bezpieczeństwa wynikające z aktualnych przepisów prawa, dobrych

praktyk branżowych i norm (wytyczne do modernizacji: sieci teleinformatycznej, sprzętu komputerowego, serwerów, zarządzania i oprogramowania użytkowego) oraz wskaże obszary zmian dotyczące stosowanej lub brakującej dokumentacji (procedury, instrukcje), organizacji Zamawiającego i innych elementów, które mają lub mogą mieć wpływ na poziom bezpieczeństwa.

6. Struktura raportu powinna odpowiadać merytorycznemu podziałowi prac na obszary podlegające audytowi np. (systemy, urządzenia sieciowe, dokumentacja).
   Wykonawca przeprowadzi prezentację wyników audytu oraz przeprowadzi minimum dwudniowe (16 godzin zegarowych) spotkanie prezentujące wyniki prac z pracownikami Zamawiającego pozwalające na zapoznanie z wykrytymi ryzykami oraz na uzyskanie rekomendacji i wiedzy w zakresie ich unikania.
7. Dokumentacja wytworzona przez Wykonawcę w ramach realizacji przedmiotu Umowy będzie miała postać Raportu spełniającego następujące wymagania;
   7.1 w zakresie jakości:
   - 7.1.1 Czytelna i zrozumiała struktura poszczególnych dokumentów z podziałem na rozdziały, podrozdziały i sekcje.
   - 7.1.2 Spójna struktura, forma i sposób prezentacji poszczególnych dokumentów.
   - 7.1.3 Kompletność dokumentu rozumiana jako pełne przedstawienie omawianego problemu, a w szczególności jednoznaczne i wyczerpujące przedstawienie wszystkich zagadnień w odniesieniu do poszczególnych usług IT.
   - 7.1.4 Spójność dokumentu rozumiana jako zapewnienie wzajemnej zgodności pomiędzy wszystkimi rodzajami informacji umieszczonymi w dokumencie oraz brak logicznych sprzeczności pomiędzy informacjami zawartymi we wszystkich przekazanych dokumentach oraz we fragmentach tego samego dokumentu.

   7.2 w zakresie zawartości;
   - 7.2.1 Streszczenie dla Kierownictwa.
   - 7.2.2 Opis przedmiotu prac i metodyki realizacji.
   - 7.2.3 Wykaz zidentyfikowanych podsystemów teleinformatycznych.
   - 7.2.4 Wykaz zidentyfikowanych podatności infrastruktury teleinformatycznej:
     a. opis podatności (ze szczególnym uwzględnieniem urządzeń i systemów wykorzystywanych przez pracowników organizacji do pracy zdalnej),
     b. zagrożenia, z którymi wiąże się podatność,
     c. poziom ryzyka (wysokie, średnie, niskie),
     d. zalecane działania korygujące,
     e. ewentualne uboczne skutki wdrożenia działań korygujących.
   - 7.2.5 Wykaz pozostałych niedoskonałości infrastruktury teleinformatycznej:
     a. opis niedoskonałości,
     b. zalecane działania korygujące,
     c. ewentualne uboczne skutki wdrożenia działań korygujących.

8. Przeniesienia na Zamawiającego autorskich praw majątkowych do raportu na polach eksploatacji, wskazanych w §6 IPU.