Załącznik nr 1 do Zapytania ofertowego

OPIS PRZEDMIOTU ZAMÓWIENIA

(OPZ)

Wykonanie usługi ekspertyzy

w zakresie koncepcji wdrożenia, rozwoju, optymalizacji i efektywności wykorzystania systemów bezpieczeństwa teleinformatycznego w BFG

Sierpień 2021 r.

I. Nazwa zamówienia.

Wykonanie usługi ekspertyzy w zakresie koncepcji wdrożenia, rozwoju, optymalizacji i efektywności wykorzystania systemów bezpieczeństwa teleinformatycznego w BFG.

II. Termin realizacji zamówienia.

Przedmiot zamówienia zostanie zrealizowany w terminie nie dłuższym niż 35 dni roboczych licząc od dnia zawarcia umowy z Wykonawcą.

III. Miejsce wykonania usługi.

1. Czynności analityczne wymagane do uzyskania niezbędnej wiedzy do realizacji przedmiotu Umowy przeprowadzone zostaną w siedzibie Zamawiającego, mieszczącej się przy ul ks. Ignacego Jana Skorupki 4 w Warszawie.
2. Czynności, o których mowa w ust. 1 będą prowadzone w godzinach pracy Zamawiającego (8-16), w ustalonym terminie.
3. Zamawiający dopuszcza kontakt zdalny za pośrednictwem narzędzi Zamawiającego do prowadzenia telekonferencji lub wideokonferencji wyłącznie w kwestiach organizacyjnych związanych z realizacją przedmiotu zamówienia.

IV. Określenie przedmiotu oraz zakresu zamówienia.

1. Przedmiotem zamówienia jest wykonanie usługi polegającej na dokonaniu analizy stanu poszczególnych obszarów bezpieczeństwa IT Zamawiającego oraz opracowaniu wytycznych i rekomendacji dla rozwiązań mających na celu podniesienie poziomu bezpieczeństwa IT Zamawiającego i rekomendacji wdrożenia rozwiązań zwiększających bezpieczeństwo, a w szczególności na:
    1) Wykonaniu analizy środowiska teleinformatycznego Zamawiającego w kontekście efektywności, optymalizacji wykorzystania systemów bezpieczeństwa IT wynikającej z oszacowanego ryzyka oraz oceny stosowanych środków technicznych. Analiza ma uwzględniać wymagane regulacje prawne z zakresu ochrony informacji i rekomendacje stosowane w obszarze sektora bankowo-finansowego.
    2) Przedstawieniu Zamawiającemu możliwości (wariantów) i kierunków, w których powinny być rozwijane systemy bezpieczeństwa IT, aby osiągnąć skuteczny nadzór i monitorowanie zdarzeń z infrastruktury systemu informatycznego oraz osiągnięcie założonych celów Zamawiającego, o których mowa w pkt VIII.
    3) Opracowaniu rekomendacji zgodnych z najnowszym stanem wiedzy i wymaganymi aktami prawnymi, umożliwiających wdrożenie spójnej i zgodnej z aktualnymi możliwościami technicznymi strategii redukcji ryzyka wynikającego z rozwoju i utrzymania systemów teleinformatycznych Zamawiającego. Dobrane zabezpieczenia muszą być adekwatne względem chronionych zasobów informacyjnych, zagrożeń dla systemu informatycznego i gotowości podjęcia akceptowalnego przez Zamawiającego poziomu ryzyka.
    4) Przedstawieniu rozwiązań systemów bezpieczeństwa IT pozwalających na ograniczenie potencjalnych, negatywnych skutków zdarzeń oraz efektywne wykorzystanie zasobów finansowych, ludzkich i materialnych.
    5) Przygotowaniu i dostarczeniu dokumentu podsumowującego, zawierającego wyniki przeprowadzonych analiz oraz rekomendacje i wytyczne dla Zamawiającego .
    6) Prezentacji wyników z przeprowadzonej analizy oraz rekomendacji i wytycznych na spotkaniu podsumowującym.
2. W ramach przewidzianego wynagrodzenia Wykonawca przeniesie na Zamawiającego autorskie prawa majątkowe do Utworu/Utworów oraz własność nośników, na których został utrwalony Utwór/Utwory.

V. Wymagania formalne w zakresie analizy i rekomendacji.

1. Analiza środowiska teleinformatycznego obejmująca systemy bezpieczeństwa IT oraz przygotowania koncepcji architektury nowych rozwiązań z obszaru bezpieczeństwa IT musi obejmować min.:
   1) opis stanu obecnego (aktualnie stosowane narzędzia w zakresie zarządzania i nadzoru bezpieczeństwa IT);
   2) ocenę kompletności stosowanych mechanizmów bezpieczeństwa;
   3) opracowanie poziomu dojrzałości systemów bezpieczeństwa IT wraz ze zidentyfikowanymi ryzykami i planem dojścia do stanu docelowego;
   4) wskazanie min. 3 możliwych rozwiązań (wariantów proponowanych rozwiązań) i ocenę ich wykonalności wraz z oszacowaniem kosztów;
   5) opracowanie kluczowych wskaźników efektywności dla proponowanego rozwiązania/systemów bezpieczeństwa IT;
   6) wskazanie kolejności wdrażania zaproponowanych zmian;
   7) rekomendacje dalszego rozwoju narzędzi bezpieczeństwa.
2. Wynikiem analizy będzie dokument końcowy nakreślający Zamawiającemu kierunki i możliwości zmian (tzw. „mapa drogowa"), które powinny być brane pod uwagę przy rozwoju platform i systemów podnoszących bezpieczeństwo teleinformatyczne.
3. Dokument musi zawierać rekomendacje odnoszące się do wymogów stawianych w przepisach prawa. Rekomendacje i wytyczne powinny odnosić się do zidentyfikowanych ryzyk technologicznych, procesowych, i biznesowych tak by można je było mitygować lub eliminować poprzez rozwój i rozbudowę systemów informatycznych.
4. Dokument końcowy wraz z rekomendacjami musi być zredagowany w języku polskim, składać się z co najmniej 50 stron formatu A4, pisanych czcionką Calibri Light 11, akapit (interlinia) 1,5 wiersza. Dokument będzie zawierał co najmniej:
   1) opis stanu obecnego – min. 20 stron,
   2) opracowanie poziomu dojrzałości – min. 10 stron,
   3) opis modeli pracy, kluczowych wskaźników efektywności (sposób i częstość pomiaru oraz powiązane z nimi korzyści wynikające z wdrażanego rozwiązania) – min. 10 stron,
   4) wskazania kolejności wdrażania zaproponowanych zmian – min. 10 stron.

VI. Wymagania formalne w zakresie spotkania podsumowującego

1. Po dokonaniu akceptacji dokumentu końcowego przez Zamawiającego, w przeciągu 7 dni roboczych Wykonawca przeprowadzi co najmniej 2 godzinne spotkanie podsumowujące z zakresu zrealizowanych prac.
2. Wykonawca przedstawi wyniki analizy, rekomendacje główne i wytyczne oraz warianty dalszych działań w obszarze bezpieczeństwa IT Zamawiającego, pozwalające na wybór odpowiednich środków zabezpieczających (technicznych i/lub organizacyjnych) przez Zamawiającego.

VII. Plan prac

1. W ramach realizacji zamówienia Wykonawca, w porozumieniu z Zamawiającym zobowiązany jest opracować w terminie 5 dni roboczych od daty podpisania umowy plan prac obejmujący harmonogram.
2. Harmonogram powinien opisywać terminy poszczególnych prac (etapów) oraz sposób ich realizacji.
3. Dla każdej czynności analitycznej i wytwórczej wymagane jest przedstawienie planu (koncepcji) przeprowadzenia tej czynności oraz określenie zakresu niezbędnego wsparcia po stronie Zamawiającego. Plan powinien obejmować w szczególności informacje na temat:
   1) Niezbędnych danych, dokumentów i informacji technicznych;
   2) Szczegółowego harmonogramu realizacji czynności w siedzibie Zamawiającego;
   3) Zakresu wykonywanych czynności i podejmowanych działań.

4. Wykonawca zobowiązany jest do uwzględnienia uwag Zamawiającego co do zakresu planu lub harmonogramu oraz formy jego realizacji.

VIII. Założone cele Zamawiającego.

Minimalne oczekiwania Zamawiającego:

1. Centralne przechowywanie i archiwizowanie zdarzeń całego systemu informatycznego.
2. Ocena i podniesienie istniejącego poziomu bezpieczeństwa IT.
3. Monitorowanie zdarzeń z infrastruktury systemu informatycznego.
4. Zapewnienie skutecznych narzędzi do monitorowania i zarządzania bezpieczeństwem IT.
5. Szybsza/efektywna analiza incydentów i reakcja na zagrożenia.
6. Raportowanie i prezentacja danych w zakresie incydentów bezpieczeństwa IT.
7. Wykrywanie zaawansowanych ataków w czasie rzeczywistym mimo ewolucji ich metod i technik.
8. Odtworzenie działań atakującego (rekonstrukcja incydentu bezpieczeństwa IT).
9. Zebranie materiału dowodowego incydentu (między innymi rekonstrukcja zdarzenia z warstwy sieciowej).
10. Utrzymanie poziomu bezpieczeństwa IT w czasie.
11. Mitygacja wykrytych, złośliwych działań na stacjach końcowych.
12. Wykorzystanie zewnętrznych źródeł danych o zagrożeniach (Threat Intelligence) do wsparcia działań obronnych.
13. Wsparcie w poszukiwaniu zagrożeń w systemie informatycznym (Thread Hunting).
14. Wsparcie sztucznej inteligencji w procesie nadzoru bezpieczeństwa IT i monitorowania zachowań użytkowników i urządzeń sieciowych.
15. Pomiar bezpieczeństwa teleinformatycznego poprzez określenie skuteczności poszczególnych zabezpieczeń, dzięki możliwości zbadania zmian poziomu bezpieczeństwa wywołanych wprowadzeniem lub usunięciem zabezpieczenia.
16. Szacowanie kosztów, jakie należy ponieść, aby zwiększyć poziom bezpieczeństwa systemu o określoną wartość.