Załącznik nr 1 do Zapytania ofertowego – Opis przedmiotu zamówienia

Szczegółowy Opis Przedmiotu Zamówienia

I. Opis przedmiotu zamówienia

1. Przedmiotem zamówienia jest ***przeprowadzenia audytu bezpieczeństwa informacji i bezpieczeństwa teleinformatycznego***, mającego na celu ocenę poziomu bezpieczeństwa u Zamawiającego (audyt). Audyt powinien objąć wszelkie niezbędne działania w celu określenia stopnia zgodności z przepisami prawa i zaleceniami norm PN-ISO/IEC 27001.
2. Wynikiem przeprowadzenia audytu będzie opracowany przez Wykonawcę raport, zawierający ocenę stanu bezpieczeństwa organizacji. Raport będzie oparty na wynikach przeprowadzonego audytu i wskazywał elementy zgodne z normą i te wymagające poprawy. Raport będzie zawierał rekomendacje odnośnie koniecznych działań zarówno doraźnych jak i długoterminowych.
3. Całość przedmiotu zamówienia będzie zrealizowana w terminie **maksymalnie do 4 tygodni od dnia podpisania Umowy**.

II. Wymagania:

1. Audyt musi zostać przeprowadzony przez **co najmniej dwóch audytorów** posiadających doświadczenie poparte przeprowadzeniem **co najmniej 8 audytów bezpieczeństwa** w okresie ostatnich dwóch lat.

2. Zespół audytowy musi posiadać doświadczenie w zakresie przeprowadzania audytów bezpieczeństwa **w przynajmniej trzech różnych profilach organizacji** (np. służba zdrowia, produkcja, jednostka samorządowa).

3. Audyt bezpieczeństwa musi zostać przeprowadzony na zgodność z wymaganiami **normy ISO PN-EN 27001**.

4. Wykonawca przeprowadzi badanie podatności infrastruktury teleinformatycznej Zamawiającego, to jest skanowanie podatności. Skanowanie podatności należy przeprowadzić za pomocą narzędzia informatycznego umożliwiającego sprawdzenie oprogramowania w oparciu o wcześniej zdefiniowane przez Wykonawcę słowniki i sygnatury zgodnie z ustaleniami z Zamawiającym. Skanowanie powinno dostarczyć informacje o występujących podatnościach ocenianych zgodnie ze skalą CVSS 3.0 lub CVSS 3.1.

5. Wykonawca wykona zlecone skanowanie podatności na określonej części infrastruktury systemu. Harmonogram wykonania skanowania podatności musi zostać wcześniej zaakceptowany przez Zamawiającego.

6. Wykonawca przeprowadzi badanie zgodności systemów teleinformatycznych zainstalowanych na: serwerach (Windows, Linux), urządzeniach Firewall, Switch oraz baz danych zgodnie z najlepszymi standardami (np. CIS Benchmark, STIG, itp.)

7. Audyt musi być przeprowadzony zgodnie z Planem Audytu (zawierającym harmonogram prac), przygotowanym przez Wykonawcę. Wykonawca do 14 dni po podpisaniu umowy przedstawi

Plan Audytu Zamawiającemu celem akceptacji. Zamawiający ma 7 dni od przedstawienia Planu Audytu na jego akceptację lub wniesienie uwag.

8. Plan Audytu musi zawierać następujące elementy:

   - Czynności wykonywane podczas prac audytowych wraz z terminami ich realizacji;
   - Przybliżony termin zakończenia prac audytowych.

9. Audyt powinien w zakresie technicznym obejmować następujące elementy:

   - techniczne zabezpieczenia stacji roboczych i serwerów;
   - techniczne zabezpieczenia infrastruktury sieciowej;
   - audyt mechanizmów logowania;
   - techniczne zabezpieczenia poczty elektronicznej;
   - audyt odporności systemów teleinformatycznych pod kątem cyberzagrożeń.

10. Podczas audytu należy poddać ocenie bezpieczeństwo fizyczne obiektów: Trylogii 2/16, 01-982 Warszawa.

11. Podczas audytu należy zbadać bezpieczeństwo sieci bezprzewodowej. Informacje o metodyce badania oraz ocenie i rekomendacjach bezpieczeństwa muszą zostać uwzględnione w raporcie z audytu.

12. Raport przedstawiony przez Wykonawcę z wyników skanowania i identyfikacji podatności musi zawierać informacje o zaistniałych anomaliach w pracy systemu, które zostały odnotowane podczas skanowania podatności i ich krytyczności w odniesieniu do prowadzonej działalności operacyjnej (usługi kluczowej). Wykonawca dokona priorytetyzacji i klasyfikacji zebranych podatności oraz opracuje sposoby zmniejszenia ryzyka.

III. Wymagania dotyczące raportu:

1. Raport musi zawierać odniesienia do wymagań wynikających z Normy ISO PN-EN 27001.

2. Raport musi uwzględniać opisany stan faktyczny podczas sesji audytowych oraz ocenę i rekomendacje audytowe.

3. Wykonawca zobowiązany jest uwzględnić wszystkie informacje na temat przeprowadzonego audytu technicznego w raporcie z uwzględnieniem zidentyfikowanych podatności oraz proponowane działania naprawcze.