załącznik A

Szczegółowy opis przedmiotu zamówienia

dla zadania

Przeprowadzenie audytu bezpieczeństwa informacji

Przedmiotem zamówienia jest wykonanie usługi polegającej na przeprowadzeniu w Urzędzie Miasta Mikołów audytu dotyczącego oceny bezpieczeństwa informacji w oparciu o przepisy Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych w Urzędzie Miasta Mikołów.

Zadanie będzie realizowany etapami:

ETAP I Zarządzanie Bezpieczeństwem Informacji – termin realizacji do 3 tygodni od dnia podpisania umowy

ETAP II Kontrola legalności oprogramowania, sieci LAN i środowiska sprzętowo – systemowego – termin realizacji do 10 tygodni od dnia podpisania umowy

ETAP I Zarządzanie Bezpieczeństwem Informacji.
Wymagania w stosunku do usługi Zarządzania Bezpieczeństwem Informacji

Zamawiający oczekuje od Wykonawcy:

a) przeglądu dokumentacji dotyczącej Bezpieczeństwa Informacji
b) przeprowadzenia analizy ryzyka
c) rozpoznanie obszarów przetwarzania danych w Urzędzie;
d) rozpoznanie zbiorów danych przetwarzanych w Urzędzie;
e) rozpoznanie systemów przetwarzających dane i ich konfiguracji;
f) przeprowadzenie analizy ochrony punktów krytycznych w obszarach przetwarzania danych w Urzędzie;
g) przeprowadzenie analizy wytycznych w zakresie dostępu osób upoważnionych do przetwarzania danych osobowych;
h) przeprowadzenie analizy możliwości dostępu do danych przez osoby nieupoważnione;
i) przeprowadzenie analizy kompletności wymaganej dokumentacji zgodnie z wytycznymi GIODO;
j) weryfikacja pracy użytkowników w obszarach, w których przetwarzane są dane osobowe;
k) weryfikacja sposobu przetwarzania danych osobowych;
l) weryfikacja kontroli nad przepływem danych osobowych;
m) identyfikacja zagrożeń, słabych stron i oszacowanie ryzyka przetwarzania danych osobowych;
n) weryfikacja dostępu osób nieupoważnionych do miejsc gdzie przetwarzane są dane osobowe;

ETAP II Kontrola legalności oprogramowania, sieci LAN i środowiska sprzętowo - systemowego

A. **Wymagania w stosunku do usługi kontroli legalności oprogramowania oraz przestrzegania praw autorskich.**

Zamawiający oczekuje od Wykonawcy:

1. dokonania skanowania jednostek komputerowych celem zweryfikowania oprogramowania.
2. wykonania przeglądu posiadanych licencji na podstawie atrybutów legalności (książki, licencje oraz nośniki).
3. uzyskanie potwierdzenia działania zgodnego z prawem;
4. uzyskanie listy programów bez odpowiedniej licencji;
5. kontrola rodzaju przechowywanych danych przez pracowników na stanowiskach komputerowych;
6. optymalizacja kosztów ponoszonych na zakup oprogramowania;

B. **Wymagania w stosunku do usługi kontroli sieci LAN i środowiska sprzętowo – systemowego.**

Zamawiający oczekuje od Wykonawcy:

1. przeprowadzenie audytu sieci Klienta dostępnej z Internetu
2. przeprowadzenie audytu sieci Klienta dostępnej z sieci lokalnej:
    a. analiza konfiguracji serwerów pod kątem bezpieczeństwa, a w szczególności:
        i. weryfikację aktualności wykorzystywanego oprogramowania serwera aplikacyjnego;
        ii. analizę i ocenę sposobu obsługi błędów;
        iii. analizę i ocenę mechanizmów logowania zdarzeń;
        iv. analizę i ocenę wykorzystywanych metod kontroli dostępu fizycznego i logicznego;
        v. weryfikację obecności domyślnych kont użytkowników;
        vi. weryfikację dostępności domyślnych/testowych aplikacji.
        vii. weryfikację sposobu zarządzania serwerem;
        viii. analizę i ocenę mechanizmów archiwizacji danych.
    b. analiza konfiguracji serwera bazy danych, będzie obejmowała co najmniej:
        i. weryfikację aktualności wersji oprogramowania bazy danych;
        ii. analizę zastosowanych metod uwierzytelniania;
        iii. weryfikację obecności domyślnych kont użytkowników;
        iv. weryfikację przyjętej polityki haseł;
        v. weryfikację zastosowanych mechanizmów kryptograficznych, w tym sposobu przechowywania haseł;
        vi. weryfikację mechanizmów logowania zdarzeń;
        vii. analizę i ocenę mechanizmów archiwizacji danych;
        viii. analizę i ocenę mechanizmów kontroli dostępu fizycznego i logicznego.
    c. analiza bezpieczeństwa danych firmowych przed nieuprawnioną ingerencją pracownika bądź ich fizyczną utratę
    d. analiza procedur wewnętrznych firmy, polityka bezpieczeństwa, prawa dostępu pracowników jak i systemów zapobiegających utracie danych
    e. analiza przepływu informacji i jej słabych węzłów

Informacje ogólne:

Całość obejmuje min 4 serwery, 130 stanowisk roboczych, 170 pracowników, lokalizacje:

a) UM Mikołów Rynek 16
b) UM Mikołów Rynek 20
c) UM Mikołów ul, Miarki 15
d) UM Mikołów ul. Miarki 16
e) UM Mikołów ul Kolejowa 2
f) UM Mikołów ul Kolejowa 4

Elementem kończącym etap jest:

A. sporządzenie raportu pokontrolnego dotyczącego aktualnego stanu bezpieczeństwa danych osobowych i zaleceń dotyczących bezpieczeństwa zgodnych z:
    a. Ustawą z dnia 29 sierpnia 1997 roku o Ochronie Danych Osobowych (tj. Dz.U. 2002 r. Nr 101, poz. 926 z późn. zm).;
    b. Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 100, poz. 1024);
    c. Wytycznymi w zakresie opracowania i wdrożenia polityki bezpieczeństwa opublikowanymi przez Głównego Inspektora Ochrony Danych Osobowych;
B. Opracowanie raportu z zakresu przeprowadzonych audytów dla każdego z etapów, który musi zawierać wyniki wykonanego audytu oraz opisywać sposób wdrożenia wymagań norm w poszczególnych obszarach bezpieczeństwa (poszczególnych punktach normy), oraz opisywać stosowne zabezpieczenia. Raport będzie zawierał:
    1. propozycje skutecznej naprawy wykrytych luk w bezpieczeństwie sieci.
    2. ocenę ryzyka i procedur bezpieczeństwa sieci,
    3. listę wykrytych zagrożeń i wykaz znalezionych błędów wraz z ich opisem,
    4. przygotowania programu naprawczego
    5. przygotowania Procedury Zarządzania Oprogramowaniem.