Zapytanie o cenę

W celu przeprowadzenia rozeznania rynku uprzejmie zapraszam Państwa do przesłania wyceny, zgodnie z podanymi poniżej wymaganiami.

Przedmiotem zamówienia jest przeprowadzenie wewnętrznego audytu zgodności Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w Centrum Projektów Europejskich z wymaganiami aktualnej normy PN-ISO/IEC 27001.

Mając na względzie powyższe uregulowania prawne, CPE jako podmiot realizujące zadania publiczne, jest zobowiązany do przeprowadzenia następujących działań w zakresie zrządzania bezpieczeństwem informacji, poprzez:

1) zapewnienie aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia;

2) utrzymywanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację;

3) przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy;

4) podejmowanie działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji;

5) zapewnienie bezzwłocznej zmiany uprawnień,

6) zapewnienie szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak:

   a) zagrożenia bezpieczeństwa informacji,

   b) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna,

   c) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich;

7) zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez:

   a) monitorowanie dostępu do informacji,

   b) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,

   c) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji;

8) ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość;

9) zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie;

10) zawierania w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji;

11) ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych;

12) zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na:

a) dbałości o aktualizację oprogramowania,

b) minimalizowaniu ryzyka utraty informacji w wyniku awarii,

c) ochronie przed błędami, utratą, nieuprawnioną modyfikacją,

d) stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa,

e) zapewnieniu bezpieczeństwa plików systemowych,

f) redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,

g) niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,

i) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa;

j) bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących;

k) zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.

Jednocześnie jak wynika z dokumentu pt.: *„Wspólne stanowisko Departamentu Informacji MAiC i Departamentu Audytu Sektora finansów Publicznych MF odnośnie zapewnienia audytu wewnętrznego w zakresie bezpieczeństwa informacji”*(w załączniku), przedmiot realizujący zadania publiczne może zrealizować obowiązek wynikający z przywołanego na wstępie przepisu min. Poprzez przeprowadzenie audytu zgodności z normą PN-ISO/IEC 27001.

Ponadto ten sam dokument pozostawia kierownictwu jednostki decyzję o wyborze wykonawcy przedmiotowego audytu.

Wymagania dotyczące zamówienia:

- Weryfikacja zgodności zabezpieczeń organizacji z wymaganiami aktualnej normy PN-ISO/IEC 27001.
- Weryfikacja zgodności SZBI z Rozporządzeniem z dnia 12 kwietnia 2012 roku Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

- Wykrycie niezgodności pomiędzy stanem faktycznym, a wymaganiami normy w poszczególnych obszarach SZBI oraz przedstawienie odpowiadających im rekomendacji i propozycji sposobu usunięcia niezgodności.
- Zamawiający przekaże Wykonawcy raport z poprzedniego roku po podpisaniu umowy.
- Porównanie raportu z roku poprzedniego wykonanego przez firmę zewnętrzną na podstawie którego zostanie przedstawiony raport porównawczy z rokiem bieżącym.
- Znajomość metodyki audytu w zakresie bezpieczeństwa informacji.
- Dysponowanie osobą/osobami posiadającą/ymi certyfikat audytora wiodącego ISO 27001 – tyko wybrany oferent dołącza kopie certyfikatów do Umowy.
- Czas wykonania usługi ; 45 dni od podpisania umowy.
- Wykonawca przekaże pierwszą wersję pełnego raportu z audytu maksymalnie do 30 dnia od podpisania umowy, po czym zamawiający ma maksymalnie 8 dni na zgłoszenie uwag do przekazanego pierwszego raportu.
- Uwagi do raportu będą zgłaszane droga elektroniczną przez osoby upoważnione w umowie.
- Wykonawca ma maksymalnie 7 dni na weryfikację uwag i przedstawienie raportu końcowego.
- Kara umowna 1% wartości umowy za każdy dzień opóźnienia wykonania usługi.

Audytem będą objęte następujące lokalizacje:

- Warszawa – ul. Domaniewska 39A – dalej CPE
- Warszawa – ul. Żurawia 3/5 (Centralny Punkt Informacyjny Funduszy Europejskich)
- Kraków – ul. Halicka 9 (Wspólny Sekretariat Techniczny Program Współpracy Transgranicznej Rzeczpospolita Polska – Republika Słowacka) – dalej WST PL-SK
- Gdańsk – al. Grunwaldzka 186 (Wspólny Sekretariat Techniczny Program Współpracy Transgranicznej Południowy Bałtyk) – dalej Southbaltic
- Wrocław ul. Świętego Mikołaja 81 (Wspólny Sekretariat Polska – Saksonia) – dalej WS PLSN
- Olsztyn ul. Głowackiego 14 (Wspólny Sekretariat Techniczny Polska-Rosja) – dalej PL-RU

Wszelkie koszty związane z zakwaterowaniem, wyżywieniem, przejazdem itp. pokrywa Wykonawca zamówienia.

Dane do przygotowania wyceny:

Zatrudnienie:
Ogółem jest zatrudnionych ok. 111 osób

W tym w placówkach:

- CPE – ok. 60 osób (Warszawa)
- CPI (Warszawa), WST PL-SK (Kraków), Southbaltic (Gdańsk), WS PL-SN (Wrocław), WST PLRU (Olsztyn)– w placówkach jest zatrudnione między 3 - 15 osób w każdej.

Struktura sieci teleinformatycznej
Każde stanowisko pracy jest wyposażone w komputer oraz telefon.
CPE posiada serwery własne jak również serwery hostowane u dostawców zewnętrznych. Pozostałe informacje ze względów bezpieczeństwa zostaną przekazane tylko i wyłącznie Wykonawcy zamówienia, po podpisaniu Umowy.

Zakres Audytu

I. Audyt SZBI na zgodność z aktualną normą PN-ISO/IEC 27001
1. Audyt bezpieczeństwa informacji we wszystkich obszarach funkcjonowania podmiotu

1.1. Formalno-prawnym
1.2. Fizycznym i środowiskowym
1.3. Teleinformatycznym

2. Zebranie obowiązującej w organizacji dokumentacji SZBI, w tym między innymi
   2.1. Polityka bezpieczeństwa informacji
   2.2. Instrukcja zarządzania systemami informatycznymi
   2.3. Zasady zarządzaniem ryzykiem
   2.4. Instrukcja sporządzania Informacji Zarządczej
   2.5. Regulaminy organizacyjne, kadrowe, działania organizacji
   2.6. Plany ciągłości działania

Powyższa lista ma charakter poglądowy, w związku z czym mogą być potrzebne dodatkowe dokumenty związane z wymogami Krajowych Ram Interoperacyjności.

3. Analiza zebranych dokumentów
4. Przeprowadzenie wywiadów z wybranymi pracownikami

II. Testy penetracyjne (wewnętrzne i zewnętrzne) infrastruktury informatycznej wg PTES-Penetration Testing Execution Standard

1. Typ Testu
   1.1. GreyBox
2. Analiza podatności
   2.1. Testowanie
   2.2. Aktywne
   2.3. Pasywne
3. Walidacja wyników
   3.1. Porównywanie wyników z różnych narzędzi
   3.2. Ręczne ponawianie testów
   3.3. Kreowanie ścieżek ataku
4. Badania
   4.1. Publiczne - poszukiwanie informacji o podatnościach w dostępnych źródłach
   4.2. Prywatne - laby testowe, analiza podatności
5. Faza Exploitacyjna
   5.1. Unikanie wykrycia
   5.2. Dostosowywanie ścieżki exploitacji
   5.3. Unikanie mechanizmów obronnych
   5.4. Exploitacja
6. Faza Post Exploitacyjna
   6.1. Analiza infrastruktury
   6.2. Profilowanie celów o wysokim znaczeniu
   6.3. Próby dostępu do danych
   6.4. Dalsza penetracja infrastruktury

III. Wykonanie i przekazanie Raportów z Audytu z omówieniem.

Propozycje ofertowe z całkowitym kosztem wykonania usługi należy przesyłać wyłącznie pocztą elektroniczną do dnia 4 kwietnia 2017 r. do godz. 17:00 na adres: ofertynw@cpe.gov.pl