Zadanie nr 2

Załącznik nr 2.1 do SWZ

Załącznik Nr 1 do umowy

II MODUŁ: IDENTYFIKACJA I ANALIZA DANYCH TELEINFORMATYCZNYCH W SYTUACJI KRYZYSOWEJ

PKT. 2 Szkolenie specjalistyczne doskonalące umiejętność analizy ruchu sieciowego

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

CZĘŚĆ A. INFORMACJE O PRZEDMIOCIE ZAMÓWIENIA

1. Opis przedmiotu zamówienia

Przedmiotem zamówienia jest świadczenie specjalistycznych usług szkoleniowych podnoszących umiejętności zzakresu zaawansowanych technik informatyki śledczej bazujących na zabezpieczaniu i analizie dowodów elektronicznych związanych z ruchem sieciowym (NetworkForensics). Szkolenia organizowane będą w ramach projektu „Skuteczni w działaniu – współpraca służb w sytuacjach zagrożenia infrastruktury krytycznej" współfinansowanego z Funduszu Bezpieczeństwa Wewnętrznego, realizowanego przez Komendę Wojewódzką Policji z siedzibą w Radomiu w formie wykładów, ćwiczeń praktycznych oraz laboratoryjnych przewidzianych dla 50 osób – specjalistów i praktyków z zakresu informatyki śledczej.

2. Cel szkolenia

Celem realizowanych szkoleń jestpodniesienie kompetencji specjalistów do walki z Cyberprzestępczością oraz praktyków informatyki śledczej w obszarzeanalizy i zabezpieczaniu dowodów związanych z ruchem sieciowym, a także w zapobieganiu i wykrywaniu incydentów sieciowych.Wykorzystanie w praktyce umiejętności nabytych na szkoleniach powinno zwiększyć skuteczność przeprowadzania analiz po włamaniowych na elementy infrastruktury sieciowej. Ponadto powinno przyczynić się do wypracowania schematów postepowania oraz dobrych praktyk organów ścigania podejmujących czynności w związku z atakami na aplikacje webowe i systemy sieciowe. Wynikiem przeprowadzonych szkoleń powinno być nabycie przez ich uczestnikówpraktycznej wiedzy i specjalistycznych umiejętności obejmujących charakterystykę ruchu sieciowego,podstawy funkcjonowania sieci oraz praktyczne aspekty wykorzystania analizy sieciowej oraz możliwości i techniki zabezpieczania dowodów pozyskanych w trakcie analizy. Ponadto uczestnicy szkoleń powinni nabyć umiejętności wykrywania zagrożeń na podstawie monitorowania ruchu sieciowego, wykrywania niezgodnego z polityką bezpieczeństwa wykorzystania dostępu do sieci, wykorzystywania narzędzi pozwalających na wyciągnięcie danych bezpośrednio z ruchu sieciowego.Pozyskane w wyniku szkoleń nowe zdolności oraz podniesione w ten sposób kompetencje powinny pozytywnie wpłynąć na prowadzone czynności w ramach procesu wykrywczego i tym samym zwiększyć skuteczność

ochrony obiektów infrastruktury krytycznej w obszarze wykorzystywanych przez nie sieci komputerowych, zarówno na etapie prewencji, jak też działań reaktywnych w sytuacji rzeczywistego zagrożenia.

3. Odbiorcy szkolenia

Odbiorcami – uczestnikami szkoleń będących przedmiotem zamówienia będą specjaliści oraz praktycy wykonujący podstawowe i wstępne analizy ruchu sieciowegooraz dokonujący zabezpieczeń dowodów i śladów dotyczących incydentów teleinformatycznych związanych z ruchem sieciowym z Wydziałów dw. z Cyberprzestępczością i Laboratorium Kryminalistycznego z Komend Wojewódzkich Policji. Uczestnikami szkolenia będzie łącznie pięćdziesiąt osób podzielonych na pięć dziesięcioosobowych grup szkoleniowych.

4. Termin realizacji szkolenia

Z uwagi na podział odbiorców docelowych na 5 grup szkoleniowych, realizacja usługi szkolenia powinna zostać przeprowadzona w 5 terminach uwzględniających 5 dni roboczych trwania zajęć szkoleniowych w systemie od poniedziałku do piątku. Każdy dzień szkoleniowy powinien się składać
z 8 godzin szkoleniowych (z wliczeniem czasu przerw kawowych i obiadowych), co odpowiada łącznie 40 godzinom szkoleniowym, z czego min. 16 godzin muszą stanowić zajęcia praktyczne. Wykonawca zobowiązuje się do wykonania szkolenia w przeciągu sześciu miesięcyod daty podpisania umowy.Szkolenie odbędzie się w pięciu terminach, osobno dla każdej grupy.Dokładne terminy przeprowadzenia szkoleń dla poszczególnych grup szkoleniowych będą uzgodnione w trybie ustaleń roboczych z wyłonionym Wykonawcą.

5. Miejsce realizacji szkolenia

Usługa szkoleniowa powinna być przeprowadzona w formie stacjonarnej, na poziomie eksperckim w postaci zajęć teoretycznych – wykładów oraz praktycznych ćwiczeń laboratoryjnych w siedzibie zapewnionej przez Wykonawcę na terenie Polski. Zamawiający wymaga, aby szkolenie zostało przeprowadzone w sali wyposażonej w klimatyzację, bezprzewodowy oraz przewodowy Internet, a także indywidualne stanowisko komputerowe dla każdego uczestnika umożliwiające przeprowadzenie zajęć praktycznych z wykorzystaniem oprogramowania informatyki śledczej.

CZĘŚĆ B. WYMAGANIA

1. Zakres merytoryczny szkolenia

Wykonawca zobowiązany jest zapewnić realizację zajęć teoretycznych z niżej wymienionych zagadnień:

- Informatyka śledcza w obszarze sieci

  - Sieciowe dowody cyfrowe
  - Aspekty pozyskiwania i zabezpieczania dowodów
  - Metodyka i technika śledcza
  - Aspekty prawne pracy śledczego
- Podstawy funkcjonowania sieci
  - Modele sieciowe (OSI/ISO , TCP/IP)
  - Protokoły sieciowe
  - Protokoły routingu
  - Adresacja sieciowa
  - Elementy sprzętowe
  - Badanie urządzeń sieciowych
  - Omówienie działania aplikacji webowych i ich architektury
- Przechwytywanie ruchu sieciowego
  - Oprogramowanie i narzędzia do przechwytywania ruchu
  - Fizyczne przechwytywanie ruchu
  - Przechwytywanie pakietów TCP, UDP, FTP, http, HTTPS, SMB
  - System SNORT
  - Ekstrakcja danych „live”
- Bezprzewodowe punkty dostępowe
  - Konfiguracja punktów dostępowych
  - Przechwytywanie i analiza ruchu bezprzewodowego
  - Ataki na sieci bezprzewodowe
- Analiza danych sieciowych
  - Analiza danych „na żywo”
  - Obróbka oraz filtrowanie informacji w plikach pcap
  - Ekstrakcja plików z pakietów
  - Analiza pakietów protokołów TCP, UDP, FTP, http, HTTPS, SMB, USB
  - Gromadzenie, weryfikacja i prezentacja dowodów
  - Web proxy, SSL i szyfrowanie
  - Analiza powłamaniowa
- Złośliwe oprogramowanie
  - Metody wprowadzania malware
  - Podstawowa analiza malware
  - Analiza incydentu

Wykonawca zobowiązany jest zapewnić realizację zajęć praktycznych (w formie ćwiczeń bądź laboratoriów) z niżej wymienionych zagadnień:

- Konfiguracja urządzeń sieciowych pod kątem monitorowania i analizy ruchu sieciowego
- Analiza ataku na infrastrukturę sieciową
- Analiza ruchu sieciowego „na żywo”
- Analiza powłamaniowa
- Pozyskiwanie dowodów w ruchu sieciowym
- Analiza przechwyconych pakietów na przykładzie wybranych narzędzi i protokołów

- Identyfikacja oraz analiza wykradzionych danych

2. Zamawiający wymaga, aby Wykonawca zapewnił w ramach usługi:

a) Zakwaterowanie uczestników szkolenia o poniższych wymaganiach:
   - Wykonawca zakwateruje uczestników szkolenia w hotelu posiadającym kategorię min. 3 gwiazdkową znajdującym się w obrębie miasta, w którym będzie realizowane szkolenie.
   - Zakwaterowanie w pokojach 1, 2 – osobowych. Pokoje dwuosobowe muszą być wyposażone w oddzielne łóżka. Wykonawca zobowiązany jest do udostępnienia pokoi dla uczestników szkolenia minimum 1 godzinę przed rozpoczęciem szkolenia.
   - w każdym pokoju musi być węzeł sanitarny (umywalka i prysznic/wanna z ciepłą i zimną wodą, toaleta), ręcznik oraz ręcznik kąpielowy, mydło, papier toaletowy;
   - Wykonawca zapewnia bezpłatny dostęp do sieci wi-fi na terenie obiektu;
   - na terenie obiektu zostaną bezpłatnie udostępnione miejsca parkingowe na 10 samochodów osobowych.

b) Wyżywienie uczestników szkolenia o poniższych wymaganiach:
   - Pełne wyżywienie uczestników szkolenia. Wyklucza się catering. Wyżywienie musi obejmować obiad i kolację (dzień 1), śniadanie, obiad i kolację (dzień 2-4), śniadanie i obiad (dzień 5).

c) Salę wykładową do przeprowadzenie zajęć teoretycznych i praktycznych. W każdym dniu szkolenia (podczas przerw) zostanie zorganizowany serwis kawowy, w trakcie których zostanie podana: kawa, herbata, woda mineralna (gazowana i niegazowana), soki, cukier, mleczko, ciastka kruche lub ciasta. Serwis kawowy musi być zorganizowany w tym samym budynku, co szkolenia (najlepiej w tej samej sali lub jej sąsiedztwie).

d) Imienne certyfikaty w wersji papierowej, zgodnie z obowiązującymi przepisami dotyczącymi danych osobowych, na podstawie uzyskanych bezpośrednio od uczestników szkolenia danych osobowych, poświadczające uczestnictwo w szkoleniu, zawierające m.in. następujące dane: temat szkolenia, czas realizacji szkolenia, miejsce szkolenia, podpisane przez organizatora szkolenia i prowadzącego zajęcia, rozdane uczestnikom najpóźniej ostatniego dnia świadczenia usługi. Certyfikaty o których mowa powyżej, muszą zawierać oznaczenia wskazujące na finansowanie ze środków FBW w ramach Projektu (Zamawiający przekaże Wykonawcy niezbędne pliki graficzne)

e) Sprzęt, oprogramowanie i narzędzia, a także materiały dydaktyczne niezbędne do realizacji programu szkolenia (m.in. stanowisko komputerowe - badawcze dla każdego uczestnika szkolenia, środki piśmiennicze, nagłośnienie, rzutnik multimedialny).

f) Udostępnienie i przekazanie uczestnikom szkolenia materiałów dydaktycznych, w formie cyfrowej, zawierających w szczególności opis oraz informacje na temat wybranych zagadnień przekazywanych i omawianych na szkoleniu (np. skrypt, opisy ćwiczeń).

3. Warunki udziału w postępowaniu

W celu zapewnienia odpowiedniego poziomu merytorycznego oraz efektywności przeprowadzonych zajęć, Zamawiający wymaga, by:

a) Trenerbądź trenerzy przeprowadzający szkolenie muszą posiadaćudokumentowane doświadczenie w przeprowadzaniu szkoleń z obszaru Informatyki śledczej dot. sieci komputerowych (Cyber/Digital/NetworkForensics) na poziomie eksperckim bądź podobnych merytorycznie minimum 5 szkoleń w ostatnich 3latach potwierdzone certyfikatami, listami referencyjnymi, dyplomami bądź innymi równoważnymi dokumentami(wymóg obligatoryjny uprawniający do składania oferty).

4. **Zatrudnienie na podstawie stosunku pracy**
   Wykonawca lub Podwykonawca zobowiązuje się do nawiązania stosunku pracy, w rozumieniu art. 22 § 1 ustawy z dnia 26.06.1974 r. – Kodeks pracy, przy wykonywaniu czynności polegających na sporządzaniu dokumentacji dot. niniejszego szkolenia (listy obecności, ankiety ewaluacyjne, zaświadczenia, certyfikaty itp.).

5. **Wnioskodawca udostępni w ramach projektu sprzęt szkoleniowy, który będzie wykorzystywany podczas szkoleń:**
   a) Nośniki danych – 12szt. (Dyski SATA, M.2)
   b) Serwer plików NAS USB 3.0 (USB – C) 1,6 GHz i 2 GB DDR3
   c) Switch 24 porty Ethernet 10/100/1000Mbps PoE+ ,340W, 4 porty Gigabit SFP/RJ-45 Combo

CZĘŚĆ C. WARUNKI WYBORU OFERTY/WYKONAWCY

Kryteria oceny ofert z podaniem ich procentowego znaczenia:

a. wartość oferty brutto - 60 %
b. doświadczenie trenera- 40 %.

Przy dokonywaniu oceny Komisja Przetargowa posłuży się następującymi wzorami

a) dla kryterium cena:

$$C = \frac{C_N}{C_O} \times 60 \text{ pkt}$$

gdzie:

C - przyznane punkty w kryterium cena,

CN - najniższa wartość ofertowa (brutto) spośród wszystkich ofert podlegających ocenie,

CO - wartość oferty ocenianej (brutto).

b) dla kryterium doświadczenie trenerów w przeprowadzaniu szkoleń w Informatyki śledczej (Cyber/Digital/ ComputerForensics) na poziomie eksperckim

Wykonawca zobowiązany jest wpisać do oferty wszystkich trenerów przeznaczonych do realizacji szkolenia.

Proponowane kryteria wyboru ofert:

- doświadczenie trenera do 3 lat - 0 punktów,
- doświadczenie trenera 4 - 5 lat - 10 punktów
- doświadczenie trenera 6 - 7 lat - 20 punktów,
- doświadczenie trenera 8 -9 lat – 30 punktów,
- doświadczenie trenera 10 i więcej lat - 40 punktów

W przypadku wskazania więcej niż jednego trenera, do wyliczenia punktów za kryterium doświadczenie trenerów prowadzących szkolenie, Zamawiający przyjmie średnią arytmetyczną będącą ilorazem sumy lat doświadczenia trenerów i ilości trenerów. Z powyższych wyliczeń, do oceny Zamawiający przyjmie wartość całkowitą (pełne lata).

Doświadczenie należy podać w pełnych latach. W przypadku podania niepełnych lat Zamawiający przyjmie jedynie pełne lata.

łączna ilość punktów ocenianej oferty (łączna punktacja):

W=C+D

gdzie:

W – łączna punktacja,
C – punkty za wartość oferty brutto,
D – punkty za doświadczenie trenera/trenerów.

Za ofertę najkorzystniejszą uznana zostanie oferta, która uzyska największą liczbę punktów w ocenie końcowej i przedstawia najkorzystniejszy stosunek ceny i doświadczenia trenerów.

Zamawiający zastosuje zaokrąglenie wyników do dwóch miejsc po przecinku

CZĘŚĆ D. POSTANOWIENIA KOŃCOWE

1. Z uwagi na obowiązujący na terenie RP stan epidemii, mając na uwadze ewentualność wprowadzenia obostrzeń w zakresie gromadzenia osób, Zamawiający zastrzega sobie możliwość zmiany terminu usługi w uzgodnieniu z wykonawcą.