Fundusze Europejskie Polska Cyfrowa | Rzeczpospolita Polska | Unia Europejska Europejski Fundusz Rozwoju Regionalnego

pieczątka Zamawiającego

BTI.271.2.86.2022

Świnoujście, dnia 2022-03-21

ZAPYTANIE OFERTOWE

Szkolenie z Cyberbezpieczeństwa – Cyfrowa Gmina

1. Zamawiający: Gmina Miasto Świnoujście (komórka organizacyjna Urzędu Miasta prowadząca postępowanie): Biuro Technologii Informacyjnych

   Dane do kontaktu: Wiktor Szymanowski, email: wszymanowski@um.swinoujscie.pl, tel: 691 441 186,

2. Szczegółowy opis przedmiotu zamówienia w załączeniu:

   Jedno szkolenie z obszarów cyberbezpieczeństwa dla obsady BTI (5 osób), prowadzone on-line, na infrastrukturze UM Świnoujście, w formie warsztatów, w wymiarze 32h (8 dni * 4h dziennie).
   Program obejmujący obszary zabezpieczeń (Fortigate), monitoringu pracy (Zabbix), monitoringu podatności (OpenVAS), integracji usług uwierzytelnienia, pod kątem cyberbezpieczeństwa. Wszystkie zagadnienia w oparciu o istniejącą infrastrukturę sieciowo, sprzętowo -programową Urzędu. Wszystkie omawiane i trenowane zagadnienia muszą występować w kontekście istniejącej domeny Active Directory, oraz cyberbezpieczeństwa. Minimalny zakres zagadnień – w załączniku nr 2.

Dodatkowe wymagania dla organizatora szkolenia:

- prowadzący szkolenie z części pierwszej, musi posiadać certyfikat Fortinet NSE 4 Network Security Professional, lub wyższy,

- wykonawca musi posiadać wiedzę i doświadczenie w zakresie implementacji środowisk sieciowych i systemowych opartych na platformach Microsoft Server, zarządzania tymi środowiskami i rozwiązywania dotyczących ich problemów, przy spełnianiu wymagań dla Microsoft Certified Solutions Associate (MCSA). Wymagany certyfikat MCSA, lub wyższy

- wykonawca musi posiadać wiedzę i doświadczenie w zakresie MITRE ATT&CK Framework, tworzenia i ulepszania polityk IDS/IPS, prowadzącego z certyfikatem co najmniej Certified Ethical Hacker (CEH).

3. Kryteria oceny ofert:
   a) wybór oferty najkorzystniejszej zostanie dokonany na podstawie następujących kryteriów: cena 100%.

4. Data realizacji zamówienia: **do dnia 2022-05-31**.
5. Okres gwarancji (jeżeli dotyczy): -.
6. Forma oferty. Sposób składania oferty:
   a) oferta powinna być sporządzona w języku polskim, na formularzu oferty według wzoru stanowiącego załącznik do Zapytania ofertowego. Oferent musi potwierdzić spełnienie wszystkich kryteriów wyszczególnionych w zapytaniu
   b) oferta powinna być podpisana przez osoby upoważnione do składania oświadczeń woli w imieniu wykonawcy. Pełnomocnictwo do podpisania oferty musi być dołączone do oferty, o ile nie wynika ono z innych dokumentów złożonych przez wykonawcę;

c) ofertę należy złożyć w formie skanu podpisanych dokumentów. Ofertę należy przesłać na adres e-mail: wszymanowski@um.swinoujscie.pl, bti@um.swinoujscie.pl ;
d) termin złożenia oferty: **do dnia 01.04.2022 godz. 10:00**;
e) oferta złożona po terminie zostanie odrzucona.

7. Data oraz miejsce otwarcia/rozpatrzenia ofert: UM Świnoujście, BTI, godz. 10:00 01-04-2022;
8. Warunki płatności: na konto bankowe w terminie do 30 dni od otrzymania prawidłowo wystawionej FV.
9. Faktura może zostać wystawiona po protokolarnym potwierdzeniu przez Zamawiającego należytego wykonania usługi.

KIEROWNIK
Biura Technologii Informacyjnych
mgr inż. Wiktor Szymanowski

.....
podpis i pieczątka
kierownika komórki organizacyjnej

sporządził: Wiktor Szymanowski

Załączniki: 1. Formularz ofertowy;
2. Specyfikacja warunków zamówienia

Fundusze Europejskie Polska Cyfrowa | Rzeczpospolita Polska | Unia Europejska Europejski Fundusz Rozwoju Regionalnego

OFERTA

Nazwa wykonawcy: .....

Adres, tel., e-mail wykonawcy: .....

NIP: ..... Regon: .....

Nr rachunku bankowego: .....

1. W odpowiedzi na zapytanie ofertowe nr BTI.271.2.86.2022 z dnia 2022-03-21 oferuję wykonanie przedmiotu zamówienia za:

   cenę netto .....:.. zł (słownie złotych: .....), powiększoną o podatek VAT ..... zł (słownie złotych: .....), tj. cenę brutto ..... zł (słownie złotych: .....).

2. Pozostałe kryteria oceny ofert (jeżeli dotyczy): .....

3. Oświadczam, że zapoznałem się z opisem przedmiotu zamówienia i nie wnoszę do niego zastrzeżeń oraz wyrażam zgodę na warunki płatności określone w zapytaniu ofertowym.

Zagadnienie	Charakterystyka (wymagania minimalne)	Potwierdzenie spełnienia wymagań
1. Fortigate	Zgodnie z charakterystyką w załączniku nr 2	
2. Monitorowanie sieci – Zabbix		
3. Monitorowanie podatności OpenVAS		
4. Uwierzytelnienie Active Directory		
certyfikat Fortinet NSE 4	Prowadzący posiada certyfikat Fortinet NSE 4 lub wyższy	
certyfikat MCSA	Prowadzący posiada certyfikat MCSA lub wyższy	
Certyfikat CEH	Prowadzący posiada certyfikat Certified Ethical Hacker (CEH) lub wyższy	

   a) Potwierdzam realizację przedmiotu zamówienia do dnia .....;

4. Oświadczam, że wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO[1] wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu (jeżeli dotyczy).

.....
miejscowość, dnia

.....
podpis wykonawcy/osoby upoważnionej

.....
pieczątka wykonawcy

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1).

Załącznik: 2. Specyfikacja warunków zamówienia:

Jedno szkolenie z obszarów cyberbezpieczeństwa dla obsady BTI (5 osób), prowadzone on-line, na infrastrukturze UM Świnoujście, w formie warsztatów, w wymiarze 32h (8 dni * 4h dziennie).

Program obejmujący obszary zabezpieczeń (Fortigate), monitoringu pracy (Zabbix), monitoringu podatności (OpenVAS), integracji usług uwierzytelnienia, pod kątem cyberbezpieczeństwa. Wszystkie zagadnienia w oparciu o istniejącą infrastrukturę sieciowo, sprzętowo -programową Urzędu. Wszystkie omawiane i trenowane zagadnienia muszą występować w kontekście istniejącej domeny Active Directowy, oraz cyberbezpieczeństwa.

Dodatkowe wymagania dla organizatora szkolenia:

- prowadzący szkolenie z części pierwszej, musi posiadać certyfikat Fortinet NSE 4 Network Security Professional, lub wyższy,

- wykonawca musi posiadać wiedzę i doświadczenie w zakresie implementacji środowisk sieciowych i systemowych opartych na platformach Microsoft Server, zarządzania tymi środowiskami i rozwiązywania dotyczących ich problemów, przy spełnianiu wymagań dla Microsoft Certified Solutions Associate (MCSA). Wymagany certyfikat MCSA.

- wykonawca musi posiadać wiedzę i doświadczenie w zakresie MITRE ATT&CK Framework, tworzenia i ulepszania polityk IDS/IPS, prowadzącego z certyfikatem co najmniej Certified Ethical Hacker (CEH).

Zagadnienie	Charakterystyka	Zakres
1. Fortigate	20h - forma zajęć: pokazy wraz z warsztatami. Szkolenie na poziomie przygotowującym do NSE4 – FortiGate Network Security Professional, wraz z elementami NSE7 – Fortinet Troubleshooting Professional, w odniesieniu do używanych FortiGate`ów 200E i 30E: Zagadnienia szczegółowe: • Routing • Software-Defined WAN (SD-WAN) • Przełączanie warstwy 2 • Wirtualne domeny • Fortinet Single Sign-On (FSSO) • High Availability (HA) • Web Proxy • Diagnostyka • Urządzenia FortiGate i Fortinet Security Fabric • Polityki zapory sieciowej • Translacja adresów sieciowych (NAT) • Logowanie i monitoring • Operacje oparte na certyfikatach • Filtr stron www • Kontrola aplikacji • Antywirus • System ochrony przed włamaniami i atakami DoS • SSSL VPN • Dial-Up IPsec VPN • Ochrona przed wyciekiem danych (DLP) oraz elementy:	

	• Zasoby systemowe • Rozwiązywanie problemów sieciowych • Problemy z uwierzytelnianiem użytkowników • FSSO • IPSec • Profile bezpieczeństwa • Explicit Web Proxy • Tryby pracy urządzenia • Zewnętrzne BGP • OSPF	
2. Monitorowanie sieci – Zabbix	8h – forma zajęć: pokazy wraz z warsztatami, w tym zagadnienia szczegółowe: • Serwer Zabbixa, • Zabbix Agent, • Aplikacja web, • Zabbix Proxy, • **Interfejs użytkownika,** • **Profil użytkownika,** • **Wizualizacja danych:** ostatnie dane, grafy, przegląd, monitoring WWW, ostrzeżenia, mapy, ekrany i prezentacje, dashboardy i widgety, inwentarz, usługi, raporty, • **Powiadomienia:** przegląd, eskalacja, monitoring proaktywny, konserwacja,	
3. Monitorowanie podatności OpenVAS	2h – forma zajęć: pokazy wraz z warsztatami, w tym zagadnienia szczegółowe: • Instalacja i skonfiguruj OpenVAS, • Funkcje i składniki OpenVAS, • Konfiguracja i implementacja skanowania zabezpieczeń sieci za pomocą OpenVAS, • Interpretacja wyników skanowania OpenVAS.	
4. Uwierzytelnienie Active Directory – integracja z tworzoną aplikacją Django	2h – forma zajęć: warsztaty, w tym zagadnienia szczegółowe: • Tworzenie wirtualnego serwera z OS Linux, • Budowa podstawowej aplikacji Django, • Integracja uwierzytelnienia z aplikacją Django za pomocą mechanizmów Active Directory,	

KIEROWNIK
Biura Technologii Informacyjnych
mgr inż. Wiktor Szymanowski