Szpital Powiatowy
w Rawiczu Sp. z o.o.

ul. Gen. Grota Roweckiego 6, 63-900 Rawicz
T: +48 65 546 24 13-16 (centrala), T: +48 65 545 21 62 (sekretariat)
F: +48 65 546 70 61, E: sekretariat@szpitalrawicz.pl, www.szpitalrawicz.pl
NIP: 699-19-19-769, REGON: 300904130, KRS: 0000316422
Getin Noble Bank SA Nr konta: 51 1560 0013 2367 2722 7424 0001
Kapitał zakładowy: 34 mln 835 tys. zł w całości opłacony

Rawicz, dnia 02.09.2022r.

NLO-3822-07/ZO/22

ZAPYTANIE OFERTOWE

Dotyczy:
Zapytanie ofertowe – dot. realizacji usługi audytu bezpieczeństwa IT

Szpital Powiatowy w Rawiczu Sp. z o.o. z siedzibą w Rawiczu (kod pocztowy: 63-900) przy ul. Gen. Grota Roweckiego 6 zaprasza do złożenia oferty na **realizację usługi audytu bezpieczeństwa IT.**

1. ZAMAWIAJĄCY:

Szpital Powiatowy w Rawiczu Sp. z o.o.
Ul. Gen. Grota Roweckiego 6
63-900 Rawicz
NIP: 699-19-19-769
tel. 65/ 537 62 24 fax 65/ 546 70 64
email: renata.pazola@szpitalrawicz.pl; marta.czerwinska@szpitalrawicz.pl

www.szpitalrawicz.pl

2. TRYB UDZIELENIA ZAMÓWIENIA:

Zamówienie jest realizowane w trybie zapytania ofertowego.
Zamówienie o wartości mniejszej niż kwoty określone w art. 2 ust. 1 pkt. 1 ustawy z dnia 11 września 2019r. Prawo zamówień publicznych (DZ.U. 2021 poz. 1129)

3. OPIS PRZEDMIOTU ZAMÓWIENIA:

1. Przedmiotem zamówienia jest wykonanie usługi audytu bezpieczeństwa IT. Usługa polega na wykonaniu:
   - Audytu „zerowego";
   - Testów penetracyjnego infrastruktury sieciowej;
   - Audytu końcowego bezpieczeństwa infrastruktury IT wraz z wykonaniem raportu.

2. Zakresem audytu objęta będzie cała działalność świadczeniodawcy. Audyt zerowy, będzie wskazywał obszary doskonalenia bez wpływu na wynik audytu ostatecznego.

Zakres audytu obejmuje:

- Ocena skuteczności działania infrastruktury (urządzenia i konfiguracja w zakresie ochrony poczty; sieci; systemów serwerowych; stacji roboczych; systemów bezpieczeństw);
- Zarządzanie bezpieczeństwem informacji (nośniki wymienne; zarządzanie tożsamością; pomieszczeń w dyspozycji struktur zespołu odpowiedzialnego za cyberbezpieczeństwo);
- Monitorowanie i reagowanie na incydenty bezpieczeństwa (procedura zarządzania incydentami, raportowanie poziomów scenariuszami znanych incydentów; prowadzenie dokumentacji w zakresie incydentów; monitorowanie i wykrycie incydentów bezpieczeństwa; identyfikacja i dokumentów przyczyn wystąpienia incydentów);
- Zarządzanie ciągłością działania (polityka wykonywania kopii bezpieczeństwa; raporty z przeglądów i testów odtwarzania kopii bezpieczeństwa; procedura wykonywania i przechowywania kopii zapasowych; strategia i polityka ciągłości działania, procedury utrzymaniowe);
- Utrzymanie systemów informacyjnych (harmonogramy skanowania podatności, aktualny status realizacji postępowania z podatnościami, procedury związane ze z identyfikowaniem (wykryciem) podatności, współpraca z osobami odpowiedzialnymi za procesy zarządzania incydentami);
- Zarządzanie bezpieczeństwem i ciągłością działania łańcucha usług (polityka bezpieczeństwa w relacjach z dostawcami, standardy i wymagania nakładane na dostawców w umowach w zakresie cyberbezpieczeństwa, dostęp zdalny, metody uwierzytelnienia).

3. Wykonawca zobowiązany jest wykonać dwukrotnie testy penetracyjne infrastruktury sieciowej, tj.: audyt zerowy oraz audyt ostateczny w zakresie określonym w poniższym punktach:
    - **Przedstawienie założeń Audytu** (automatyczny i manualny sposób wykonania audytu);
    - **Weryfikacja dokumentacji sieci, topologii sieci, kluczowych elementów sieci;**
    - **Skanowanie sieci – rekonesans sieci** (Sprawdzenie jakie hosty są w sieci widoczne, ile ich jest, usługi jakie są uruchomione na hostach, jakie systemy operacyjne działają na wykrytych hostach. W szczególności ten etap polega na: skanowaniu sieci w poszukiwaniu wszystkich podłączonych hostów, wykryciu czy jest dostęp do innych podsieci z danej podsieci, wykryciu usług działających na hostach podłączonych do sieci, wykryciu podatności na wybranych hostach w sieci);
    - **Skanowanie będzie powtórzone dla każdej wskazanej przez zamawiającego sieci** (przeprowadzenie skanowania w prawidłowo działającej sieci nie powinno mieć negatywnego wpływu na działanie sieci. Po przeskanowaniu sieci wraz z Zamawiającym zostanie wybrana pula hostów do dalszego badania);

- **Skanowanie najistotniejszych hostów w sieci (serwery kluczowe stacje końcowe, kamery, rejestratory), które zostały wybrane na podstawie wcześniejszej analizy** (weryfikacja występowania luk bezpieczeństwa dla konkretnych usług; w zależności od wykrytej usługi weryfikacja haseł; weryfikacja dostępu użytkowników do odpowiednich usług; weryfikacja możliwości dostępu do usługi; weryfikacja luk bezpieczeństwa w systemie operacyjnym; weryfikacja luk bezpieczeństwa w oprogramowaniu firm trzecich);
- **Sprawdzenie domyślnych haseł dla najistotniejszych hostów w sieci (serwery, bramy, switche, access point), które zostały wybrane na podstawie wcześniejszej analizy** (weryfikacja haseł w usługach umożliwiających logowanie);
- **Sprawdzenie możliwości wylistowania użytkowników oraz zdobycia haseł;**
- **Weryfikacja możliwości uzyskania dostępu do zasobów współdzielonych;**
- **Weryfikacja zabezpieczeń urządzeń sieciowych** (badanie odporności switchy na ataki sieciowe; weryfikacja zabezpieczeń monitoringu wizyjnego);
- **Testy sieci bezprzewodowej oraz weryfikacja zabezpieczeń sieci bezprzewodowej** (weryfikacja pod kątem dostępu, zabezpieczeń, haseł, w przypadku przechwycenia hasła – weryfikacja pod katem możliwości złamania hasła);
- **Zdalne testy adresów publicznych;**
- **Badanie ankietowe** (dot. pracowników działu IT Zamawiającego oraz pozostałych pracowników wyznaczonych do audytu);
- **Testy socjotechniczne** (kampanie phishingowe).

4. Wykonawca po wykonaniu usługi zobowiązany będzie do sporządzenia raportu dotyczącego bezpieczeństwa audytowanych elementów wraz ze wskazówkami jak poprawić sposób ochrony zasobów przedsiębiorstwa. Raport zostanie sporządzony i przekazany Zamawiającemu w terminie do 30 listopada 2022r..

5. Wykonawca udzieli Zamawiającemu wsparcia poaudytowego w zakresie udzielenia informacji na temat audytowanych elementów wynikających z raportu.

6. Audyt Bezpieczeństwa oparty będzie o:
   - Ankietę weryfikacji pod kątem dojrzałości cyberbezpieczeństwa;
   - Wymagania normatywne PN-EN ISO/IEC 27001:2017-06;
   - Wymagania normatywne PN-EN ISO 22301:2020-04;
   - Wewnętrzną dokumentację Zamawiającego;
   - Przepisy prawne o Krajowym Systemie Cyberbezpieczeństwa;
   - Standardy Krajowych Ram Interoperacyjności (KRI)

7. Nazwy i kody dotyczące przedmiotu zamówienia określone we Wspólnym Słowniku Zamówień:

   72.81.00.00-1 Usługi audytu komputerowego

4. TERMIN WYKONANIA ZAMÓWIENIA:

Termin wykonania zamówienia:

- Audyt zerowy: do 30.09.2022r.;
- Testy penetracyjne infrastruktury sieciowej i kampania phisingowa: do 15.11.2022r.;
- Audyt końcowy – do 30.11.2022r.

5. WARUNKI UDZIAŁU W POSTĘPOWANIU:

1. O zamówienie mogą ubiegać się Wykonawcy, którzy:
   - zaoferują przedmiot zamówienia zgodny z wymogami Zamawiającego określonymi w niniejszym zapytaniu ofertowym,
   - posiadają stosowne uprawnienia do przeprowadzenia audytu bezpieczeństwa IT;
   - posiadają certyfikat ISO/IEC 27001:2017,
   - udokumentują swoje doświadczenie w przygotowywaniu studiów wykonalności dla inwestycji o zakresie zbliżonym do przedmiotu niniejszego zamówienia/zapytania ofertowego. W celu spełnienia w/w wymogu Wykonawca zobowiązany jest do przedstawienia wykazu usług, zgodnie z załącznikiem nr 2 do niniejszego zapytania.
2. Okres związania ofertą wynosi 30 dni, licząc od dnia złożenia oferty.

6. KRYTERIA WYBORU OFERTY:

1. Przy wyborze oferty Zamawiający będzie kierował się następującym kryterium:
   Cena brutto – 100%
   (100% = 100,00 pkt.)
2. Przez cenę brutto należy rozumieć wartość całości zamówienia brutto (zawierającą obowiązujący podatek VAT), zaproponowaną w ofercie i zawierającą wszelkie koszty niezbędne do zrealizowania zamówienia.
3. Punktacja za kryterium „Cena brutto" zostanie obliczona z dokładnością do dwóch miejsc po przecinku w następujący sposób:

$$P_{bad.C} = \frac{C_{\min}}{C_{bad.}} x P_{C\max}$$ gdzie:

$P_{bad.C}$	- punkty za kryterium „Cena brutto" przyznane badanej ofercie
$C_{min.}$	- najniższa cena brutto spośród ocenianych ofert
$C_{bad.}$	- cena brutto badanej oferty
P_{Cmax}	- maksymalna liczba punktów, jaką można otrzymać w kryterium „Cena brutto"

4. Za najkorzystniejszą ofertę Zamawiający uzna ofertę niepodlegającą odrzuceniu z najniższą ceną.

7. SPOSÓB PRZYGOTOWANIA OFERTY:

1. Zamawiający dopuszcza wyłącznie składnie ofert obejmujących wykonanie całego przedmiotu zamówienia. Zamawiający nie dopuszcza możliwości składania ofert częściowych.
2. Wykonawca może złożyć tylko jedną ofertę, w formie pisemnej, na druku/wzorze stanowiącym Załącznik nr 1 do niniejszego zapytania ofertowego, w języku polskim.
3. Zamawiający nie dopuszcza ofert wariantowych lub alternatywnych.
4. Koszty związany z przygotowaniem oferty ponosi składający ofertę.
5. Do oferty Wykonawca zobowiązany jest dołączyć:
   - podpisane oświadczenie (Załącznik nr 2);
   - dokument/certyfikat potwierdzający wdrożenie systemu Zarządzania Bezpieczeństwem Informacji ISO/IEC 27001:2017
   - dwie referencje lub inne dokumenty, z ostatnich trzech lat, potwierdzających należyte wykonanie realizacji prezentowanych w ramach jego doświadczenia realizacji usług audytu bezpieczeństwa IT.
5. Oferta oraz dokumenty składane wraz z ofertą wymagają podpisu osób uprawnionych do reprezentowania Wykonawcy w obrocie gospodarczym, zgodnie z przepisami prawa.

8. MIEJSCE, SPOSÓB ORAZ TERMIN SKŁADANIA OFERT:

1. Termin składania ofert upływa: 07 września 2022r. do godz. 12.00.
2. Oferty można składać:
   1) w siedzibie Zamawiającego, tj. w sekretariacie (budynek administracji, I piętro, pokój nr 119) Szpitala Powiatowego w Rawiczu Sp. z o.o., ul. Gen. Grota Roweckiego 6, 63-900 Rawicz.,
   2) za pośrednictwem poczty elektronicznej na adres: renata.pazola@szpitalrawicz.pl wpisując w tytule maila: „Oferta na realizacji usługi audytu bezpieczeństwa IT",
   3) drogą pocztową na adres: Szpital Powiatowy w Rawiczu Sp. z o.o., ul. Gen. Grota Roweckiego 6, 63-900 Rawicz (decyduje data wpłynięcia oferty do sekretariatu Szpitala Powiatowego w Rawiczu Sp. z o.o., ul. Gen. Grota Roweckiego 6, 63-900 Rawicz. - budynek administracji, I piętro, pokój nr 119).
3. Oferty złożone po wyznaczonym terminie do składania ofert nie będą rozpatrywane.

9. INFORMACJE DODATKOWE:

1. Zamawiający informuje, że dopuszcza porozumiewanie się z potencjalnymi wykonawcami w formie pisemnej, elektronicznej lub faxem.
2. Okres związania ofertą wynosi 30 dni.
3. Zamawiający zastrzega sobie prawo do wyjaśnienia treści oferty w sytuacji gdy nie będzie w stanie prawidłowo jej ocenić oraz prawo żądania uzupełnienia dokumentów wymaganych od Wykonawcy.
4. Oferty których treść będzie sprzeczna z treścią „zapytania ofertowego" lub będą nieważne na podstawie przepisów prawa, zostaną odrzucone.
5. Zamawiający po wyborze oferty najkorzystniejszej prześle dla każdego z Wykonawców informację o wyborze pocztą elektroniczną lub faksem.

6. Zamawiający zawrze umowę z wybranym Wykonawcą bez zbędnej zwłoki.
7. Wykonawca zobowiązuje się po wyborze jego oferty jako najkorzystniejszej, do podpisania umowy z Zamawiającym na warunkach określonych w załączniku nr 3 do niniejszego zapytania ofertowego oraz treści oferty Wykonawcy.
8. Zamawiający zastrzega sobie prawo do unieważnienia „zapytania ofertowego" w sytuacji gdy realizacja jego przedmiotu nie będzie leżała w interesie Zamawiającego albo w sytuacji, kiedy cena najkorzystniejszej oferty przewyższać będzie kwotę, którą Zamawiający może przeznaczyć na sfinansowanie objętego nim zamówienia.
9. Potencjalnym wykonawcom nie przysługują środki ochrony prawnej, określone ustawie z dnia 11 września 2019r. Prawo zamówień publicznych (Dz.U.2021r. poz. 1129).

10. KONTAKT:

Wykonawca może zwrócić się z zapytaniem dot. treści zapytania ofertowego pisemnie na adres: renata.pazola@szpitalrawicz.pl .
Uprawniona do kontaktów w Wykonawcami jest:
Renata Pazoła – tel. 65 537 62 22.

WICEPREZES ZARZĄDU
Ewa Kaźmieruk