# Formularz cenowy

Dane WYKONAWCY\*:

*Pieczęć Wykonawcy\**

1. Nazwa wykonawcy: ................................................................................................
2. **NIP** wykonawcy: .....................................................................................................
3. **REGON** wykonawcy: .............................................................................................
4. Nazwisko osoby upoważnionej do kontaktów: .......................................................
5. adres wykonawcy: ..................................................................................................
6. kod pocztowy i miejscowość: .................................................................................
7. województwo..........................................................................................................
8. telefon: .............................................................
9. faks: .................................................................
10. poczta elektroniczna (e-mail): .................................................................................
11. adres internetowy (URL): ........................................................................................
12. kapitał zakładowy: .............................................

Ww. dane są niezbędne w celu wysyłania pod właściwy adres wszelkiej korespondencji, jak również do wpisywania odpowiednich danych w drukach ogłoszeń.

**Tabela nr 1**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***L.p.*** | **Przedmiot zamówienia** | | **Oferowany Produkt (symbol Produktu oraz nazwa producenta)** | **Cena jednostkowa**  **netto (PLN)** \* | **Wartość netto (PLN)** \* | **Stawka VAT %**\* | **Wartość VAT**\* | **Wartość brutto (PLN)** \* |
|  | System bezpieczeństwa w obrębie ruchu LAN i WAN | |  |  |  |  |  |  |
|  | | **CENAOFERTY** wynosi:  Słownie:................................................................................................................................\* PLN netto  Słownie:...............................................................................................................................\* PLN brutto  Wartość VAT wynosi słownie: ................................................................................................................\*PLN | | | |  |  |  |

1. Oferent udzieli Zamawiającemu gwarancji na dostarczony przedmiot zamówienia na okres ……. miesięcy.
2. Oświadczamy, że:

* zapoznaliśmy się z formularzem ofertowym i nie wnosimy do niego zastrzeżeń;

Stworzenie infrastruktury bezpieczeństwa zapewniającej zwiększenie poziomu detekcji zagrożeń w obrębie sieci LAN i WAN. Ponadto w obrębie danego systemu musi istnieć funkcja zdefiniowania Sewera pocztowego który pozwoli na szczegółową analizę ruchu SMTP oraz wykrywania zagrożeń związanych z zainfekowanymi plikami lub spoofingiem. W związku z dużą liczbą użytkowników znajdujących się w organizacji szpitalnej konieczna jest stworzenie struktury AAA (Authentication, Authorization, Accounting) pozwalającej na kontrolę dostępów do sieci komputerowej organizacji jak i zapewniającej centralizację uwierzytelnienia   
z wykorzystaniem mechanizmów 2FA. Konieczne jest aby dane związane z powyższymi założeniami trafiały na centralne repozytorium logów umożliwiające ich analizę wraz z generowaniem raportów związanych   
z naruszeniem zasad bezpieczeństwa jak i przepływem ruchu sieciowego.

Specyfikacja systemu:

**1. Minimalne wymagania systemu bezpieczeństwa w obrębie ruchu LAN i WAN:**

• Obsługę przynajmniej 270 tysięcy połączeń TCP na sekundę

• Wydajność w obrębie SSL-VPN na poziomie minimum 2 Gbps

• Wydajność skanowania ruchu na poziomie minimum 3 Gbps

• Możliwość inspekcji ruchu szyfrowanego na poziomie minimum 3.9 Gbps

• Realizowanie kontroli Aplikacji, IPS oraz Antywirusowej

• Możliwość tworzenia profili filtrów WEB

• Rozwiązanie musi posiadać dostęp do baz reputacyjnych zawierających adresy IP oraz wpisy FQDN dla poszczególnych domen

• W obrębie sygnatur wymagane jest aby system posiadał sygnatury związane z ochroną urządzeń mobilnych

• System musi realizować funkcje wysokiej dostępności gdzie w razie uszkodzenia jednego z elementów nie dojdzie do przerwania procesów związanych z analizą reguł bezpieczeństwa

**2. Minimalna funkcjonalność systemu ochrony poczty w obrębie systemu musi zapewniać:**

• Ochronę antyspamową, antywirusową antyspyware’ową bez limitu licencyjnego na ilość chronionych kont użytkowników

• Obsługę serwisów pocztowych: SMTP, POP3, IMAP.

• Szyfrowany dostęp do poczty poprzez WebMail – z wykorzystaniem protokołu SSL (w tym zakresie musi wspierać protokoły: SSL, TLS 1.0, TLS 1.1, TLS 1.2 oraz TLS 1.3).

• Lokalne konta użytkowników oraz możliwość czerpania kont pocztowych z zewnętrznego serwera LDAP.

• Możliwość zdefiniowania nie mniej niż 60 polityk kontroli antywirusowej oraz antyspamowej

• Funkcję usuwania z załączników aktywnej zawartości która może wymusić uruchomienie procesów na komputerze odbiorcy a tym samym doprowadzić do naruszenia bezpieczeństwa infrastruktury szpitalnej

• Funkcję wykrywania i ochrony przed spoofingiem pod widomościami wysyłanymi przez osoby znajdujące się na decyzyjnych stanowiskach w obrębie infrastruktury Zamawiającego

**3. Minimalna funkcjonalność systemu pozwalająca na centralne zarządzanie kontami użytkowników wraz z monitoringiem ich procesów uwierzytelnienia:**

• Obsługa minimum 2000 użytkowników w obrębie systemu obsługując:

• Konfiguracje polityk wymuszających na użytkownikach zasady złożoności haseł czy 2FA

• Obsługę serwera CA w obrębie systemu oraz funkcjonalność zarządzania certyfikatami

• System musi umożliwiać realizację uwierzytelniania z wykorzystaniem protokołu 802.1x, spełniając nie mniej niż następujące warunki:

• Umożliwia wdrożenia mechanizmów 2FA

**4. Minimalne funkcjonalności systemu zapewniające centralizację systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń:**

• Wymagane jest aby system potrafił przyjąć minimum 5 GB logów dziennie wraz z zapewnieniem korelacji z co najmniej 1000 systemów

• Funkcję analizy logów archiwalnych względem aktualnej wiedzy producenta o zagrożeniach, w celu wykrycia potencjalnych stacji narażonych na zagrożenie

Jeżeli system nie może być dostarczony w postaci jednolitego rozwiązania wymagane jest aby poszczególne jego elementy współpracowały ze sobą pozwalając np. na centralizację procesów logowania zdarzeń.