Załącznik nr 2b do SWZ

**Formularz cenowy/ Opis minimalnych parametrów technicznych**

**Cześć II: Zakup, dostawa, uruchomienie i wdrożenie urządzenia brzegowego UTM+ rozwiązanie MDR + Ochrona poczty**

**Cena Sprzętu:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Lp.** | **Nazwa sprzętu** | **Producent i typ/ model urządzenia** | **Ilość** | **Cena netto** | **Wartość netto** | **Podatek VAT %** | **Wartość VAT w zł.** | **Wartość brutto** |
| **1.** | **Urządzenie brzegowe UTM** |  | **2** |  |  |  |  |  |
| **2.**  | **Ochrona poczty** |  |  |  |  |  |  |  |
| **3.** | **Rozwiązanie MDR** |  |  |  |  |  |  |  |
| **4.**  | **Uruchomienie** |  |  |  |  |  |  |  |

Wykonawca dostarczy, zainstaluje i uruchomi i wdroży urządzenia brzegowego UTM+ rozwiązanie MDR + Ochrona poczty w lokalizacji Zamawiającego o cechach i parametrach zgodnych z poniższymi tabelami:

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Nazwa elementu, parametru****lub cechy** | **Minimalne parametry techniczne** | **Parametry oferowane** |
| **1.** | Typ obudowy | Obudowa powinna umożliwiać zainstalowanie w standardowej szafie RACK 19”. W obudowie podstawowej o wysokości nie przekraczającej 2U. |  |
|  | Parametry oraz funkcje | 1. Rozwiązanie powinno być dostarczone jako klaster wysokiej dostępności pracujący w trybie HA Active-Passive lub Active-Active. Rozwiązanie powinno posiadać:
* port USB umożliwiający podłączenie modemów 4G/LTE produkowanych przez firmy trzecie.
1. Parametry:
* pamięć operacyjna RAM nie mniej niż 8 GB,
* liczba fizycznych interfejsów 1000BASE-T nie mniej niż 8,
* liczba fizycznych interfejsów 1000BASE-X nie mniej niż 2,
* Musi obsługiwać protokoły dynamicznego routingu: RIP v1/v2, OSPF i BGP4,
* wydajność sprzętu nie może być mniejsza niż 10 Gbps,
* liczba równoczesnych połączeń nie może być mniejsza niż 2.200.000,
* wydajność IPS nie mniejsza niż 6 Gbps,
* wydajność IPsec VPN nie może być mniejsza niż 5 Gbps,
* liczba nowych połączeń na sekundę nie mniejsza niż: 130.000,
* wydajność dla inspekcji ruchu SSL/TSL, nie może być mniejsza niż 696 Mbps,
* liczba równoczesnych połączeń SSL/TLS nie może być mniejsza niż 2500,
* liczba równoczesnych tuneli SSL VPN nie może być mniejsza niż 2500,
* ochrona IPS musi opierać się co najmniej na analizie protokołów i bazie minimum 5000 sygnatur,
1. Funkcje:
* musi umożliwiać zdefiniowanie co najmniej 5 stref bezpieczeństwa (Zewnętrzna, DMZ1, DMZ2, Wewnętrzna1, Wewnętrzna2),
* powinno oferować mechanizm uwierzytelniania dwuskładnikowego w oparciu o token sprzętowy lub programowy,
* rozwiązanie powinno być zarządzane przez webowy graficzny interfejs administratora (Web GUI) działający w czasie rzeczywistym,
* możliwość zmiany nazw interfejsów sieciowych,
* możliwość definiowania profili administracyjnych,
* narzędzie analizy incydentów bezpieczeństwa,
* rozwiązanie powinno zawierać kategorie stron Web oraz umożliwiać dodawanie własnych kategorii stron lub dodawanie wyjątków na podstawie wyrażeń regularnych,
* wymagane jest, aby system automatycznie aktualizował sygnatury zagrożeń,
* system powinien zapewniać ochronę przed atakami DoS czy DDoS – co najmniej (ICMP Flood, Syn Flood, UDP Flood, Ilość połączeń, IP Spoofing),
* możliwość składowania oraz archiwizacji logów na urządzeniu oraz przeglądania w czasie rzeczywistym,
* rozwiązanie musi posiadać zestaw predefiniowane raportów, które mają możliwość dopasowania do instytucji użytkującej rozwiązanie,
* system ma być w stanie zautomatyzować generowanie raportów i mieć możliwość wysyłania ich pocztą e-mail,
* system powinien oferować funkcjonalność serwera DHCP dla IPv4 oraz IPv6 i DHCP Relay,
* musi mieć możliwość automatycznego przełączania ruchu pomiędzy interfejsami zewnętrznymi w przypadku awarii jednego z nich,
* musi umożliwiać transparentne uwierzytelnianie użytkowników przy integracji z Active Directory,
* musi pełnić rolę bramki VPN terminującej połączenia VPN site-to-site i client-to-site,
* rozwiązanie powinno w trybie rzeczywistym weryfikować bazę zagrożeń producenta,

producent musi dostarczyć bezpłatnie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPsec client-to-site VPN jak i SSL client-to-site VPN. |  |
| **2.** | Ochrona poczty e- mail | Rozwiązanie musi umożliwiać:* skanowanie poczty email przy wykorzystaniu protokołów SMTP, POP3 i IMAP oraz zapewniać szyfrowanie TLS dla tych protokołów,
* blokowanie spamu oraz zainfekowanych plików, wsparcie funkcjonalności;
* musi posiadać min. 2 silniki antywirusowe,
* skanowanie, wykrywanie i blokowania załączników określonych typów,
* kwarantannę wiadomości e-mail przesyłanych protokołem SMTP, wskazanych przez moduł Antyspam,

licencja rozwiązania nie powinna opierać się na ilości skrzynek e-mail użytkowników i objąć wszystkie skrzynki w obrębie domeny. |  |
|  | Integracja | Dostarczone rozwiązanie powinno umożliwiać zintegrowanie w ramach całościowego spójnego systemu zapewniającego większy poziom cyberbezpieczeństwa. Musi być dostarczone ze wszystkimi licencjami/subskrypcjami umożliwiającymi uzyskanie funkcjonalności wymienionymi w niniejszej specyfikacji. Długość trwania licencji/subskrypcji nie może być krótsza niż okres wsparcia technicznego. Wykonawca musi do realizacji zamówienia wskazać minimum dwie osoby legitymujące się certyfikatem producenta oferowanego rozwiązania. Urządzenie musi być nowe, nigdy wcześniej nie używane i pochodzić z autoryzowanego kanału dystrybucji producenta. |  |
|  | Instalacja | Prace instalacyjne: 1. Przygotowanie i przedstawienie koncepcji wdrożenia w środowisku Zamawiającego.2. Wdrożenie urządzenia UTM:2.1. Dostarczenie urządzenia do siedziby Zamawiającego.2.2. Montaż urządzenia w siedzibie Zamawiającego.2.3. Podłączenie logiczne i elektryczne urządzenia.2.4. Konfiguracja adresacji IP.2.5. Konfiguracja kont administracyjnych z odpowiednio silnym hasłem.2.6. Konfiguracja wysyłania powiadomień o problemach na email.2.7. Aktualizacja oprogramowania sprzętowego do najnowszej dostępnej wersji rekomendowanej przez producenta.2.8 Szkolenie pracownika IT w zakresie obsługi nowego urządzenia w ramach prac wdrożeniowych, potwierdzone protokołem – transfer wiedzy z użytych w czasie wdrożenia funkcjonalności oraz technik ich konfiguracji, omówienie procedur serwisowych i eskalacyjnych w przypadku zaistnienia problemów.2.9. Przeprowadzenie testów Sprzętu, polegających na:- sprawdzeniu zgodności wdrożenia z dokumentacją powykonawczą opracowaną przez Wykonawcę,- sprawdzenie parametrów dostarczonego Sprzętu.3. Przygotowanie dokumentacji powdrożeniowej |  |
|  | Gwarancja | Wymagana jest gwarancja świadczona na wszystkie elementy urządzenia (sprzęt oraz oprogramowanie) na okres minimum 36 miesięcy. Zamawiający wymaga, aby usługi serwisowe świadczone były wyłącznie przez autoryzowany serwis producenta oferowanego sprzętu. Dostarczone licencje nie mogą być krótsze niż okres 36 miesięcy.Dostawca będzie odpowiedzialny za pełną integrację nowych urządzeń UTM z istniejącą infrastrukturą sieciową Zamawiającego, w tym z przełącznikami sieciowymi. |  |
|  | Wymagane certyfikaty: | Wykonawca musi do realizacji zamówienia wskazać osoby/ę legitymujące się certyfikatem producenta oferowanego rozwiązania. Wdrożenia i dostawy musi dokonać Wykonawca będący autoryzowanym partnerem wszystkich szczebli producentów oferowanych rozwiązań lub posiadać stosowne umowy z producentem lub oficjalnym dystrybutorem marki na przeprowadzenie wdrożeń oraz dostawy w/w sprzętu i oprogramowania. Wykonawca przedstawi stosowne dokumenty (certyfikat lub umowy współpracy z producentem marki). Wykonawca dostarczy oświadczenie o pochodzeniu sprzętu z oficjalnej dystrybucji. Wdrożenie zostanie przeprowadzone przez certyfikowanego inżyniera danego rozwiązania. |  |

Dostawa oraz uruchomienie oprogramowania do ochrony stacji końcowych i serwerów wraz z zapewnieniem usługi całodobowego monitorowania i analizy zagrożeń oraz reagowania na nie.

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Nazwa elementu, parametru****lub cechy** | **Parametry wymagane minimalne** | **Parametry oferowane** |
| **3.** | Parametry oraz funkcje | Oprogramowanie musi:* zawierać funkcję zastosowania wielu polityk bezpieczeństwa jednocześnie,
* być zarządzane z pojedynczej, centralnej konsoli, znajdującej się na serwerach producenta, do której dostęp zapewniony jest przez przeglądarkę internetową,
* posiadać zarządzalny mechanizm aktualizacji,
* mechanizm kontroli aplikacji, mechanizm kontroli dostępu dla urządzeń peryferyjnych,
* wykrywanie zagrożeń typu malware w oparciu o mechanizm tzw. głębokiego uczenia,
* posiadać ochronę typu anty - ransomware, w tym także dla MBR (Master Boot Record),
* umożliwiać zintegrowanie z urządzeniem typu UTM przedstawionym w części I,
* agent implementowany na stacjach końcowych oraz serwerach musi posiadać interfejs użytkownika w języku polskim,
* lista urządzeń posiadających zainstalowanego agenta zawiera informacje dotyczące: nazwy hosta, adresu IP, systemu operacyjnego, informacji o ostatnim podłączeniu oraz aktualnym statusie,
* agent instalowany na stacjach końcowych i serwerach monitoruje i zbiera informacje na temat co najmniej następujących zdarzeń:

• dostę­­p do pliku,• tworzenie nowego procesu,• nawiązane połączenia sieciowe,• wpisy dziennika systemu, niezbędne do wykrycia naruszeń bezpieczeństwa,• zawartość skryptów uruchamianych na monitorowanej stacji.Oprogramowanie powinno wykorzystywać następujące mechanizmy: * analiza przed uruchomieniem programu (HIPS);
* blokowanie potencjalnie niechcianych aplikacji (PUA),
* analiza zachowań aplikacji (HIPS),
* wykorzystywać mechanizmy wykrywania zagrożeń powiązanych ze sobą procesów,
* wykrywanie podejrzanych zdarzeń i przydzielanie im poszczególnych priorytetów.

Ilość stacji roboczych – 60 szt.Ilość systemów serwerowych – 10 szt. Dostarczone licencje nie mogą być krótsze niż okres 36 miesięcy. |  |
|  | Usługa całodobowego monitorowania i analizy zagrożeń oraz reagowania na nie | Producent oprogramowania musi być w stanie zapewnić usługę całodobowego monitorowania, wykrywania i analizy zagrożeń oraz reagowania na nie. Analiza musi być prowadzona przez ekspertów w zakresie cyberbezpieczeństwa w harmonogramie 24/7/365. Prowadzona analiza dotyczyć musi danych zebranych w wyniku działania dostarczonego oprogramowania do ochrony stacji końcowych oraz serwerów, a także danych uzyskanych dzięki działaniu urządzenia klasy UTM (opisanym w części I).Identyfikacja potencjalnych incydentów bezpieczeństwa na podstawie wykryć poprzez ich weryfikację i badanie w celu ustalenia, czy są to prawdziwe incydenty, które wymagają działań naprawczych, czy incydenty typu false-positive, które można zamknąć.Podejmowanie zdecydowanych i odpowiednich działań wyjaśniających, ograniczających i eliminujących w imieniu ZamawiającegoProducent musi dostarczać klientowi cotygodniowe oraz miesięczne raporty na temat przeprowadzonej analizy oraz stanu zagrożeń. Producent musi mieć możliwości do przerwania wykrytego ataku oraz podjęcia kroków w celu zapobiegnięcia rozprzestrzenianiu się ataku na inne elementy infrastruktury klienta. Producent musi zapewnić klientowi bezpośrednie wsparcie telefoniczne oraz doradztwo w zakresie podejmowanych działań w przypadku wystąpienia incydentu bezpieczeństwa. Dane zbierane przez agentów na stacjach końcowych i serwerach są, przechowywane i przetwarzane na obszarze Europejskiej Wspólnoty Gospodarczej. |  |
|  | Instalacja | Prace instalacyjne:1. Przygotowanie i przedstawienie koncepcji wdrożenia w środowisku Zamawiającego.2. Wdrożenie rozwiązania w środowisku Zamawiającego:2.1. Konfiguracja kont administracyjnych z odpowiednio silnym hasłem.2.2. Konfiguracja wysyłania powiadomień o wykrytych zdarzeniach.2.3. Pomoc w opracowaniu polityk bezpieczeństwa zgodnych z przyjętymi politykami bezpieczeństwa w organizacji Zamawiającego.3. Przygotowanie dokumentacji powdrożeniowej |  |