



**Załącznik nr 1
do zapytania ofertowego**

Opis przedmiotu zamówienia

Załącznik do zapytania ofertowego na: Dostarczenie, wdrożenie i utrzymanie systemów zapewniających prewencję, detekcję i reakcję na zagrożenia cyberbezpieczeństwa w ramach projektu "Zwiększenie poziomu bezpieczeństwa informacji w jednostkach organizacyjnych Powiatu Braniewskiego"

1. Opis wdrożenia:

Celem przedsięwzięcia jest modernizacja i rozbudowa istniejącej infrastruktury sieciowej Starostwa Powiatowego w Braniewie i dwunastu jednostek organizacyjnych Powiatu Braniewskiego.

Starostwo i jednostki zostaną połączone w jedną sieć, w ramach której realizowany będzie dostęp do wspólnych zasobów i sieci Internet, zarządzany centralnie. Dostęp ten zostanie zrealizowany za pomocą urządzenia klasy UTM, które zastąpi obecnie używaną jednostkę. Dostęp do sieci Internet zostanie zapewniony poprzez bezpośrednie połączenie łącz WAN pochodzących od dwóch niezależnych dostawców usługi. Dla łączy tych zostanie skonfigurowane połączenie SD-WAN, dzięki czemu możliwe będzie zapewnienie automatycznego, dynamicznego wyboru wykorzystywanego łącza na podstawie zdefiniowanych parametrów takich jak np. jakość lub dostępność łącza w danym czasie.

Dodatkowo, w ramach modernizacji infrastruktury w siedzibie Starostwa, dostarczone zostaną 3 szt. switchy posiadających minimum 48 portów GE RJ45 i 4 porty 10GE SFP+. Ze switchami zostanie dostarczonych 8 wkładek SFP+ 10 Gbps wraz z patchcordami światłowodowymi o długości 3 m, które posłużą do połączenia switchy z modernizowaną infrastrukturą. Połączenie z pozostałymi elementami infrastruktury zostanie zrealizowane przy zapewnieniu agregacji przepustowości jak również redundancji połączenia. Zarządzanie switchami będzie się odbywało z poziomu kontrolera stanowiącego integralną część głównej jednostki UTM.

Celem zapewnienia bezpiecznego i niezawodnego dostępu do sieci bezprzewodowej w siedzibie Starostwa zostaną dostarczone i skonfigurowane dwa wewnętrzne punkty dostępowe działające w technologii RF - 2x2 Wi-Fi 6 (802.11ax).

Połączenia pomiędzy Starostwem a jednostkami organizacyjnymi Powiatu zostaną wykonane przy pomocy posiadanej przez Starostwo infrastruktury światłowodowej i switcha, który będzie posiadał minimum 24 porty GE SFP i 4 porty 10GE SFP+. Wraz ze switchem zostanie dostarczonych 12 wkładek SFP 1 Gbps wraz z patchcordami światłowodowymi o długości 1 m oraz 4 wkładki SFP+ 10 Gbps wraz z patchcordami światłowodowymi o długości 3 m. Połączenie z pozostałymi elementami infrastruktury zostanie zrealizowane przy zapewnieniu agregacji przepustowości jak





również redundancji połączenia. Switch ten zarządzany będzie przy pomocy tego samego kontrolera, co wymienione powyżej switche wykorzystane do modernizacji infrastruktury sieciowej Starostwa.

Ponadto do jednostek organizacyjnych Powiatu dostarczone zostaną urządzenia klasy UTM wyposażone minimum w 1 port GE RJ45 WAN oraz 4 porty GE RJ45 LAN tak, aby można było definiować reguły i profile bezpieczeństwa dla potrzeb zarządzanej jednostki bez konieczności zakłócania pracy Starostwa czy też pozostałych jednostek.

W Starostwie i w każdej jednostce organizacyjnej Powiatu, w zależności od potrzeby, zostanie przeniesiona z dotychczas używanych urządzeń lub utworzona od podstaw konfiguracja zapewniająca prawidłowe funkcjonowanie urządzenia UTM. Konfiguracja będzie obejmowała również utworzenie tuneli IPSec, z sieci publicznej do siedziby Starostwa i każdej jednostki organizacyjnej Powiatu, zapewnienie bezpiecznego dostępu z zewnątrz do utrzymywanych przez Starostwo usług oraz zabezpieczenie pozostałego ruchu wychodzącego i przychodzącego.

Dopełnieniem wyżej opisanego projektu będzie dostarczenie i konfiguracja narzędzia do centralnego zarządzania posiadaną infrastrukturą. Rozwiązanie do centralnego zarządzania umożliwi kontrolę i monitorowanie pracy rozproszonych urządzeń UTM. Pozwoli na zdalne wdrażania polityk bezpieczeństwa, kontrolowanie profili UTM oraz wdrożenie wieloosobowego trybu pracy administratorów. Dodatkowo pozwoli kontrolować proces zdalnego wdrażania aktualizacji oprogramowania.

Kolejnym elementem uzupełniającym strukturę będzie narzędzie do analizy zagrożeń i logów z wszystkich urządzeń UTM. Narzędzie pozwoli na centralne składowanie logów i zdarzeń z określonego przedziału czasu, wdrożenie mechanizmu alarmowania oraz umożliwi generowanie raportów zarówno predefiniowanych i jak personalizowanych.

Wspomniane narzędzia dostępne będą w postaci maszyn wirtualnych uruchamianych w ramach infrastruktury posiadanej przez Starostwo. Rozwiązanie do centralnego zarządzania zapewni obsługę minimum 20 urządzeń sieciowych. Narzędzie przeznaczone do analizy zagrożeń pozwoli na gromadzenie minimum 10 GB danych dziennie.

Przeprowadzone zostaną szkolenia administratorów w zakresie obsługi tych rozwiązań, tj. szkolenie obejmujące administrowanie systemem zarządzania urządzeniami sieciowymi oraz systemem zbierającym i analizującym logi z urządzeń sieciowych.

Dostarczone rozwiązania muszą być zgodne i współpracować z używanymi w Starostwie Powiatowym w Braniewie i jednostkach organizacyjnych Powiatu urządzeniami Fortinet.

2. Wymagania, dotyczące wsparcia serwisowego w czasie procesie wdrożeniowym oraz powdrożeniowym:

2.1. Wdrożony system musi być objęty serwisem gwarancyjnym producenta przez okres 18 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach





tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Kluczowe dla ciągłości działania, wskazane elementy systemu muszą być ponadto objęte rozszerzonym wsparciem technicznym gwarantującym udostępnienie, dostarczenie oraz instalację sprzętu zastępczego na czas naprawy sprzętu w ciągu 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 18 miesięcy. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe muszą być przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7.

Wymagania powinny być potwierdzone następującymi dokumentami:

- a) Oświadczenie podmiotu świadczącego wsparcie techniczne (producenta lub autoryzowanego dystrybutora) o gotowości świadczenia wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej),
- b) Kopię certyfikat ISO 9001 podmiotu świadczącego wsparcie techniczne.

2.2. Wykonawca w całym procesie wdrożeniowym oraz powdrożeniowym zapewni pełne wsparcie serwisowe oraz pomoc techniczną dla dostarczonego rozwiązania w postaci minimum 2 inżynierów posiadających certyfikaty znajomości dostarczonego systemu. Kopie niżej wymienionych certyfikatów potwierdzających kompetencje Wykonawcy w minimum trzech obszarach bezpieczeństwa, należy dołączyć do formularza ofertowego jako załączniki:

- a) FCP Security Operations: Umiejętność zabezpieczania sieci i aplikacji poprzez wdrażanie, zarządzanie i monitorowanie urządzeń Fortinet związanych z operacjami bezpieczeństwa.
- b) FCSS Network Security: Umiejętność zabezpieczania sieci i aplikacji za pomocą produktów Fortinet do zabezpieczenia sieci, w tym wdrażania, zarządzania i monitorowania.
- c) FCP Public Cloud Security: Umiejętność zabezpieczania aplikacji działających w chmurze publicznej poprzez zarządzanie, wdrażanie i monitorowanie rozwiązań Fortinet.

2.3. Wykonawca ponadto przekaze Zamawiającemu kopie certyfikatów pracowników potwierdzające kompetencje w obszarach rozwiązań, których wdrożenie dotyczy, tj:

- a) Certyfikat egzaminu Enterprise Firewall Administrator potwierdza specjalistyczną wiedzę w zakresie rozwiązań Fortinet w środowiskach infrastruktury bezpieczeństwa przedsiębiorstwa składających się z wielu urządzeń FortiGate. (integracja, administrowanie, rozwiązywanie problemów i centralnego zarządzania rozwiązaniem korporacyjnej zapory ogniowej).
- b) Certyfikat egzaminu FortiAnalyzer Analyst potwierdza specjalistyczną wiedzę w zakresie analityki i automatyzacji sieci zabezpieczeń przy użyciu FortiAnalyzer





- (scentralizowane rejestrowanie i analiza logów FortiAnalyzer oraz korzystania z podręczników do zarządzania incydentami, raportami i automatyzacją zadań).
- c) Certyfikat egzaminu administratora FortiManager potwierdza wiedzę specjalistyczną w zakresie zarządzania zaporami sieciowymi i siecią za pomocą FortiManager (wdrażanie, konfiguracja i codzienne administrowanie FortiManager oraz scentralizowane administrowanie siecią urządzeń FortiGate).
 - d) Certyfikat egzaminu SD-WAN Architect potwierdza wiedzę specjalistyczną w zakresie rozwiązania Fortinet SD-WAN (integracja, administrowanie, rozwiązywanie problemów i centralne zarządzanie bezpiecznym rozwiązaniem SD-WAN składającym się z FortiOS, FortiManager i FortiAnalyzer).

3. Zestawienie urządzeń i usług

- 3.1. Ochrona sieci w warstwie brzegowej - wymiana urządzenia UTM w Starostwie oraz zakup wsparcia, tj.: Wymiana urządzenia FortiGate 60E na urządzenie Fortigate 120G z pakietem licencyjnym UTP (Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium) na okres 18 miesięcy oraz rozszerzonym wsparciem Hezo SOS na okres 18 miesięcy
- 3.2. Ochrona sieci - zakup nowych i wymiana urządzeń UTM do jednostek organizacyjnych. Zakup usług wsparcia dla 24x7 dla urządzeń, tj.:
- a) zakup **sześciu** urządzeń Fortigate 40F z pakietem Forticare Premium (FortiCare Premium Ticket Handling, Advanced Hardware Replacement (NBD), Firmware and General Upgrades, Application Control) na okres 18 miesięcy
 - b) wymiana **dwóch** urządzeń FortiGate 30E na urządzenia Fortigate 40F z pakietem Forticare Premium (FortiCare Premium Ticket Handling, Advanced Hardware Replacement (NBD), Firmware and General Upgrades, Application Control) na okres 18 miesięcy
- 3.3. Ochrona sieci - zakup urządzenia do zarządzania połączeniami i monitorowania połączeń z jednostkami. Zakup urządzenia ze wsparciem, tj.: Zakup urządzenia FortiSwitch 424E-Fiber z pakietem Forticare Premium (FortiCare Premium Ticket Handling, Advanced Hardware Replacement (NBD), Firmware and General Upgrades, Application Control) na okres 18 miesięcy oraz rozszerzonym wsparciem Hezo SOS na okres 18 miesięcy wraz z modułami optycznymi, tj. 12 modułami 1GE SFP LX LC oraz 4 modułami 10GE SFP+ SR LC. Moduły optyczne mogą pochodzić od innego producenta, ale muszą być w pełni kompatybilne z urządzeniem.
- 3.4. Ujednolicenie urządzeń sieciowych w Starostwie poprzez zakup i wymianę przełączników zarządzalnych w warstwie sieci, tj.: Zakup trzech przełączników FortiSwitch FS-148F z pakietem Forticare Premium (FortiCare Premium Ticket Handling, Advanced Hardware Replacement (NBD), Firmware and General Upgrades, Application Control) wraz z modułami optycznymi, tj.





łącznie 8 modułami 10GE SFP+ SR LC. Moduły optyczne mogą pochodzić od innego producenta, ale muszą być w pełni kompatybilne z przełącznikami.

- 3.5. Utworzenie bezpiecznych i nadzorowanych sieci bezprzewodowych poprzez zakup punktów dostępowych, tj. Zakup dwóch urządzeń FortiAP-231F z pakietem Forticare Premium (FortiCare Premium Ticket Handling, Advanced Hardware Replacement (NBD), Firmware and General Upgrades, Application Control) na okres 18 miesięcy oraz zasilaczem GPI-130
- 3.6. Zakup i wdrożenie menedżera urządzeń aktywnych sieci: UTM routery i switchy: narzędzia umożliwiającego zarządzanie urządzeniami aktywnymi w Starostwie i jednostkach organizacyjnych Powiatu, tj.: Zakup i wdrożenie systemu do zarządzania FortiManager z pakietem FortiCare Premium (Subscription license for 20 devices/vdoms managed by FortiManager VM S-series, including FortiCare Premium.) na okres 18 miesięcy
- 3.7. Zakup systemu monitorującego zdarzenia na urządzeniach aktywnych sieci, tj.: Zakup systemu do analizy logów FortiAnalyzer w pakiecie z licencjami IOC, Security Automation, Outbreak Detection oraz FortiCare Premium (Subscription license for 10 GB/Day Central Logging & Analytics. Include FortiCare Premium support, IOC, Security Automation Service and FortiGuard Outbreak Detection Service) na okres 18 miesięcy.
- 3.8. Instalacja i konfiguracja urządzeń i systemów ochrony sieci
- 3.9. Szkolenie dla dwóch informatyków, w wymiarze 16 godzin, obejmujące administrowanie urządzeniami sieciowymi oraz systemem zbierającym i analizującym logi z urządzeń sieciowych.

4. Inne wymagania

- 4.1. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2023, poz. 1582) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
- 4.2. Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

