Murowana Goślina, dnia 18.05.2023 r.

Burmistrz Miasta i Gminy Murowana Goślina
z siedzibą w Murowanej Goślinie przy placu Powstańców Wielkopolskich 9

ZAPRASZA
do złożenia oferty na rozbudowę zabezpieczeń logicznych (firewall, systemy IDS, IPS), szkolenie online dla pracowników urzędu w zakresie obsługi zakupionego sprzętu i oprogramowania, długookresowe utrzymanie logów z urządzenia UTM w chmurze, licencje oprogramowania do zintegrowanego zarządzania urządzeniami w sieci i bezpieczeństwa IT oraz moduł oprogramowania do zintegrowanego zarządzania urządzeniami w sieci i bezpieczeństwa IT.

I. Zamawiający:

Gmina Murowana Goślina
plac Powstańców Wielkopolskich 9
62-095 Murowana Goślina
tel. (+48) 61 8923 600
www.murowana-goslina.pl

II. Tryb postępowania:

1. Postępowanie prowadzone w oparciu o art. 2 pkt. 1 ust. 1 ustawy z dnia 11 września 2019 roku Prawo Zamówień Publicznych.
2. Zamówienie prowadzone jest zgodnie z zasadą konkurencyjności, o której mowa w sekcji 6.5.2 Wytycznych w zakresie kwalifikowalności wydatków w ramach Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego oraz Funduszu Spójności na lata 2014-2020.
3. Zamawiający informuje, że może unieważnić postępowanie, jeżeli cena najkorzystniejszej oferty przewyższy kwotę, którą Zamawiający może przeznaczyć na zamówienie.

III. Miejsce i sposób składania ofert:

1. Każdy Oferent może złożyć tylko jedną ofertę w niniejszym postępowaniu.
2. Zamawiający nie dopuszcza składania ofert częściowych oraz ofert wariantowych.
3. **Ofertę należy złożyć w nieprzekraczalnym terminie do dnia 25.05.2023 r. do godz. 12:00.**
4. Ofertę należy sporządzić w formie pisemnej, w języku polskim, z uwzględnieniem waluty polskiej PLN, na Formularzu ofertowym, stanowiącym Załącznik nr 1 do niniejszego Zapytania ofertowego.
5. Oferta musi zostać złożona w następującej formie:
   - w formie elektronicznej poprzez stronę internetową **https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl**

Instrukcja złożenia oferty przez oferenta znajduje się pod linkiem https://archiwum-bazakonkurencyjnosci.funduszeeuropejskie.gov.pl/info/web_instruction

6. Oferta oraz wszelkie oświadczenia składane przez Wykonawcę w toku postępowania winny być podpisane przez osoby upoważnione do składania oświadczeń woli w imieniu Wykonawcy. Jeżeli Wykonawcę reprezentuje pełnomocnik, do oferty należy dołączyć pełnomocnictwo udzielone przez uprawnione osoby w imieniu Wykonawcy, zgodnie z zasadami reprezentacji wskazanymi we właściwym rejestrze lub ewidencji działalności gospodarczej.
7. Oferta winna być podpisana w sposób umożliwiający identyfikację osoby składającej podpis - elektronicznym podpisem zaufanym poprzez Profil Zaufany lub kwalifikowanym podpisem elektronicznym.
8. Oferent jest związany ofertą przez okres 30 dni. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.
9. Wszelkie koszty związane z przygotowaniem oferty ponosi Wykonawca.
10. Wykonawca może wprowadzić zmiany lub wycofać złożoną ofertę pod warunkiem, że Zamawiający otrzyma pisemne powiadomienie o wprowadzeniu zmian lub wycofaniu przed upływem terminu składania ofert. Zarówno zmiana jak i wycofanie oferty wymagają zachowania formy wskazanej w ustępie 5 niniejszego rozdziału.
11. Wykonawca nie może wycofać oferty ani wprowadzić jakichkolwiek zmian w treści oferty po upływie terminu składania ofert.
12. Oferty złożone po terminie bądź w inny sposób niż wskazany powyżej nie będą rozpatrywane.
13. **Otwarcie ofert nastąpi w siedzibie Zamawiającego w dniu 25.05.2023 r. o godz. 13:00.**
14. Zamawiający nie przewiduje publicznego otwarcia ofert.

IV. Komunikacja z Zamawiającym:

1. Komunikacja z Zamawiającym odbywa się poprzez stronę internetową **https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl**
2. Oferent może zwrócić się do Zamawiającego o wyjaśnienie treści Zapytania ofertowego w sposób wskazany w ust. 1 niniejszego rozdziału, nie później jednak niż na dwa dni przed upływem terminu składania ofert.
3. Zamawiający będzie publikował wszelkie informacje dotyczące postępowania, w tym odpowiedzi na wnioski o wyjaśnienie treści Zapytania ofertowego lub zmiany treści zapytania na stronie: https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl
4. Osobą upoważnioną z ramienia Zamawiającego do kontaktu i udzielania wyjaśnień w sprawie niniejszego Zapytania ofertowego jest Dominik Kowal; e-mail: **ofertyit@murowana-goslina.pl**; tel. **61 8923 651**.

V. Opis przedmiotu zamówienia

Przedmiotem zamówienia są:

A. Rozbudowa zabezpieczeń logicznych (firewall, systemy IDS, IPS)

Warunki realizacji zamówienia:
Zakup nowego, nieregenerowanego urządzenia Unified Threat Managament (UTM) dla sieci komputerowej około 20 komputerów z gwarancją i licencjami na co najmniej 12 miesięcy. Przez ten okres licencje muszą umożliwiać dostęp do aktualizacji oprogramowania oraz wsparcie technicznego w trybie 24x7.

Minimalne parametry techniczne i wydajnościowe, które musi spełniać zamawiane urządzenie:

- Przepustowość firewall'a (Firewall Throughput): nie mniej niż 5 Gb/s dla pakietów 512 B
- Przepustowość/wydajność szyfrowania IPsec VPN (IPsec VPN Throughput): 4 Gb/s
- Przepustowość IPS (IPS Throughput): 1 Gb/s
- Przepustowość z włączonymi usługami firewall, IPS, kontrola aplikacji: 800 Mb/s
- Przepustowość z włączoną usługą antywirusa/ochrony przed zagrożeniami: 600 Mb/s
- Przepustowość SSL VPN (SSL VPN Throughput): 480 Mb/s
- Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 950 Mb/s
- Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu HTTPS – minimum 300 Mb/s
- Opóźnienie firewall'a (Firewall Latency): 3 µs
- Jednoczesna połączenia (sesje równoległe) Firewall'a: 700000
- Nowe połączenia (sesje) Firewall'a na 1 sekundę: 35000
- Porty interfejsów: 5 szt. Gigabit Ethernet RJ45
- Port konsoli: RJ45, na tej samej ścianie urządzenia co porty interfejsów
- Wysokość urządzenia: maksymalnie 1 U

Wymagania Ogólne UTM
Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu,

Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.

System musi wspierać IPv4 oraz IPv6 w zakresie:

- Firewall,
- Ochrony w warstwie aplikacji,
- Protokołów routingu dynamicznego.

Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.

Interfejsy, USB, Zasilanie

System realizujący funkcję Firewall musi dysponować minimum 5 portami Gigabit Ethernet RJ-45.

1. System Firewall musi posiadać wbudowane gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
2. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
3. System musi być wyposażony w zasilanie AC dostosowane do sieci energetycznej działającej w Polsce.

Funkcje Systemu Bezpieczeństwa

W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa.
2. Kontrola aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware - co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2

tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.

11. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.
12. Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system

Polityki, Firewall

1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
   - Translację jeden do jeden oraz jeden do wielu.
   - Dedykowany application level gateway) dla protokołu SIP.
3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP, nazwy domenowe, hash'e złośliwych plików.
5. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.
   - Amazon Web Services (AWS),
   - Microsoft Azure,
   - Google Cloud Platform (GCP),
   - OpenStack,
   - VMware NSX.

Połączenia VPN

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
   - Wsparcie dla IKE v1 oraz v2.
   - Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy typu galois/counter mode.
   - Obsługa protokołu Diffie-Hellman grup 19 i 20.
   - Wsparcie dla pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
   - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
   - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
   - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
   - Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
   - Mechanizm Split tunneling dla połączeń Client-to-Site.

2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
   - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
   - Pracę w trybie Tunnel z możliwością włączenia funkcji Split tunneling przy zastosowaniu dedykowanego klienta.
   - Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

Routing i obsługa łączy WAN

W zakresie routingu rozwiązanie powinno zapewniać obsługę:
- Routingu statycznego.
- Policy Based Routingu.
- Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

Funkcje SD-WAN

1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.

Zarządzanie pasmem

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, rar.
3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
6. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.

Ochrona przed atakami

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

Kontrola aplikacji

1. Funkcja Kontroli aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

Kontrola WWW

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.
6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.

7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii URL lub wskazanych URL - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
   - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
   - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
   - Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

Logowanie

1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze producenta.
2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów,

zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
4. Musi istnieć możliwość logowania do serwera SYSLOG.

Certyfikaty
Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje: ICSA lub EAL4 dla funkcji Firewall.

Serwisy i licencje
W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować funkcje: Kontrola aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen oraz chmurowy system logowania.

Gwarancja oraz wsparcie
Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 12 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.

Urządzenie w żadnym zakresie technologicznym nie może się opierać na rozwiązaniach sprzętowych lub programowych będących w konflikcie z ustawą z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego.

B. Szkolenie online dla pracowników urzędu w zakresie obsługi zakupionego sprzętu i oprogramowania

Warunki realizacji zamówienia:
1. Szkolenie musi się odbyć w formie online lub w siedzibie Zamawiającego w wymiarze czasowym minimum 8 godzin (po 60 minut każda).
2. Szkolenie poza częścią teoretyczną powinno zawierać część warsztatową, w której każdy z uczestników szkolenia posiada swój osobny dostęp i możliwość szkolenia na oprogramowaniu urządzenia FortiGate.
3. Liczba pracowników Zamawiającego biorących udział w szkoleniu: 2.
4. Szkolenie musi zostać przeprowadzone przez osobę posiadającą jeden z certyfikatów wskazanych w rozdziale VII, ustęp 1, litera c.
5. Szkolenie musi się zakończyć wydaniem dla szkolonych osób imiennego certyfikatu ukończenia szkolenia.

6. Szkolenie musi obejmować minimum poniższe zagadnienia odnoszące się do urządzeń Fortinet FortiGate (w szczególności modele z serii E i F od 40E/F do 200E/F) i oprogramowania producenta do zarządzania tymi urządzeniami:
   a) wstępna konfiguracja urządzenia FortiGate (konfiguracja sieci, routingu; tryby pracy NAT/Transparent; Administracja urządzeniem przez interfejs WWW i CLI; dashboard i moduły systemu), omówienie budowy urządzeń;
   b) polityki firewall (modyfikacja i tworzenie obiektów dla reguł firewall, translacja adresów NAT i Virtual IP);
   c) obsługa systemu (konta użytkowników i profile dostępu, aktualizacja firmware, tworzenie backupu konfiguracji i jej odtwarzanie);
   d) konfiguracja funkcji ochronnych (profile bezpieczeństwa, antywirus, filtrowanie SPAM, IPS / DoS Policy, kontrola ruchu WWW, blokowanie URL, DNS Filter, kontrola aplikacji, reputacja klienta, Data Leakage Prevention);
   e) optymalizacja ruchu sieciowego (kształtowanie pasma);
   f) logowanie i alerty (konfiguracja, FortiCloud, sposoby logowania);
   g) konfiguracja połączeń SSL VPN;
   h) inspekcja ruchu SSL.

C. Długookresowe utrzymanie logów z urządzenia UTM w chmurze

Warunki realizacji zamówienia:

1. Przedmiotem zamówienia jest zakup usługi rocznego utrzymanie logów w chmurze z posiadanego przez Zamawiającego urządzenia UTM – FortiGate Cloud Management, Analysis and 1 Year Log Retention.
2. Podstawowe wymagania:
   a) Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze producenta urządzenia UTM, z funkcją rocznej retencji logów;
   b) Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa urządzenia UTM. Usługa musi zapewniać przekazywanie logów o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu;
   c) Musi istnieć możliwość logowania do serwera SYSLOG;
   d) Usługa ma umożliwiać przechowywanie i analizę logów w usłudze chmurowej, przez okres 12 miesięcy;
   e) Zamawiana usługa SaaS musi być realizowana na serwerach producenta urządzenia UTM;
   f) Dostarczany dostęp do usługi musi być w pełni funkcjonalny i nieobciążony prawami osób trzecich;
   g) Wykonawca musi skonfigurować w porozumieniu z Zamawiającym jego urządzenie UTM, tak by zamawiana usługa prawidłowo funkcjonowała.

D. Licencje oprogramowania do zintegrowanego zarządzania urządzeniami w sieci i bezpieczeństwa IT

Warunki realizacji zamówienia:

1. Przedmiotem zamówienia jest zakup komercyjnych licencji dla dodatkowych Agentów posiadanego przez Zamawiającego oprogramowania Axence nVision.
2. Podstawowe wymagania:
   a) Właścicielem licencji musi być Zamawiający - Urząd Miasta i Gminy Murowana Goślina.
   b) Licencje mają umożliwiać Zamawiającemu korzystanie ze wszystkich posiadanych przez Zamawiającego modułów oprogramowania Axence nVision.
   c) Rozszerzenie licencji ma obejmować 10 Agentów Axence nVision, które będą zainstalowane na stacjach roboczych (komputerach pracowników Zamawiającego).
   d) Zamawiane licencje muszą być typu komercyjnego, bezterminowe. Nie mogą to być licencje testowe lub czasowe.
   e) Zamawiane licencje dla Agentów muszą być dodane do internetowego Konta Axence Zamawiającego i być dostępne bez dodatkowych działań Zamawiającego w konsoli administracyjnej na serwerze Axence nVision zainstalowanej na serwerze w sieci LAN Zamawiającego.
   f) Zamawiający informuje, że posiada wykupione wsparcie techniczne nVision (umowa serwisowa), nie krótsze niż do końca 2023 roku.

E. Moduł oprogramowania do zintegrowanego zarządzania urządzeniami w sieci i bezpieczeństwa IT

Warunki realizacji zamówienia:

1. Przedmiotem zamówienia jest zakup komercyjnej licencji na moduł DataGuard dla posiadanego przez Ośrodek Pomocy Społecznej w Murowanej Goślinie oprogramowania Axence nVision.
2. Podstawowe wymagania:
   a) Właścicielem licencji musi być Zamawiający – Ośrodek Pomocy Społecznej w Murowanej Goślinie.
   b) Licencja ma umożliwiać korzystanie z dodatkowego modułu DataGuard oprogramowania Axence nVision.
   c) Zamawiana licencja musi być typu komercyjnego, bezterminowa. Nie może to być licencja testowa lub czasowa.
   d) Licencja na zamawiany moduł musi być dodana do internetowego Konta Axence właściciela licencji i być dostępna w konsoli administracyjnej na serwerze Axence nVision zainstalowanej na serwerze w sieci LAN właściciela licencji.
   e) Zamawiający informuje, że właściciel licencji posiada wykupione wsparcie techniczne nVision (umowa serwisowa), nie krótsze niż do końca października 2023 roku.

VI. Termin i miejsce wykonania zamówienia oraz warunki płatności:

1. Wykonawca wykona przedmiot zamówienia w terminie do **23.06.2023 r.**
2. Miejscem realizacji zamówienia będzie Urząd Miasta i Gminy w Murowanej Goślinie.
3. Potwierdzeniem wykonania przedmiotu zamówienia będzie podpisany przez strony Protokół zdawczo-odbiorczy prawidłowo wykonanego przedmiotu zamówienia, stwierdzający kompletność i zgodność wykonania przedmiotu zamówienia określonego w opisie przedmiotu zamówienia znajdującym się w rozdziale V.
4. Zapłata za wykonany przedmiot zamówienia nastąpi na podstawie faktury VAT wystawionej przez Wykonawcę, w terminie 14 dni od dnia jej doręczenia Zamawiającemu.
5. Wynagrodzenie ma charakter ryczałtowy i obejmuje wszelkie czynności niezbędne do wykonania zamówienia.

VII. Warunki udziału w postępowaniu:

1. O udzielenie zamówienia mogą ubiegać się Wykonawcy:
   a) osoby fizyczne, osoby prawne i jednostki organizacyjne nie posiadające osobowości prawnej, wobec których nie zachodzą podstawy wykluczenia określone w Rozdziale XII niniejszego Zapytania ofertowego;
   b) którzy posiadają uprawnienia do wykonywania określonej działalności lub czynności, jeżeli przepisy prawa nakładają obowiązek posiadania takich uprawnień.
   c) Zamawiający wskazuje certyfikaty uprawniające trenera do prowadzenia zamawianego szkolenia (opisanego w rozdziale V):
   – Fortinet NSE 7 – Network Security Architect
   lub
   – Fortinet NSE 8 – Network Security Expert
   W ofercie należy wskazać imię i nazwisko osoby posiadającej odpowiednie uprawnienia (jeden z powyższych certyfikatów), która będzie prowadziła szkolenie. Dla tej osoby należy wskazać, który z ważnych certyfikatów posiada.
2. Ocena spełnienia warunków udziału w postępowaniu przeprowadzona zostanie w oparciu o przedłożone przez Wykonawcę Oświadczenia wyodrębnione w Formularzu ofertowym stanowiącym Załącznik nr 1 do zapytania ofertowego oraz wymagane w ust. 1 niniejszego rozdziału dokumenty.
3. W toku badania i oceny ofert Zamawiający może żądać od Wykonawców dodatkowych dokumentów potwierdzających spełnienie powyższych warunków udziału w postępowaniu.
4. Wykonawcy, którzy nie wykażą spełnienia warunków udziału w postępowaniu, podlegać będą wykluczeniu z udziału w postępowaniu. Ofertę Wykonawcy wykluczonego uznaje się za odrzuconą.
5. Złożenie oferty jest jednoznaczne z zapoznaniem się z treścią zapytania ofertowego i akceptacją warunków realizacji zamówienia określonych w niniejszym Zapytaniu ofertowym.

6. Zamawiający informuje, że niniejsze Zapytanie ofertowe nie stanowi oferty zawarcia umowy, ani też oferty prowadzenia negocjacji w tym celu i jest skierowane do wielu adresatów.

VIII. Dodatkowe warunki:

1. Zamawiający zastrzega sobie prawo zmiany treści niniejszego zapytania przed terminem składania ofert, a w przypadku, gdy zmiany będą miały istotny wpływ na treść składanych ofert wydłuży termin na ich składanie.
2. Zamawiający zastrzega sobie prawo do poprawienia w tekście przysłanej oferty oczywistych omyłek pisarskich lub rachunkowych, niezwłocznie zawiadamiając o tym danego Wykonawcę.
3. Zamawiający zastrzega sobie prawo do unieważnienia postępowania o udzielenie zamówienia na każdym etapie jego realizacji bez podania przyczyny oraz w szczególności w przypadku gdy wystąpiła istotna zmiana okoliczności powodująca, że wykonanie zamówienia nie leży w interesie Zamawiającego, czego nie można było wcześniej przewidzieć, gdy postępowanie obarczone jest wadą, która może mieć wpływ na wynik postępowania lub gdy zaistnieją inne uzasadnione okoliczności.
4. Zamawiający może odstąpić od podpisania umowy z przyczyny powstania nowych, uniemożliwiających podpisanie umowy okoliczności.
5. W każdym przypadku skorzystania przez Zamawiającego z uprawnień opisanych powyżej nie będzie przysługiwało oferentom żadne roszczenie wobec Zamawiającego, a w szczególności roszczenie o zawarcie umowy lub zwrot kosztów uczestnictwa w postępowaniu.

IX. Zawarcie umowy po wyborze najkorzystniejszej oferty i warunki zmiany umowy.

1. Niezwłocznie po wyborze najkorzystniejszej oferty Zamawiający zawiadamia Wykonawców, którzy złożyli oferty o wyborze najkorzystniejszej oferty, podając nazwę (firmę), siedzibę i adres Wykonawcy, którego ofertę wybrano, uzasadnienie jej wyboru, a także nazwy (firmy), siedziby i adresy Wykonawców, którzy złożyli oferty oraz punktację przyznaną ofertom a także informację o Wykonawcach, których oferty zostały odrzucone, podając uzasadnienie.
2. Niezwłocznie po wyborze najkorzystniejszej oferty Zamawiający zamieszcza informacje, o których mowa w ust. 1 powyżej na stronie internetowej prowadzonego postępowania: https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl
3. Zamawiający zawiera umowę w sprawie zamówienia publicznego z Wykonawcą, którego oferta:
   a) spełnia wymagania określone przez Zamawiającego;
   b) została uznana za najkorzystniejszą w oparciu o kryteria oceny ofert.
4. Zamawiający poinformuje Wykonawcę, którego oferta została wybrana jako najkorzystniejsza o miejscu i terminie zawarcia umowy.
5. Wszelkie zmiany Umowy wymagają formy pisemnej pod rygorem nieważności.
6. W uzasadnionych przypadkach Zamawiający dopuszcza możliwość zmiany terminu realizacji zamówienia oraz osób dedykowanych do realizacji zamówienia, na etapie

realizacji umowy, o ile Wykonawca przedstawi osoby, które spełniają wymogi określone w zapytaniu ofertowym i zostaną zaakceptowane przez Zamawiającego.

7. W sytuacji, w której wybrany Wykonawca odstąpi od podpisania umowy lub Zamawiający albo Wykonawca odstąpią od zawartej umowy, Zamawiający może podpisać umowę z kolejnym Wykonawcą, który w postępowaniu o udzielenie zamówienia uzyskał kolejną najwyższą liczbę punktów. Zawarta z takim Wykonawcą umowa może zawierać zmiany w stosunku do treści Zapytania Ofertowego oraz oferty Wykonawcy.
8. W sprawach nieuregulowanych Umową zastosowanie mają przepisy prawa powszechnie obowiązującego, a w szczególności Kodeksu cywilnego.

X. Kryteria oceny ofert i sposób przyznawania punktacji

1. Oferent musi spełnić wszystkie kryteria formalne przystąpienia do postępowania, w tym złożenie oferty wraz z wymaganymi załącznikami na kompletnych formularzach załączonych do niniejszego zapytania.
2. Wybór Wykonawcy dokonany zostanie na podstawie uzyskania najwyższej liczby punktów w kryterium cena za realizację zamówienia. Taka oferta uznana zostanie za ofertę najkorzystniejszą:
   Kryterium: Cena brutto – waga 100%
3. Sposób oceny oferty dokonany zostanie na podstawie wzoru:
   $C = C_N/C_B \times 100$
   gdzie C - ilość punktów oferty rozpatrywanej
   C_N- Cena najniższej oferty wśród ofert nieodrzuconych
   C_B- cena oferty rozpatrywanej
   100 % = 100 punktów
   Maksymalna liczba punktów do uzyskania wynosi 100.
4. W przypadku, gdy dwie lub więcej ofert uzyska tę samą liczbę punktów, Zamawiający zwróci się do Wykonawców o przedłożenie oferty dodatkowej w terminie określonym przez Zamawiającego. Oferty dodatkowe muszą zawierać nową cenę i jednocześnie nie mogą opiewać na cenę wyższą od pierwotnie zaoferowanej.
5. Cena oferty wskazana w Formularzu ofertowym musi uwzględniać wszystkie wymagania Zamawiającego oraz obejmować wszelkie koszty, jakie poniesie Wykonawca z tytułu należytej i zgodnej z Zapytaniem ofertowym realizacji zamówienia.
6. Cena oferty powinna być wyrażona w złotych polskich (PLN) z dokładnością do dwóch miejsc po przecinku cyfrowo i słownie. W ofercie Wykonawca określi cenę brutto i netto za realizację całego zamówienia.
7. Cena ofertowa musi być jednoznaczna i ostateczna. Zostanie wprowadzona do umowy zawartej z Wykonawcą jako obowiązujące strony umowy wynagrodzenie.
8. Cena oferty powinna zawierać należny podatek VAT. Ustalenie prawidłowej stawki VAT należy do obowiązków Wykonawcy, zgodnie z przepisami ustawy z dnia 11 marca 2004 roku o podatku od towarów i usług.
   Zamawiający informuje, że szkolenie wskazane rozdziale V (opis przedmiotu zamówienia) jest finansowane w minimum 70% ze środków publicznych.

XI. Wykluczenia z postępowania

1. Wykluczeniu z postępowania podlega Wykonawca który jest powiązany z Zamawiającym osobowo lub kapitałowo, tzn. zachodzą wzajemne powiązania pomiędzy Zamawiającym lub osobami upoważnionymi do zaciągania zobowiązań w imieniu Zamawiającego lub osobami wykonującymi w imieniu Zamawiającego czynności związane z przeprowadzeniem procedury wyboru Wykonawcy a Wykonawcami, polegające w szczególności na:
   a) uczestniczeniu w spółce jako wspólnik spółki cywilnej lub spółki osobowej,
   b) posiadaniu co najmniej 10% udziałów lub akcji, o ile niższy próg nie wynika z przepisów prawa lub nie został określony przez Instytucję Zarządzającą projektem „Cyfrowa Gmina" w wytycznych programowych,
   c) pełnieniu funkcji członka organu nadzorczego lub zarządzającego, prokurenta, pełnomocnika,
   d) pozostawaniu w takim stosunku prawnym lub faktycznym, który może budzić uzasadnione wątpliwości, co do bezstronności w wyborze Wykonawcy, w szczególności pozostawaniu w związku małżeńskim, w stosunku pokrewieństwa lub powinowactwa w linii prostej, pokrewieństwa lub powinowactwa w linii bocznej do drugiego stopnia lub w stosunku przysposobienia, opieki lub kurateli;

   Wykonawca składa oświadczenie o braku powiązań osobowych i kapitałowych, wyodrębnione w Formularzu ofertowym, stanowiącym Załącznik nr 1 do zapytania ofertowego.
2. W udziale w postępowaniu nie mogą brać udziału także Oferenci, którzy w ciągu ostatnich 3 lat przed wszczęciem postępowania wyrządzili Zamawiającemu szkodę przez to że nie wykonali lub nienależycie wykonali zobowiązanie wobec Zamawiającego, chyba że było to następstwem okoliczności, za które Oferent nie ponosił odpowiedzialności.
3. O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy nie podlegają wykluczeniu na podstawie art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspierania agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego.

XII. Informacja o przetwarzaniu danych osobowych kontrahentów

Zgodnie z Rozporządzeniem 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, dalej zwane „RODO") (Dz. Urz. UE L 119 z 4 maja 2016, str. 1 z późn. zm) informujemy, że:

1. Administratorem danych osobowych jest Burmistrz Miasta i Gminy Murowana Goślina, z siedzibą w (62-095) Murowanej Goślinie, plac Powstańców Wielkopolskich 9;
2. Dane kontaktowe Inspektora Ochrony Danych: Urząd Miasta i Gminy, plac Powstańców Wielkopolskich 9, 62-095 Murowana Goślina; e-mail: inspektorochronydanych@murowana-goslina.pl;

3. Dane osobowe są przetwarzane w celu przeprowadzenia postępowania o udzielenie zamówienia publicznego, zawarcia i realizacji umowy o której mowa w rozdziale IX oraz dopełnienie obowiązków określonych w przepisach prawa (m.in. ustawa o finansach publicznych, realizacja obowiązków księgowych, podatkowych) oraz ustalenie i dochodzenie roszczeń lub obrona w razie zaistnienia ewentualnych roszczeń;
4. Podstawą prawną przetwarzania danych jest art. 6 ust. 1 lit. b, c oraz f RODO;
5. Podanie danych osobowych jest wymogiem ustawowym określonym w przepisach ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego;
6. Dane osobowe będą przechowywane przez okres niezbędny do realizacji celu, a po tym czasie przez okres zgodny z ustawą z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach lub innymi szczegółowymi przepisami prawa;
7. Odbiorcami danych osobowych w projekcie „Cyfrowa Gmina" będą Centrum Projektów Polska Cyfrowa oraz Minister Funduszy i Polityki Regionalnej.
   Odbiorcami danych osobowych mogą być organy władzy publicznej, podmioty wykonujące zadania publiczne lub działające na zlecenie organów władzy publicznej, w zakresie i w celach, które wynikają z przepisów powszechnie obowiązującego prawa. Odrębną kategorią odbiorców są podmioty uprawnione do obsługi doręczeń oraz podmioty dostarczające Administratorowi rozwiązania teleinformatyczne;
8. Informujemy, że dane osobowe nie będą przekazywane do państw trzecich, ani udostępniane organizacjom międzynarodowym;
9. Na podstawie podanych danych nie nastąpi zautomatyzowane podejmowanie decyzji, w tym profilowanie;
10. Informujemy o prawie dostępu do treści swoich danych osobowych oraz z zastrzeżeniem przepisów prawa do ich sprostowania (wyjaśnienie: skorzystanie z prawa do sprostowania nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia publicznego, ani zmianą postanowień umowy w zakresie niezgodnym z ustawą Prawo zamówień publicznych), ograniczenia przetwarzania, wniesienia sprzeciwu wobec przetwarzania;
11. Ma Pani/Pan prawo wniesienia skargi do organu nadzorczego w zakresie ochrony danych osobowych, jeśli stwierdzi Pani/Pan, że przetwarzanie danych osobowych narusza przepisy prawa.

XIII. Załączniki

1. Załącznik nr 1 – Formularz ofertowy.

Signed by / Podpisano przez:
Adrianna Urbaniak
Date / Data: 2023-05-18 14:18

ZATWIERDZAM:

Adrianna Urbaniak
/podpisano kwalifikowanym podpisem elektronicznym/