

Opis Przedmiotu Zamówienia

Dostawa i wdrożenie systemów cyberbezpieczeństwa NAC (Network Access Control) w związku z realizacją przez Gminę Starachowice zadania w ramach realizacji grantu pn. „Cyberbezpieczny Samorząd”.

Rozdział I. Założenia początkowe oraz wymagania ogólne

I.1 Wprowadzenie

1. Przedmiot zamówienia jest realizowany w ramach grantu pn. „Cyberbezpieczny Samorząd” współfinansowanego ze środków Unii Europejskiej: Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2. - Wzmocnienie krajowego systemu cyberbezpieczeństwa, Fundusze Europejskie na Rozwój Cyfrowy 2021-2027.
2. Realizacja grantu ma na celu podniesienie cyberbezpieczeństwa oraz zdolności do skutecznego zapobiegania incydentom bezpieczeństwa teleinformatycznego w Gminie Starachowice

I.2 Ogólny opis przedmiotu zamówienia system NAC

1. Przedmiot zamówienia obejmuje: dostawę i wdrożenie systemu NAC (Network Access Control)
2. Przedmiot zamówienia musi być dostarczony, wdrożony i zainstalowany w całości w siedzibie Zamawiającego we wskazanym miejscu.
3. Wszystkie dostarczane Produkty (rozumiane jako elementarny efekt działań/prac/dostaw objętych całym zakresem przedmiotu zamówienia wykonywanych przez Wykonawcę podczas realizacji Umowy w poszczególnych Etapach) oraz Komponenty (rozumiane jako integralna część dostawy i wdrożenia przedmiotu zamówienia, składający się przynajmniej z jednego Produktu lub wielu Produktów powiązanych ze sobą merytorycznie) podlegają usługom projektowania, dostaw, instalacji, konfiguracji i wdrożenia.
4. Usługi projektowania, instalacji, konfiguracji i wdrożenia Wykonawca musi przeprowadzić zgodnie z postanowieniami niniejszego OPZ w uzgodnieniu z Zamawiającym, zgodnie z obowiązującymi przepisami, zasadami wykonywania projektów teleinformatycznych oraz najlepszymi praktykami w ich realizacji.
5. Wykonawca jest zobowiązany do realizacji Przedmiotu Zamówienia zgodnie z zasadami i wytycznymi Zamawiającego, zapisami OPZ oraz Umowy.
6. Ilekroć w niniejszym OPZ Zamawiający użył w opisie oznaczeń norm, aprobat, specyfikacji technicznych i systemów odniesienia należy je rozumieć jako przykładowe. Zamawiający dopuszcza rozwiązanie równoważne. Jeżeli zapisy zawarte w OPZ wskazywałyby w odniesieniu do rozwiązań, materiałów lub urządzeń znaki towarowe lub pochodzenie Zamawiający dopuszcza składanie ofert na rozwiązania równoważne. Wszelkie „produkty” pochodzące od konkretnych producentów określają minimalne parametry jakościowe i cechy użytkowe, jakim musi odpowiadać produkt, aby spełnić wymagania stawiane przez Zamawiającego stanowią wyłącznie wzorzec jakościowy przedmiotu zamówienia. Poprzez zapis dot. minimalnych wymagań parametrów

jakościowych Zamawiający rozumie wymagania materiałów, sprzętu i urządzeń zawarte w ogólnie dostępnych źródłach, katalogach, stronach internetowych producentów. Operowanie przykładowymi nazwami producenta ma jedynie na celu doprecyzowanie poziomu oczekiwań Zamawiającego w stosunku do określonego rozwiązania. Tak więc posługiwanie się nazwami producentów /produktów/ ma wyłącznie charakter przykładowy. Zamawiający, przy opisie przedmiotu zamówienia, wskazując oznaczenie konkretnego producenta (dostawcy) lub konkretny produkt, dopuszcza jednocześnie produkty równoważne o parametrach jakościowych i cechach użytkowych, co najmniej na poziomie parametrów wskazanego produktu, uznając tym samym każdy produkt o wskazanych parametrach lub lepszych. W takiej sytuacji Zamawiający wymaga złożenia stosownych dokumentów, wykazujących spełnienie przez produkty równoważne ww. parametrów i cech.

I.3 Termin realizacji Przedmiotu Zamówienia

Zamawiający wymaga wykonania przedmiotu zamówienia w terminie do 4 miesięcy od daty zawarcia umowy.

I.3.1 Przygotowanie Dokumentacji

1. W ramach realizowanych prac Wykonawca musi opracować dla Zamawiającego Dokumentację Przedmiotu Zamówienia (zwaną dalej Dokumentacją), która składa się z nw. zakresów:

- 1) Harmonogram Wdrożenia,
- 2) Dokumentacja Analizy Przedwdrożeniowej (DAP),
- 3) Testy
- 4) Dokumentacja Powykonawcza.

I.3.2 Dodatkowe zobowiązania Wykonawcy

1. Wykonanie przedmiotu zamówienia z efektywnością oraz zgodnie z praktyką i wiedzą zawodową.
2. Dokonanie z Zamawiającym wszelkich koniecznych ustaleń mogących wpływać na zakres i sposób realizacji Przedmiotu Zamówienia oraz ciągła współpraca z Zamawiającymi na każdym etapie realizacji.
3. Stosowanie się do wytycznych i polityk bezpieczeństwa informacji obowiązujących u Zamawiającego.
4. Udzielanie na każde żądanie Zamawiającego pełnej informacji na temat stanu realizacji Przedmiotu Zamówienia.
5. Współdziałanie z osobami wskazanymi przez Zamawiającego.

Rozdział II. Szczegółowy opis przedmiotu zamówienia

II. Systemu NAC (Network Access Control)

Zamawiający wymaga dostarczenia licencji wieczystej ze wsparciem technicznym i dostępem do najnowszych wersji i poprawek przez okres min. 12 miesięcy. Zamawiający wymaga wdrożenia oferowanego systemu w taki sposób, aby możliwe było używanie systemu z wymaganą poniżej funkcjonalnością. W ramach wdrożenia Wykonawca przestawi Zamawiającemu wytyczne do skonfigurowania urządzeń sieciowych. Na bazie przedstawionych wytycznych Zamawiający przeprowadzi rekonfigurację wszystkich urządzeń sieciowych (około 80 przełączników sieciowych) do prawidłowej współpracy z wdrażanym systemem.

Wykonawca przeprowadzi analizę posiadanego przez Zamawiającego środowiska Active Directory oraz działającej sieci LAN/MAN. W oparciu o analizę przygotowany zostanie projekt wdrożenia polityk uwierzytelniających, które zostaną zaimplementowane w dostarczonym systemie. Zostaną przygotowane odpowiednie polityki GPO, na podstawie których zostanie uruchomione uwierzytelnianie w oparciu o protokół 802.1X na urządzeniach końcowych a w przypadku urządzeń nie obsługujących wymienionego protokołu zostaną stworzone polityki uwierzytelniające w oparciu o profilowanie i adres MAC.

Zamawiający wymaga pełnego wdrożenia dostarczanego systemu na zasobach Zamawiającego. Po zakończeniu wdrożenia, Wykonawca przeprowadzi szkolenie dla administratorów w zakresie co najmniej niezbędnym do prawidłowego użytkowania, konfiguracji i zarządzania problemami występującymi we wdrożonym systemie. Szkolenie musi być przeprowadzone w języku polskim, w formie zrozumiałej dla administratorów. Przekazane materiały szkoleniowe muszą być sporządzone w języku polskim. Szczegółowy zakres, plan wdrożenia i szkolenia zostanie określony podczas analizy przedwdrożeńiowej.

Wymagania funkcjonalne:

- 1) Musi być systemem współpracującym z urządzeniami wielu producentów (tzw. multi vendor)
- 2) Musi obsługiwać minimum 1 000 urządzeń klienckich (jednoczesnych unikatowych uwierzytelnień do sieci w ciągu dnia, w tym gości) oraz zapewnić skalowalność do co najmniej 2500 jednoczesnych unikatowych autoryzacji do sieci poprzez rozbudowę oferowanego rozwiązania. Licencje mają dotyczyć aktualnie podłączonych urządzeń i muszą być zwalniane po rozłączeniu urządzenia
- 3) System musi pracować w trybie HA – klaster dwóch maszyn wirtualnych pracujących w trybie wysokiej dostępności (redundancja).
- 4) Interfejs graficzny musi być dostępny w języku polskim. Zamawiający oczekuje, że interfejs graficzny będzie miał możliwość zmiany języka na inne języki co najmniej na język angielski.
- 5) Musi posiadać wbudowany serwer Radius
- 6) Musi posiadać wbudowany serwer TACACS +
- 7) Musi wspierać RADIUS VSA co najmniej, w tym:
 - a. Cisco Systems
 - b. Fortinet
 - c. Microsoft
 - d. Aruba Networks
 - e. Huawei Networks
 - f. Extreme Networks
 - g. DCN
 - h. Watchguard
 - i. Dell
 - j. TP-Link

- k. Mikrotik
 - l. Unifi
- 8) System musi posiadać możliwość przesyłania atrybutów VSA do kontrolera sieci bezprzewodowej takich jak rola użytkownika oraz VLAN bez potrzeby dokonywania dodatkowej konfiguracji kontrolera.
- 9) System musi posiadać możliwość otrzymywania od kontrolera sieci bezprzewodowej dodatkowych informacji o autoryzacji użytkownika między innymi takich jak SSID, grupa punktów dostępowych, IP punktu dostępowego.
- 10) Wszystkie wymagane licencje muszą działać permanentnie (dożywotnio), nie dopuszcza się licencji czasowych.
- 11) Musi posiadać wbudowaną bazę użytkowników oraz móc integrować się z następującymi bazami danych
- a. Microsoft Active Directory
 - b. Radius
 - c. Kerberos
 - d. LDAP
 - e. ODBC
 - f. Współpraca z serwerami tokenów
 - g. Microsoft Azure Active Directory
 - h. Google G Suite
- 12) Musi obsługiwać metody profilowania do wykrywania typu urządzenia, systemu operacyjnego co najmniej poprzez:
- a. DHCP
 - b. SNMP
 - c. Vendor OUI
 - d. TCP
 - e. Active Directory
 - f. Cisco device sensor
 - g. CDP/LLDP
 - h. DNS
 - i. Radius
 - j. WMI
 - k. WinRM
 - l. ONVIF
 - m. HTTP, HTTPS
 - n. MDM
- 13) Wspierać min poniższe protokoły:
- a. Radius, Radius CoA, TACACS +, web authentication, SAML v2.0
 - b. EAP-FAST (EAP-MSCHAPv2, EAP-GTC, EAP-TLS)
 - c. PEAP (EAP-MSCHAPv2, EAP-GTC, EAP-TLS,)
 - d. TTLS (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-MD5, PAP, CHAP)
 - e. EAP-TLS
 - f. 802.1X-2010, 802.1X-2020
 - g. PAP, CHAP, MSCHAPv1 i v2, EAP-MD5
 - h. NAC, Microsoft NAP
 - i. Windows machine authentication
 - j. MAC Auth
 - k. OCSP (Online Certificate Status Protocol)

- I. CEF (Common Event Format),
 - m. TLS 1.2
- 14) Funkcja integracji z systemem monitorowania sieci w celu ułatwienia diagnozowania problemów z klientami (zamawiający posiada system Nagios).
- 15) Maszyna wirtualna musi mieć możliwość uruchomienia na platformach witalizacyjnych:
- a. Co najmniej ESXi 7.0
 - b. Co najmniej Windows 2016 i 2019 z Hyper-V
 - c. Co najmniej KVM on CentOS 7.7. Ubuntu 18.04, and Ubuntu 20.04
 - d. Co najmniej Amazon AWS (EC2)
 - e. Co najmniej Microsoft Azure
- 16) Posiadać moduł odpowiedzialny za Dostęp Gościnny. Obsługa użytkowników typu Gość w liczbie co najmniej równej minimalnej liczbie obsługiwanych urządzeń klienckich (1 000). Jeżeli moduł ten wymaga dodatkowych licencji, muszą być one dostarczone.
- 17) System obsługi ruchu gościnnego musi spełniać poniższe funkcjonalności:
- Samodzielna rejestracja klientów gościnnych w oparciu o:
 - a. Adres e-mail
 - b. Numer telefonu (wiadomość SMS)
 - c. Dostęp sponsorowany (gość musi podać adres e-mail pracownika, na który jest wysłana prośba o autoryzację dostępu poprzez kliknięcie w znajdujący się w wiadomości link)
 - Logowanie w oparciu o portale społecznościowe
 - Funkcja integracji z systemami trzecimi poprzez API
 - Wsparcie dla tworzenia komercyjnych systemów HOT-SPOT wykorzystujących do płatności systemy płatności karta kredytową
 - Wbudowany system reklamowy umożliwiający integrację z zewnętrznymi serwisami umożliwiającymi w prosty sposób promowanie ofert promocyjnych, materiałów multimedialnych oraz aplikacji mobilnych.
 - Wspieranie rozwiązań mobilnych poprzez automatyczne skalowanie portalu gościnnego do rozmiarów urządzeń mobilnych.
 - Funkcja personalizacji strony gościnnej
 - Obsługa wielu wersji językowych (min. w języku polskim, angielskim, niemieckim, ukraińskim)
- 18) Posiadać moduł odpowiedzialny za obsługę urządzeń typu BYOD.
- Konfiguracja urządzeń ma odbywać się bez potrzeby angażowania pracowników działu IT
 - System musi wspierać obsługę następujących systemów operacyjnych
 - a. MS Windows
 - b. Mac OS X
 - c. iOS
 - d. Android
 - e. Chromebook
 - f. Ubuntu
- 19) Umożliwienie klientowi samo rejestracji oraz bezpiecznego skonfigurowania urządzenia do pracy w sieci
- 20) Automatyczna konfiguracja urządzeń do pracy w sieci przewodowej jak i bezprzewodowej
- 21) Użycie profilowania do identyfikacji rodzaju urządzenia, producenta oraz modelu.
- 22) Funkcja tworzenia unikalnych certyfikatów dla urządzeń.
- 23) Wbudowane CA na potrzeby generowania certyfikatów konfigurowanych urządzeń
- 24) Funkcja konfiguracji urządzeń bezprzewodowych w oparciu o jedną lub więcej sieci SSID

25) Posiadać moduł odpowiedzialny za kontrolę końcówek klienckich.

26) System kontroli końcówek klienckich musi mieć następujące funkcjonalności

- System musi wspierać następujące systemy operacyjne
 - a. Microsoft Windows 7 i nowsze (może być uruchomiony jako serwis)
 - b. Apple Mac OS X 10.7 i nowsze
 - c. Red HAT Enterprise Linux 7 i nowsze
 - d. CentOS 7 (Community Enterprise Operating System) i nowsze
 - e. SUSE linux 10.x i nowsze
- Funkcja kontroli stanu oprogramowania antywirusowego, anty-spyware, firewall
- Wyświetlanie informacji on-line o statusie monitorowanych końcówek
 - a. System powinien obsługiwać agenta co najmniej w formie stałej (Persistent Agent) lub agenta NAP

Rozdział III. Gwarancja

III.1 Okres gwarancji

1. Wykonawca w ramach realizacji przedmiotu zamówienia udzieli Zamawiającemu gwarancji jakości (dalej zwanej „gwarancją”) na okres 12 miesięcy.
2. Bieg terminów gwarancji określonych w ust. 1 będą rozpoczynać się z dniem podpisania Protokołu Końcowego bez uwag przez Zamawiającego.
3. Dostarczone system muszą być objęty gwarancją (serwisem) producenta przez okres wskazany w ust.1. Gwarancja musi zapewniać dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego w trybie 8x5 (w godz. 7-15 w dni robocze) na wszystkie elementy i licencje. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta lub jego autoryzowany serwis. Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego producenta.

III.2 Reżimy realizacji usług serwisowych

W okresie gwarancji Wykonawca będzie zobowiązany do nieodpłatnego usuwania Wad Przedmiotu Zamówienia rozumianych jako Awaria lub Usterka zgodnie z definicjami, jak poniżej:

- 1) **Awaria** - Kategoria Wady powodująca brak działania lub niepoprawne działanie Przedmiotu Zamówienia u Zamawiającego, uniemożliwiające jego użytkowanie. Sytuacja, w której Oprogramowanie w ogóle nie funkcjonuje lub nie jest możliwe realizowanie istotnych funkcjonalności Komponentów/Produktów Przedmiotu Zamówienia.
- 2) **Usterka** - Należy przez to rozumieć kategorię Wady oznaczającą funkcjonowanie niezgodne z opisem przedmiotu zamówienia, nie wpływającą istotnie na funkcjonowanie dostarczanego rozwiązania u Zamawiającego, utrudniającą pracę Użytkownikowi Zamawiającego.

KWALIFIKACJA ZGŁOSZENIA WADY	ROZWIĄZANIE ZASTĘPCZE	CZAS REAKCJI WYKONAWCY	CZAS NAPRAWY
AWARIA	niezwłocznie, nie później niż 12 godziny od czasu przyjęcia zgłoszenia	niezwłocznie, nie później niż 4 godziny od czasu przyjęcia zgłoszenia	niezwłocznie, nie później niż 4 dni robocze od czasu zgłoszenia
USTERKA	niezwłocznie, nie później niż 3 dni od czasu przyjęcia zgłoszenia	niezwłocznie, nie później niż 24 godziny od czasu przyjęcia zgłoszenia	niezwłocznie, nie później niż 10 dni roboczych od czasu zgłoszenia

1. Dopuszcza się zmianę kwalifikacji zgłoszenia Wady, po uprzedniej zgodzie Zamawiającego. Do czasu potwierdzenia zmiany kwalifikacji, uznaje się za obowiązującą kwalifikację pierwotną.
2. Czasy naprawy mogą być inne niż wskazane w powyższych tabelach, jeżeli Zamawiający zaakceptuje zmianę kwalifikacji zgłoszenia, o której mowa w punkcie 1).
3. W przypadku braku możliwości usunięcia Wady lub przedstawienia rozwiązania zastępczego zdalnie, Wykonawca zobowiązany jest do świadczenia gwarancji bezpośrednio w lokalizacji Zamawiającego.
4. Wszelkie zgłoszenia awarii i usterek realizowane będą poprzez system zgłoszeniowy Zamawiającego.

III.3 Informacje dodatkowe

Zamawiający informuje, że wszystkie urządzenia sieciowe na których realizowane będzie zamówienie objęte są gwarancją wynikającą z realizacji projektu pn.: „Zwiększenie dostępności e-usług dla miasta Starachowice”. W trakcie realizacji niniejszego zamówienia Wykonawca zobligowany będzie do dokonywania ustaleń technicznych z Gwarantem w taki sposób aby wdrożenie systemu NAC nie spowodowało utraty gwarancji uzyskanej w ramach poprzedniego projektu.

Rozdział IV – Warunki udziału w postępowaniu

O udzielenie zamówienia mogą ubiegać się wykonawcy, którzy:

1. Nie podlegają wykluczeniu
2. Spełniają warunki udziału w postępowaniu, dotyczące:
 - a. zdolności do występowania w obrocie gospodarczym, tj. wpisanie do jednego z rejestrów zawodowych lub handlowych: nie przewiduje się szczegółowego warunku w tym zakresie,
 - b. uprawnień do prowadzenia określonej działalności gospodarczej lub zawodowej, o ile wynika to z odrębnych przepisów, tj. nie przewiduje się szczegółowego warunku w tym zakresie,
3. zdolności technicznej lub zawodowej, tj. w okresie ostatnich 3 lat, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie, wykonał, a w przypadku świadczeń powtarzających

się lub ciągłych również wykonywanych, minimum dwie dostawy i wdrożenie systemu klasy NAC współpracujący z urządzeniami wielu producentów (tzw. multi vendor) i obsługujący min. 500 urządzeń klienckich, o wartości nie mniejszej niż 50 000 zł brutto każda.

4. dysponuje lub będzie dysponował osobami zdolnymi do realizacji przedmiotowego zamówienia, posiadającymi kwalifikacje niezbędne do wykonania zamówienia tj. minimum jedną osobą posiadającą ważny certyfikat techniczny potwierdzający kompetencje z zakresu wdrażania i konfigurowania oferowanego systemu NAC. Wszystkie osoby, o których mowa powyżej, powinny biegłe posługiwać się językiem polskim (w mowie i piśmie), w przeciwnym wypadku Wykonawca musi zapewnić tłumacza zapewniającego stałe tłumaczenie dla potrzeb realizacji zamówienia