WIM.DO.ZST.811.BEZ.03.2019 Szczytno, dn. 24-10-2019

ZAPYTANIE OFERTOWE

(niniejsze zapytanie nie stanowi zapytania ofertowego w rozumieniu ustawy pzp i stanowi rozeznanie rynku)

Zwracamy się z prośbą o przesłanie zgłoszenia na poniżej opisany przedmiot zamówienia. Usługodawcom, którzy się zgłoszą, zostanie udostępniona dokumentacja, po pisemnym zobowiązaniu do zachowania danych dotyczących systemów bezpieczeństwa wyłącznie do celu realizacji niniejszego zlecenia, w dniu 30.10.2019 w Porcie Lotniczym Olsztyn Mazury do wglądu. Dostarczenie oferty cenowej, po zapoznaniu się z dokumentacją, do dnia 4.11.2019.

Zakres prac:

Integracja dwóch systemów kontroli dostępu i systemów sygnalizacji włamania i napadu wraz z implementacją systemu rejestracji czasu pracy Portu Lotniczego Olsztyn Mazury

PRZEDMIOT POSTĘPOWANIA

Przedmiotem niniejszego postępowania jest wykonanie integracji dwóch systemów kontroli dostępu i systemów sygnalizacji włamania i napadu zainstalowanych na terminalu pasażerskim oraz części administracyjnej Portu Lotniczego „Olsztyn-Mazury", Szymany 150 na podstawie:

1. ustawy z dnia 22 sierpnia 1997 r. o ochronie osób i mienia,
2. PN-EN 50131 Systemy alarmowe - Systemy sygnalizacji włamania
3. PN-EN 60839 Systemy alarmowe i elektroniczne systemy zabezpieczeń

Systemy podlegające integracji:
- Kontrola dostępu KD-T wraz z SSWIN,
- Kontrola dostępu KD-A wraz zz SSWIN.

CPV:
80.20.Z usługi ochrony osób i mienia realizowanych w formie zabezpieczenia technicznego.
50324100-3 Usługi w zakresie konserwacji systemu,
35121700-5 Systemy alarmowe,
42961100-1 System kontroli dostępu.

OPIS PRZEDMIOTU ZAMÓWIENIA

Istniejący na obiekcie system kontroli dostępu (SKD) jak i również system sygnalizacji włamania i napadu (SSWiN) oparty jest o urządzenia i rozwiązania firmy UTC Fire & Security, serii ATS Advisor Master. ATS Master jest systemem w pełni elastycznym, spełniającym wymagania dla stopnia 3 wg PN-EN-50131, pozwalający na rozbudowę dostosowaną do potrzeb obiektu. Elementy adresowalne systemu komunikują się poprzez magistralę systemową, której konstrukcja pozwala na wysoką odporność na zakłócenia zewnętrzne, a jej topologia linii, dzięki zastosowaniu specjalnych urządzeń magistralnych może przyjmować konfigurację gwiazdy, łańcucha lub, co jest rzeczą najbardziej pożądaną, jeżeli chodzi o niezawodność systemów najwyższej klasy – pętli z dozorem jej uszkodzenia. Medium komunikacyjnym z kolei może być zarówno przewód symetryczny jak i kabel światłowodowy. Funkcjonalnie jednostka Master pełni rolę procesora zarówno dla systemu sygnalizacji włamania i napadu (SSWiN) oraz systemu kontroli dostępu (SKD). Jednocześnie te same elementy mogą być skonfigurowane do sterowania i detekcji w obydwu systemach, które są ze sobą zintegrowane.

W istniejącym systemie ATS Master do komunikacji z aplikacją nadrzędną służy interfejs IP pozwalający dołączyć centrale do sieci Ethernet. Dzięki szyfrowaniu danych zapewnione jest maksymalne bezpieczeństwo pracy. Interfejs służy także do uzyskania zdalnego dostępu do zintegrowanego systemu SSWiN oraz kontroli dostępu przez aplikacje zarządzające. Stosowane są też różne algorytmy szyfrowania danych, w tym AES 128-bit.

Obecnie funkcjonujące na obiekcie centrale, należy zastąpić 4 nowymi centralami, pochodzącymi z oferty producenta obecnego sprzętu, z zastrzeżeniem, że nowe centrale, jako urządzenia systemowe wykorzystywać będą istniejące kontrolery, czytniki i urządzenia systemowe wraz z doprowadzonym okablowaniem.

Oprogramowanie integrujące należy zainstalować na istniejącym serwerze i stacjach roboczych Zamawiającego.

Nowe centrale powinny spełniać poniższe parametry:

- obsługiwać jednocześnie system kontroli dostępu (SKD) jak i również system sygnalizacji włamania i napadu (SSWiN),
- posiadać dwie niezależne magistrale systemowe, pozwalające na integracji co najmniej 30 urządzeń modułów zbierania danych co najmniej 32 stacje zazbrajania,
- posiadać zintegrowany port komunikacyjny TCP/IP służący do celów serwisowych, do programowania,

wizualizacji i zarządzania systemem oraz integracji z innymi elementami systemu z wykorzystaniem połączenia z aplikacjami szyfrowanego algorytmem AES 128-bit,
- umożliwiać zwiększenie ilości linii w systemie z 256 do 512,
- posiadać 255 wyjść w systemie, linie parametryzowane oraz 16-32 linii dozorowych,
- umożliwiać nadzorowanie 3 stanów detektora za pomocą 1 wejścia (alarm, antymasking, sabotaż),
- posiadać 64 niezależnych obszarów (zamiast obecnych 16), 138 Grupy Alarmowe, 120 Grupy Drzwi (strefy kontroli dostępu),
- obsługiwać co najmniej 1000 użytkowników
- posiadać rejestr zdarzeń alarmowych co najmniej 10000 zdarzeń,
- posiadać rejestr zdarzeń kontroli dostępu co najmniej 15000 zdarzeń,
- umożliwiać podłączenie co najmniej 16 urządzeń sterujących systemem (czytniki kart, klawiatury),
- zapewnić komunikacji pomiędzy urządzeniami za pomocą magistrali RS485,
- dawać możliwość zbudowania pętli dwustronnie zasilanej,
- zapewnić nadzór zdalny po TCP/IP, synchronizację czasu po NTP, sterowanie systemem poprzez kalendarz oraz wykorzystanie kart kontroli dostępu do sterowania systemem,
- zapewnić współpracę z istniejącymi kontrolerami 4-drzwi
  - 4 jedno lub obustronne przejścia
  - Nie mniej niż 16 wyniesionych czytników na magistrali lokalnej, przeznaczonych do sterowania przejściami oraz systemem alarmowym
  - Od 8 do 32 linii wejściowych w kontrolerach, 4 wyjścia przekaźnikowe do sterowania zamkami , do 52 wyjść dodatkowych
  - Pełna, lokalna kopia bazy danych użytkowników oraz praca autonomiczna
  - Wykorzystanie czujników kontroli dostępu w ochronie obszarów
  - Definiowane czasy otwarcia drzwi dla typów kart
  - Blokowanie linii na czas otwarcia
  - Sygnalizacja zbyt długiego otwarcia drzwi
  - Sygnalizacja wymuszonego otwarcia drzwi
  - Sterowanie drzwiami za pomocą kombinacji kart i kodów
  - Funkcja anty pass-back
  - Zaawansowane funkcje związane z regionami
  - Realizacja funkcji “śluza”
  - Blokowanie przejść przy zazbrojonym obszarze
  - Sterowanie systemem włamaniowym

Integrację systemów kontroli dostępu (SKD) oraz sygnalizacji włamania i napadu (SSWiN) zbudowanych w oparciu o nowe centrale należy wykonać z wykorzystaniem specjalistycznego oprogramowania właściwe zsynchronizowanego z zainstalowanymi systemami dedykowanego przez producenta sprzętu, urządzeń i systemów zainstalowanych na obiekcie.

Zastosowane oprogramowanie powinno być łatwe zarówno w instalacji, jak i w użyciu, intuicyjny i zaprojektowany dla użytkownika końcowego. Wyświetlane informacje powinny być dostosowane do uprawnień operatora, charakteryzować się zunifikowaną obsługą urządzeń dla wszystkich systemów i nie powinno wymagać specjalistycznej wiedzy operatora ze sposobu działania urządzeń wchodzących w skład integrowanych systemów.

System powinien być oparty o architekturę klient-serwer i pracować w oparciu o standardową bazę danych np.: MS SQL. Połączenie klienta z serwerem odbywać powinno się z udziałem szyfrowania SSL, a połączenie pomiędzy nadzorowanymi systemami bezpieczeństwa prowadzone powinno być z udziałem sieci Etehernet.

Oprogramowanie powinno zapewniać możliwości związane z funkcjami w programie dla różnych operatorów poprzez definiowanie tak zwanych „Ról”:
- Definiowanie użytkowników systemu
- Definiowanie praw dostępu do aplikacji
- Definiowanie kart, kodów PIN
- Definiowanie praw dostępu do systemu
- Konfigurację integracji systemów
- Konfigurację sterowania i zarządzania zdarzeniami
- Konfigurację praw dostępu
- Wydruki raportów praw dostępu
- Wizualizację stanu urządzeń i zdarzeń

Ekran monitora alarmów stacji klienckiej powinien stanowić podstawowe narzędzie do zarządzania alarmami oraz kontrolą systemu przez operatora. Powinien umożliwiać między innymi potwierdzanie alarmów,

dodawanie własnych komentarzy do zdarzeń, przeglądanie historii, otwieranie drzwi, zazbrajanie i rozbrajanie stref czy też zawieszanie wejść. Funkcjonalność „strażnika" powinna pozwalać na monitorowanie przejścia i wyświetlanie statusów osób przechodzących przez wskazane drzwi. Hierarchiczna struktura powinna pozwalać na proste zarządzanie osobami, dzięki dziedziczeniu uprawnień z nadrzędnych węzłów. Dodatkowo program powinien umożliwiać przeprowadzanie akcji automatycznych umożliwiając zdefiniowanie różnych scenariuszy działania systemów w zależności od konkretnego zdarzenia.

WARUNKI PROWADZENIA PRAC

Warunkiem integracji jest wykorzystanie istniejących kontrolerów, czytników i okablowania. Integracja systemów nie może zakłócić pracy portu lotniczego, zmienić poziomu zabezpieczenia dostępu i ochrony obiektów. Prace powinny być wykonywane poza godzinami pracy portu lotniczego. Wykonawcę obowiązują regulaminy, przepisy i zasady poruszania się po lotnisku. Prace będą prowadzone w strefie zastrzeżonej i wymaga to asysty pracowników Służby Ochrony Lotniska. Wykonawca musi uwzględnić koszty związane ze świadczeniem asysty według obowiązującego cennika PLOM.

WYMAGANIA W STOSUNKU DO WYKONAWCY

1. Firma biorąca udział w procedurze wyboru Wykonawcy powinna:
   a) posiadać Koncesję MSWiA na wykonywanie działalności gospodarczej w zakresie usług ochrony osób i mienia realizowanych w formie zabezpieczenia technicznego,
   b) posiadać świadectwo bezpieczeństwa przemysłowego I stopnia lub pisemne potwierdzenie zdolności przedsiębiorcy do zapewnienia ochrony informacji niejawnych o klauzuli ZASTRZEŻONE, wydane w związku z realizacją umów lub zadań,
   c) posiadać polisę ubezpieczenia Odpowiedzialności Cywilnej przedsiębiorcy prowadzącego działalność gospodarczą na kwotę min. 100 000, 00 zł,
   d) posiadać autoryzację producenta systemów SKD i SSWiN, firmy UTC Fire & Security,
   e) dysponować odpowiednim potencjałem technicznym oraz osobami zdolnymi do wykonania przedmiotu postępowania, tj.:
      - co najmniej 2 osoby wpisane na listę kwalifikowanych pracowników zabezpieczenia technicznego, posiadające pisemne upoważnienie kierownika jednostki organizacyjnej lub ważne poświadczenie bezpieczeństwa osobowego do dostępu do informacji niejawnych oznaczonych klauzulą ZASTRZEŻONE wraz z zaświadczeniem stwierdzającym odbycie szkolenia w zakresie ochrony informacji niejawnych,
      - co najmniej 2 osoby posiadające świadectwo ukończenia kursu projektowania i montażu elektronicznych urządzeń i systemów alarmowych oraz eksploatacji, konserwacji i napraw w miejscach zainstalowania,
      - co najmniej 1 osobę posiadającą certyfikat ukończenia kursu specjalistycznego z zakresu systemu alarmowego Advisor Advanced oraz aplikacji Advisor Management (ATS8600)
   f) posiadać niezbędną wiedzę i doświadczenie do wykonania zamówienia, tj. w okresie ostatnich 5 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie, należycie wykonała co najmniej jedno zamówienie o wartości min. brutto 100.000,00 zł dotyczące instalacji i uruchomienia systemu lub oprogramowania integrującego systemy kontroli dostępu i sygnalizacji włamania i napadu dla min. 4 central UTC Fire&Security, wraz z podaniem jej wartości, przedmiotu, dat wykonania i podmiotów, na rzecz których usługa ta została wykonana oraz załączeniem dowodów, czy została wykonana należycie.
2. Firma biorąca udział w procedurze wyboru Wykonawcy powinna przedłożyć:
   a) Aktualny odpis z właściwego rejestru, jeżeli odrębne przepisy wymagają wpisu do rejestru, wystawiony nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert, a w stosunku do osób fizycznych stosowne oświadczenie;
   b) Aktualne zaświadczenia właściwego naczelnika urzędu skarbowego potwierdzające, że Wykonawca nie zalega z opłacaniem podatków lub zaświadczenie, że uzyskał przewidziane prawem zwolnienie, odroczenie lub rozłożenie na raty zaległych płatności lub wstrzymanie w całości wykonania decyzji właściwego organu - wystawione nie wcześniej niż 3 miesiące przed upływem terminu składania ofert;
   c) Aktualne zaświadczenia właściwego oddziału Zakładu Ubezpieczeń Społecznych lub Kasy Rolniczego Ubezpieczenia Społecznego potwierdzające, że Wykonawca nie zalega z opłacaniem składek na ubezpieczenie zdrowotne i społeczne, lub potwierdzenie, że uzyskał przewidziane prawem zwolnienie, odroczenie lub rozłożenie na raty zaległych płatności lub wstrzymanie w całości wykonania decyzji właściwego organu - wystawione nie wcześniej niż 3 miesiące przed upływem terminu składania ofert;

d) Aktualną informację z Krajowego Rejestru Karnego, wystawioną nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert;

TERMIN REALIZACJI ZAMÓWIENIA

Wszelkie prace związane z realizacją niniejszego zadania należy wykonać nie później niż do 31.12.2019 r.

KRYTERIUM OCENY OFERT

Wartość oferty 100%

W przypadku pytań: prosimy zadawanie drogą elektroniczną na adres poczty elektronicznej: m.kucman@mazuryairport.pl. Odpowiedzi będą zamieszczane na stronie www.mazuryairport.pl.

Informację o chęci dostępu do dokumentacji projektowej w dniu 30.10.2019 prosimy przesyłać na adres poczty elektronicznej:m.kucman@mazuryairport.pl do dnia 29-10-2019 r. do godz. 14.00.

Informację ofertową prosimy przesyłać na adres poczty elektronicznej:m.kucman@mazuryairport.pl do dnia 4-11-2019 r. do godz. 12.00.

Marek Kucman
Port Lotniczy Olsztyn - Mazury
Warmia i Mazury Sp. z o.o.
Szymany 150, 10-100 Szczytno
+48 89 6231976
+48 604987777