Załącznik nr.1

SZCZEGÓŁÓWY OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiot zamówienia: Dostawa systemu uwierzytelniania, autoryzacji i kontroli dostępu

System uwierzytelniania, autoryzacji i kontroli dostępu
Przedmiotem zamówienia jest dostarczenie, instalacja, konfiguracja oraz wdrożenie systemu służącego do centralnego zarządzania tożsamością, uwierzytelnianiem oraz kontrolą dostępu użytkowników.

Parametry systemu
System musi obsługiwać co najmniej:

- System musi być dostarczony w formie rozwiązania sprzętowego, Zamawiający wyklucza dostarczenia systemu w formie usługi chmurowej lub w formie maszyny wirtualnej;
- System musi posiadać co najmniej 4 interfejsy GbE RJ45;
- System musi posiadać co najmniej dwa dyski twarde o pojemności minimum 1TB każdy;
- System musi umożliwiać zamontowanie go w 19” szafie rack, maksymalna wysokość urządzenia 1U;
- Uwierzytelnianie dla minimum 1500 użytkowników lokalnych i zdalnych;
- System musi umożliwiać rozbudowę do 2000 tokenów mobilnych dla uwierzytelniania dwuskładnikowego;
- 300 klientów protokołu RADIUS;
- Możliwość zdefiniowania co najmniej 100 grup użytkowników;
- Minimum 10 lokalnych centrów certyfikacji (CA);
- Możliwość wygenerowania co najmniej 5 tys. certyfikatów dla użytkowników;
- Uwierzytelnianie dla co najmniej 1500 użytkowników w oparciu o dedykowaną aplikację (agenta), umożliwiającą po jej zainstalowaniu na stacji roboczej z systemem Windows 10/11, aktualizowanie informacji o aktualnie zalogowanym w ramach infrastruktury AD użytkowniku.

W ramach postępowania wymaganym jest dostarczenie bezterminowych licencji na min. 50 tokenów mobilnych/programowych oraz bezterminowych licencji dla min. 1500 użytkowników SSO.

Wymaga się aby dostawa obejmowała również serwis producenta przez okres 12 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.

Wymagania ogólne
System musi zapewniać nie mniej niż:

1. Możliwość pracy w konfiguracji HA (High Availability) z trybem Active-Passive lub Active-Active w celu zwiększenia niezawodności;

2. Graficzną reprezentację statusu uwierzytelnionych użytkowników;
3. Logowanie wszystkich zdarzeń uwierzytelniania wraz z ich statusem, szczegółami dotyczącymi powodów niepowodzenia oraz nazwą użytkownika:
    a. Lokalnie;
    b. Zdalnie w oparciu o protokół Syslog.

Wymagania funkcjonalne – uwierzytelnianie

Celem realizacji funkcji uwierzytelniających, system musi zapewniać nie mniej niż:

1. Lokalną, wbudowaną bazę użytkowników;
2. Przechowywanie następujących informacji o użytkowniku: nazwa, imię i nazwisko, adres email, numer telefonu, adres, kraj;
3. Możliwość zdefiniowania co najmniej 3 indywidualnie konfigurowalnych pól dla każdego z użytkowników;
4. Możliwość importu informacji o użytkownikach z zewnętrznego serwera LDAP lub pliku CSV;
5. Konfigurowalną politykę haseł użytkowników w ramach której możliwym jest określenie:
    a. poziomu złożoności hasła (jego długości minimalnej, występowania małych i dużych liter, cyfr i znaków specjalnych);
    b. czasu ważności hasła;
6. Konfigurowalną politykę blokowania kont, która będzie uwzględniać:
    a. ilość nieudanych logowań;
    b. czas blokowania konta;
    c. okres nieaktywności, po którym konto jest blokowane;
7. Możliwość odzyskiwania haseł:
    a. z wykorzystaniem adresu email;
    b. z wykorzystaniem pytania pomocniczego;
8. Obsługę protokołu RADIUS zgodną z RFC, w tym zakresie system musi oferować:
    a. wbudowany serwer RADIUS;
    b. integrację z zewnętrznymi serwerami RADIUS – praca jako klient;
9. Obsługę protokołu LDAP, w tym zakresie system musi oferować:
    a. wbudowany serwer LDAP;
    b. możliwość zautomatyzowanej synchronizacji z zewnętrznym serwerem LDAP (zarówno kont użytkowników jak i atrybutów LDAP);
10. Obsługę protokołu SAML - Identity Provider (IdP) proxy;
11. Realizację funkcji SSO (Single Sign On) w oparciu o:
    a. integrację z Active Directory, również bez konieczności instalacji dodatkowego oprogramowania na kontrolerach domeny;
    b. dedykowaną aplikację instalowaną na stacjach roboczych z systemem Windows;
    c. kontekst użytkownika przesyłany z serwera RADIUS;
    d. informacje uzyskiwane poprzez protokół Syslog;

Wymagania funkcjonalne – uwierzytelnianie dwuskładnikowe
Realizując uwierzytelnianie dwuskładnikowe, system musi zapewniać nie mniej niż:

1. Obsługę dla tokenów sprzętowych (hardware):
   a. tokeny muszą pochodzić od tego samego producenta co system uwierzytelniania;
2. Wsparcie dla tokenów programowych (software token) dla takich systemów operacyjnych jak iOS, Android;
3. Dla tokenów na system iOS i Android wymaga się:
   a. aktywacji z centralnego systemu uwierzytelniania (seed provisioning);
   b. możliwości konfiguracji ilości generowanych cyfr;
   c. generowania kodu (cyfr) co 30 lub 60 sekund;
   d. możliwości dezaktywacji tokenu oraz jego reinstalacji (przeniesienia na inne urządzenie mobilne);
   e. ochrony dostępu poprzez konfigurowalny kod PIN;

System musi umożliwiać integrację z logowaniem do systemu Windows.

Wymagania funkcjonalne – 802.1x
System powinien umożliwiać realizację uwierzytelniania z wykorzystaniem protokołu 802.1x, spełniając nie mniej niż następujące warunki:

1. Obsługa co najmniej poniższych protokołów EAP:
   a. PEAP;
   b. EAP-TTLS;
   c. EAP-TLS;
   d. EAP-GTC;
2. Wsparcie dla uwierzytelnienia w oparciu o adres MAC (MAC based authentication);
3. Zarządzanie certyfikatami (w oparciu o własne CA) celem wykorzystania w ramach PEAP, TTLS, TLS;

Wymagania funkcjonalne – zarządzanie certyfikatami
System powinien spełniać następujące wymagania w zakresie zarządzania certyfikatami, nie mniej niż:

1. Obsługa wbudowanego CA (Certificate Authority);
2. Obsługa CA pośredniczących (Intermediate CA);
3. Ręczne generowanie certyfikatów z wykorzystaniem interfejsu graficznego;
4. Możliwość pobrania wygenerowanych certyfikatów;
5. Możliwość podpisywania certyfikatów z wykorzystaniem protokołu SCEP;
6. Możliwość automatycznego i ręcznego generowania certyfikatów z wykorzystaniem protokołu SCEP;
7. Możliwość generowania certyfikatów typu wildcard;
8. Realizacja CRL (Certificate Revocation List);
9. Wsparcie dynamicznego odwoływania certyfikatów z wykorzystaniem protokołu OCSP (RFC2560);

Zarządzanie

1. Zarządzanie w oparciu o protokół HTTPS (interfejs graficzny) z wykorzystaniem przeglądarki;
2. System musi udostępniać graficzny interfejs zarządzania poprzez szyfrowane połączenie HTTPS;
3. Tworzenie kopii bezpieczeństwa konfiguracji z poziomu graficznego interfejsu zarządzającego (GUI) oraz na zewnętrzny serwer FTP/SFTP w oparciu o harmonogram, który będzie umożliwiał wskazanie konkretnego czasu kiedy proces ma się rozpocząć;
4. System musi posiadać możliwość zdefiniowania co najmniej 4 lokalnych kont administracyjnych;

Funkcjonalności konieczne do działania z systemami posiadanymi przez Zamawiającego:

1. System musi być zgodny z systemem FortiAnalyzer, celem logowania, korelacji i analizy informacji, koniecznych do utrzymania spójności działania systemów posiadanych przez Zamawiającego, a tym samym zapewnienia spójności utrzymywania bezpieczeństwa;
2. System musi być zgodny z systemem FortiGate, celem wymiany danych o autentykacji i autoryzacji użytkowników znajdujących się w sieci, potrzebnych to utrzymania spójności działania systemów posiadanych przez Zamawiającego, a tym samym zapewnienia spójności utrzymywania bezpieczeństwa. System musi zapewnić dostarczenie informacji o użytkownikach i zdarzeniach w sieci, z ich udziałem (zalogowaniem, wylogowaniem, adres IP) do środowiska zawierającego UTM FortiGate posiadanego przez Zamawiającego, umożliwiając budowę polityk w oparciu o tożsamość użytkownika, ustalaną na bieżąco z przekazanych danych;
3. System musi być gotowy do wdrożenia i integracji z innymi elementami i urządzeniami, odpowiadającymi za bezpieczeństwo infrastruktury, posiadanymi przez Zamawiającego, takimi jak FortiGate, FortiAnalyzer, FortiClient EMS, FortiMail, FortiClient, FrotiWeb oraz działać w oparciu o dane wymieniane między tymi systemami, za pomocą ich wbudowanej funkcjonalności – Secure Fabric, umożliwiającej automatyczne reagowanie na wykryte zagrożenia. Musi posiadać możliwość automatyzacji wymiany danych o użytkownikach w czasie rzeczywistym z systemem FortiClient EMS, FortiClient oraz FortiGate posiadanym przez Zamawiającego;

Szkolenia i usługi

Wdrożenie systemu musi objąć co najmniej:

1. Integrację wdrażanego Systemu z systemem FortiGate, FortiAnalyzer oraz FortiClient EMS;
2. Przygotowanie konfiguracji Systemu właściwej dla integracji z posiadanymi przez Zamawiającego systemami FortiGate, FortiAnalyzer oraz FortiClient EMS;
3. Przygotowanie powdrożeniowej dokumentacji technicznej oraz dokumentacji użytkownika Systemu zawierającej architekturę rozwiązania, spis wszystkich wdrożonych polityk bezpieczeństwa, opis konfiguracji Systemu (w tym nietypowe ustawienia) oraz instrukcję dla użytkownika/administratora Systemu w języku polskim, w formie elektronicznej – PDF oraz Word;

Warsztaty powdrożeniowe

1. Omówienie funkcji wdrażanego Systemu;
2. Omówienie działania mechanizmu identyfikacji oraz autentykacji użytkownika;
3. Omówienie konfiguracji mechanizmów identyfikacji oraz autentykacji użytkownika;
4. Omówienie zarządzania użytkownikami, politykami MDA oraz SSO;
5. Omówienie integracji Systemu z systemami FortiGate oraz FortiAnalyzer;
6. Omówienie tworzenia kopii zapasowej Systemu i odtwarzania w razie awarii;

Zakres warsztatów powinien obejmować co najmniej:

a. Czas trwania warsztatów: co najmniej 16 godzin, podzielonych na min. 4 spotkania;
b. Zajęcia muszą być przeprowadzone w języku polskim;
c. Warsztaty musza się odbyć w formie wideokonferencji w dni robocze w godzinach 9.00 – 14.00;
d. Uczestnikom zapewnione zostaną materiały dydaktyczne w formie elektronicznej w języku polskim;