Łukasiewicz
Instytut Technik
Innowacyjnych
EMAG

OPIS PRZEDMIOTU ZAMÓWIENIA

„Dostawa oprogramowania do nadzorowania sesji uprzywilejowanych"
– nr postępowania FH/02/07/23

OPOGRAMOWANIE DO NADZOROWANIA SESJI UPRZYWILEJOWANYCH

Opis oprogramowania	**Oprogramowanie do nadzorowania sesji uprzywilejowanych**
Warunki licencji	1. Licencja nie może ograniczać ilości użytkowników, których w danym momencie sesje są nadzorowane, 2. Licencja powinna umożliwiać nadzorowanie dostęp do co najmniej 25 usług, 3. Wsparcie producenta, które obejmuje roczne aktualizacje oraz wsparcie liczone od dnia 31.12.2022. 4. Zamawiający posiada u siebie wdrożone rozwiązanie BeyondTrust Privilege Remote Access, zatem zaproponowane licencje mogą tyczyć się przedłużenia działania tego rozwiązania lub całkowicie nowego, równoważnego, spełniające opisywane funkcjonalności wraz z wdrożeniem
Cechy oprogramowania równoważnego	**Architektura** 1. System musi być dostarczany w formie zamkniętej platformy wirtualnej przygotowanej do implementacji w infrastrukturze. Przez zamkniętą platformę rozumiemy wyspecjalizowane rozwiązanie, w ramach którego zainstalowana jest całość oprogramowania (system operacyjny, baza danych, aplikacja), realizujące funkcjonalności systemu. 2. System musi być zaprojektowany i przygotowany do umieszczenia w DMZ (hardening producenta). 3. System na potrzeby realizacji swoich funkcji nie może wymagać zestawienia tunelu VPN pomiędzy siecią LAN organizacji, a komputerem zewnętrznego dostawcy. Nie może też wykorzystywać technologii chmurowej do nawiązania połączenia. 4. System musi umożliwiać tryb pracy awaryjnej zapewniający synchronizację danych między dwoma urządzeniami do

	uprzywilejowanego dostępu zdalnego, tworząc uproszczony proces bezpiecznej wymiany uszkodzonego urządzenia na zapasowe. 5. System musi umożliwiać nawiązywanie sesji przynajmniej w dwóch trybach: a) Z wykorzystaniem instalowanego agenta na systemie, do którego będzie nawiązywana sesja, b) Z wykorzystaniem serwerów proxy bez potrzeby instalacji agenta na systemie, do którego będzie nawiązywana sesja. 6. Serwery proxy (nawiązywanie sesji w sposób bezagentowy) muszą być zarządzane w sposób centralny z poziomu oprogramowania do uprzywilejowanego dostępu zdalnego (konfiguracja minimalnie w zakresie: nadawania uprawnień dostępowych do serwera proxy dla zewnętrznych dostawców, utworzenie serwera proxy, wyłączenie serwera proxy). 7. Komunikacja między elementami systemu do uprzywilejowanego dostępu zdalnego (tj. oprogramowaniem uprzywilejowanego dostępu zdalnego, agentami instalowanymi na urządzeniach końcowych oraz serwerami proxy) musi być szyfrowana (TLS) i odbywać się na jednym porcie 443. 8. Elementy systemu (agenci, serwery proxy, klienci) instalowani na zasobach i stacjach roboczych muszą umożliwiać pracę w trybie aktywnego nawiązywania połącznia z systemem uprzywilejowanego dostępu zdalnego, tj. bez pozostawiania otwartych portów nasłuchujących na urządzeniach końcowych. 9. System musi posiadać wsparcie dla protokołów SSH, RDP oraz VNC. 10. System musi posiadać możliwość rozbudowy o moduł obsługi sesji do aplikacji WEB (wbudowana przeglądarka WWW). 11. Systemu musi posiadać możliwość uruchomienia sesji aplikacyjnych (uruchomienie wskazanej aplikacji z serwera usług terminalowych lub uruchomienie aplikacji za pomocą dedykowanego agenta) 12. Systemu musi posiadać możliwość tunelowania protokołów TCP na zdefiniowanym porcie między komputerem zewnętrznego dostawcy a zarządzanym systemem. 13. System ma być dostarczony w polskiej wersji językowej (zarówno menu konfiguracyjne systemu jak i interfejs klientów, za pomocą których realizowane są sesje). **Funkcje operacyjne sytemu uprzywilejowanego dostępu zdalnego** 1. Logowanie do systemu uprzywilejowanego dostępu zdalnego musi odbywać się poprzez konta lokalne (tworzone na poziomie

	systemu do uprzywilejowanego dostępu zdalnego) lub konta i grupy importowane z Active Directory. 2. Logowanie dostawców zewnętrznych do systemu uprzywilejowanego dostępu zdalnego musi być zabezpieczone drugim składnikiem (2FA). 3. System musi realizować następujące scenariusze nawiązywania sesji przez zewnętrznego dostawcę: a) za pomocą klienta zainstalowanego na komputerze zewnętrznego dostawcy (gruby klient), b) za pomocą przeglądarki WWW z komputera zewnętrznego dostawcy (bez potrzeby instalacji klienta), c) za pomocą klienta zainstalowanego na urządzeniu mobilnym (minimum wsparcie dla systemu Android). 4. System musi umożliwiać opcję zastosowania przez kontraktora własnych klientów RDP i SSH. 5. System musi umożliwiać realizację sesji do stacji roboczych (przynajmniej Windows i Linux) i współdzielenie tej samej sesji między kontraktorem a operatorem pracującym przy stacji roboczej. 6. Rozpoczęcie sesji współdzielonej między kontraktorem a operatorem stacji roboczej musi podlegać procesowi akceptacji przez operatora stacji roboczej do której realizowana jest ta sesja. 7. Rozpoczęcie sesji przez zewnętrznego dostawcę musi podlegać kontroli dostępu poprzez: a) Wysyłanie powiadomień o zdarzeniu rozpoczęcia i zakończenia sesji przez zewnętrznego dostawcę do zdefiniowanej listy osób, b) Ograniczenie możliwości nawiązywania sesji przez zewnętrznych dostawców do określonych dni i godzin, oraz do określonych grup zasobów. c) Włącznie procesu wnioskowania przez zewnętrznego dostawcę o dostęp do zasobów i mechanizmu akceptacji lub odrzucenia wniosku przez właściciela zasobu. We wniosku muszą znaleźć się przynajmniej zakres dat, kiedy zewnętrzny dostawca będzie nawiązywał sesję oraz pole pozwalające opisać zakres wykonywanych przez niego prac. Wniosek musi być wysyłany w celu akceptacji do zdefiniowanej listy osób. 8. Konsola dostępowa dla zewnętrznego dostawcy musi posiadać co najmniej poniższe funkcje:

	a) widok grup zasobów z możliwością nawiązania sesji do tych zasobów (za pomocą menu kontekstowego lub podwójnego kliknięcia), oraz możliwością wyszukiwania zasobów po ciągach znaków b) szczegółowy opis zasobu, do którego możliwe jest nawiązanie sesji, zawierający nazwę hosta / adres IP, status (aktywny/nieaktywny), typ systemu operacyjnego, edytowalną nazwę skróconą. c) funkcję wieloosobowego chatu działającą między uczestnikami sesji. 9. System musi umożliwić wyłączenie synchronizacji schowka i kopiowania plików między komputerem zewnętrznego dostawcy a zarządzanym zasobem. 10. System w trakcie sesji realizowanej przez zewnętrznego dostawcę musi umożliwiać: a) Dołączenie do sesji dodatkowych użytkowników posiadających konta w systemie uprzywilejowanego dostępu zdalnego; b) Dołączenie dodatkowych użytkowników do sesji nieposiadających konta w systemie uprzywilejowanego dostępu zdalnego przy jednoczesnej możliwości nałożenia dodatkowych restrykcji dla takiej osoby (minimum w zakresie odebrania kontroli myszy i klawiatury, automatyczne zakończenie sesji w przypadku braku połączenie autoryzowanego użytkownika ulegnie awarii); c) Przejęcie sesji zewnętrznego dostawcy przez uprawnioną osobę (audytora) i jej zakończenie. **Funkcje raportowania** 1. System musi posiadać wbudowany i centralnie zarządzany moduł raportowy. 2. System musi generować centralnie konfigurowane i składowane raporty z przeprowadzonych sesji (łącznie z nagraniami sesji). 3. System musi rejestrować sesje graficzne oraz sesje z wierszem poleceń. 4. System musi umożliwiać wybór rozdzielczości rejestrowanych sesji. 5. W systemie muszą być dostępne raporty dotyczące co najmniej przeprowadzonych sesji i wykorzystania poświadczeń z wbudowanego magazynu haseł. 6. Raporty dotyczące przeprowadzonych sesji muszą podlegać filtrowaniu co najmniej (wymagane wszystkie wymienione) w

	zakresie daty, nazwy użytkownika (zewnętrznego dostawcy), nazwy / adresu IP zarządzanego zasobu, grupy zarządzanych zasobów. 7. System musi posiadać możliwość uruchomienia filtrowania odbytych sesji po ciągach znaków pisanych z klawiatury w trakcie ich trwania. 8. W szczegółach raportu sesji muszą znajdować się co najmniej informacje na temat: a) daty rozpoczęcia i zakończenia sesji (długość trwania sesji), b) nazwy konta przechowywanego we wbudowanym magazynie haseł za pomocą którego zalogowano się do systemu, c) przesyłanych plików między maszyną zewnętrznego dostawcy a zarządzanym zasobem, d) nagrania z sesji (sesje graficzne oraz okna konsoli), e) transkrypcji chatu, f) wszystkich uczestników sesji (osoby, które dołączały do sesji w trakcie jej trwania), g) listy zdarzeń (log) dotyczący pracy narzędzia uprzywilejowanego dostępu zdalnego. **Konfiguracja i instalacja agentów** 1. Plik instalacyjny agenta instalowanego na zarządzanym zasobie musi być przygotowany do masowej instalacji. 2. Plik instalacyjny agenta instalowanego na zarządzanym zasobie musi posiadać datę ważności, po upływie której niemożliwe będzie jego wykorzystanie. 3. Agent instalowany na zarządzanym zasobie musi być aktualizowany w sposób centralny z poziomu systemu uprzywilejowanego dostępu zdalnego. 4. System musi zapewniać możliwość określenia polityk aktualizacji agenta (możliwość definiowania co najmniej liczby jednocześnie aktualizowanych agentów oraz pasma przeznaczonego na aktualizację przez sieć). 5. System musi zapewnić możliwość zdefiniowania akcji zbierania dodatkowych danych na temat zdalnego hosta przez agenta, bez konieczności nawiązywania sesji (przynajmniej w zakresie zużycia CPU, nazwy zalogowanego użytkownika, zajętości dysku). **Wbudowany magazyn haseł**

	1. System musi posiadać wbudowaną funkcjonalność magazynu poświadczeń (przechowywanie nazw kont i haseł, ukrywanie widoczności haseł przed zewnętrznymi dostawcami). 2. System musi umożliwiać dodawanie kont wykorzystywanych do zdalnego logowania co najmniej poprzez: a) wprowadzenie ręczne z poziomu interfejsu konfiguracyjnego narzędzia, b) wyszukanie i import z Active Directory, z możliwością automatycznej zmiany haseł na takich kontach. c) możliwość zintegrowania pobierania poświadczeń z systemu PAM (przynajmniej jednego), poświadczenia muszą być prezentowane w kontekście zasobu, do którego łączy się zewnętrzny dostawca (przy nawiązywaniu sesji musi być możliwość wyboru poświadczeń występujących wyłącznie na danym zasobie). 3. Użycie poświadczeń przez zewnętrznych dostawców musi podlegać kontroli dostępu. Uprawnienia do korzystania z danych poświadczeń (haseł) muszą być przyznawane dla pojedynczego konta dostawcy lub dla grupy kont dostawców. 4. Hasła przechowywane w magazynie haseł muszą być szyfrowane AES256 lub lepszym. **Integracje** 1. System musi posiadać otwarte API w zakresie pozwalającym na wykonanie integracji z oprogramowaniem firm trzecich. 2. System musi umożliwiać wykonanie integracji z systemami typu SIEM (syslog). 3. System musi umożliwiać wykonanie integracji z systemem PAM w zakresie pobierania z niego poświadczeń. 4. System musi umożliwiać wysyłanie powiadomień z wykorzystaniem SMTP. **Kontrola dostępu** 1. System musi posiadać możliwość zdefiniowania restrykcji sieciowych pozwalających ograniczyć dostęp do interfejsu zarządzającego oprogramowaniem przynajmniej w zakresie zdefiniowania adresów IP hostów lub adresów sieci znajdujących się na białej liście (liście dostępowej) i domyślnej akcji odrzucania innego ruchu skierowanego do interfejsu zarządzającego.

	2. System musi umożliwiać edycję poziomu uprawnień użytkowników lub grup użytkowników co najmniej w zakresie: a) edycji grup zasobów w zakresie nadawania uprawnień dostępowych do zasobów dla zewnętrznych dostawców oraz uprawnień do edycji tych zasobów (zabronienie możliwości edycji zasobów w systemie uprzywilejowanego dostępu zdalnego), b) edycji i tworzenia nowych poświadczeń w magazynie haseł oraz do przyznawania uprawnień dla zewnętrznych dostawców do możliwości wykorzystania tych poświadczeń, c) generowania i podglądu raportów w tym nagrań z sesji, d) możliwości zapraszania do sesji dodatkowych użytkowników, e) możliwości odebrania lub nadania uprawnień do realizowania sesji z wykorzystaniem instalowanych agentów, serwerów proxy, protokołu RDP lub SSH. f) możliwości definiowania białych lub czarnych list poleceń w sesjach uruchamianych w konsoli.
Zakres wdrożenia dla rozwiązania równoważnego:	1. Inicjalizacja oprogramowania w środowisku Zamawiającego 2. Konfiguracja i instalacja agentów (5 sztuk na systemach Windows i Linux) lub utworzenie elementów połączeniowych (5 sztuk RDP oraz SSH) 3. Instalacja konsol dostępowych oraz ich konfiguracja 4. Skonfigurowanie integracji z domeną na potrzeby logowania do dostarczanego systemu 5. Konfiguracja i instalacja jump point jeśli jest dostępny 6. Konfiguracja sejfu haseł, import i tworzenie kont zarządzanych 7. Utworzenie do 3 grup użytkowników i nadanie uprawnień (role administratorzy, wnioskujący – firma zewnętrzna, pracownicy domowi) oraz skonfigurowanie uprawnień 8. Utworzenie polityk dla sesji 9. Testy odbiorcze konfiguracji 10. Opracowanie dokumentacji powdrożeniowej oraz instrukcji używania systemu dla użytkowników końcowych