Ogólne - architektura

1. System PAM musi być rozwiązaniem bezagentowym tj. umożliwiającym nawiązywanie sesji z wykorzystaniem serwerów proxy bez potrzeby instalacji oprogramowania (agenta) na systemie, do którego będzie nawiązywana sesja, umożliwiającym uwierzytelnianie wieloskładnikowe i obsługujące wiele platform i systemów operacyjnych. System PAM ma zabezpieczać dostęp do maszyn fizycznych, maszyn wirtualnych, sprzętu sieciowego m.in. routery, przełączniki, zapory sieciowe, aplikacje, bazy danych itp.
2. System musi być dostarczany w formie zamkniętej platformy wirtualnej przygotowanej do implementacji w infrastrukturze Hyper-V lub VMware . Przez zamkniętą platformę rozumiemy wyspecjalizowane rozwiązanie, w ramach którego zainstalowana jest całość oprogramowania (system operacyjny, baza danych, aplikacja), realizująca wszystkie funkcjonalności systemu.

Licencjonowanie

1. System PAM musi zostać dostarczony z kompletem licencji dla co najmniej 5 użytkowników, którzy będą korzystali z Systemu PAM, minimum dla następującej liczby funkcjonalności:
    a. Ochrona kont uprzywilejowanych,
    b. Ochrona kluczy SSH,
    c. Zarządzanie i monitorowanie sesji uprzywilejowanych,
    d. Rejestrowanie sesji uprzywilejowanych
    e. Raportowanie wykorzystania kont uprzywilejowanych,
2. Dostarczone licencje na System PAM do ochrony kont uprzywilejowanych nie mogą mieć ograniczeń czasowych. Dostarczone licencje będą udzielone bezterminowo.
3. Dostarczone licencje na system PAM nie mogą w żaden sposób limitować ilości chronionych systemów docelowych.
4. System powinien być dostarczony wraz z rocznym/trzyletnim serwisem umożliwiającym korzystanie ze wsparcia producenta oraz dystrybutora oraz pobieranie aktualizacji przygotowanych przez producenta.

Funkcjonalności

1) System PAM musi zapewniać możliwość zarządzania (w szczególności):
    a) Użytkownikami na systemach operacyjnych: Windows, Unix/Linux,
    b) Kontami domenowymi: MS Active Directory,
    c) Kontami lokalnymi: VMware ESX/ESXi,
    d) Kontami na urządzeniach m.in.: Cisco, Aruba, Alcatel, CheckPoint, Fortigate, Huawei, IBM AIX, Brocade,
    e) Kontami baz danych: Microsoft SQL, Oracle, MySQL, PostgreSQL
    f) Kontami do zarządzania i monitorowania serwerów: m.in. iLO, iDRAC,
    g) Kontami aplikacji webowych: Facebook, Google, Twitter, Linkedin, Instagram, Openstack, AWS
    h) Kontami w innych nie wymienionych systemach/urządzeniach do których dostęp odbywa się po protokołach: SSH, RDP,VNC, TELNET, HTTP/HTTPS.
2) System PAM musi umożliwiać usługę pośredniczenia w dostępie do systemów i urządzeń dla użytkowników domenowych oraz użytkowników zewnętrznych, rejestrując obsługiwane sesje, oraz obsługując minimum następujące protokoły: SSH, RDP,VNC, TELNET, HTTP/HTTPS.
3) System PAM musi umożliwiać dostęp użytkowników do systemu docelowego następującymi narzędziami:
    a) przeglądarka internetowa,
    b) klient RDP,

c) klient protokołu SSH/Telnet (np. putty).

4) System PAM musi wspierać minimum następujące mechanizmy uwierzytelniania: LDAP, RADIUS, Tacacs Active Directory, OpenID.
5) System PAM powinien zapewniać możliwość dwuskładnikowego uwierzytelniania.
6) System PAM musi obsługiwać monitorowanie i ochronę nawet kilkudziesięciu jednoczesnych połączeń od jednego użytkownika końcowego, do różnych systemów poprzez wiele lub jedno konto uprzywilejowane.
7) System PAM musi ograniczać administratorowi możliwość dostępu do haseł lub ograniczać podgląd do haseł uprzywilejowanych.
8) System PAM musi umożliwiać budowanie polityk kontroli dostępu w oparciu o role, np. na podstawie przynależności do grup AD/LDAP.
9) System PAM musi posiadać log dla wszystkich zdarzeń systemowych.
10) System PAM musi umożliwiać wskazanie kont użytkowników, które realizowały logowanie do stacji/serwera.
11) System PAM musi umożliwiać raportowanie wszystkich zmian wprowadzonych przez administratorów.
12) System PAM musi umożliwiać raportowanie wszystkich logowań do systemu.
13) System PAM musi umożliwiać raportowanie oparte na nietypowym źródle, czasie i długości połączenia do systemu docelowego.
14) Rozwiązanie musi posiadać graficzną wizualizację przedstawiającą status bezpieczeństwa aktywnych oraz historycznych sesji do systemów zdalnych.
15) System PAM musi umożliwiać ograniczenie dostępu do raportów dla wskazanej grupy użytkowników lub administratorów.
16) System PAM musi mieć możliwość zmiany wartości hasła na systemie docelowym zgodnie z ustawioną polityką m.in.:
    a) umożliwiać zdefiniowanie wymagań na: długość hasła, znaki w haśle (małe i duże litery, cyfry, znaki specjalne),
    b) generować automatycznie hasła kont systemów docelowych w sposób pseudo losowy,
    c) generować unikalne hasła dla konta systemów docelowych,
    d) wymuszać automatyczną zmianę hasła po jego podglądzie
17) System PAM musi umożliwiać transparentne połączenie do systemu docelowego, bez konieczności podawania przez użytkownika hasła konta uprzywilejowanego.
18) System PAM musi umożliwiać ograniczanie dostępu do systemów docelowych oraz tworzenie białych i czarnych list poleceń wykonywanych w systemie docelowym (audyt poleceń).
19) Audyt poleceń musi umożliwiać podjęcie co najmniej akcji, zablokuj polecenie i rozłącz sesję po wykryciu audytowanego polecenia a także automatyczne umieszczenie na liście blokowanych użytkowników użytkownika, który próbował wykonać blokowane polecenie.
20) System PAM musi umożliwiać nagrywanie sesji wraz z podglądem sesji aktywnej oraz możliwość jej przerwania.
21) Nagrywanie sesji nie może mieć żadnego wpływu na wydajność systemu docelowego.
22) System PAM musi rejestrować znaki wprowadzone z klawiatury przez użytkownika co najmniej dla sesji SSH i RDP oraz umożliwiać szybkie przeszukiwanie zapisanych danych pod kątem występowania wskazanych słów kluczowych.
23) System PAM musi umożliwiać odtworzenie zarejestrowanych nagrań sesji.
24) Oprogramowanie dostarczone w ramach realizacji zamówienia musi pochodzić z oficjalnego kanału dystrybucyjnego producenta na terenie Polski. W przypadku zaproponowania rozwiązania z innego kanału dystrybucji Wykonawca musi przedstawić dokument potwierdzający, iż zaoferowany produkt posiada wsparcie producenta na terenie Polski.

25) System PAM musi być kompletny i pozwalać na uruchomienie minimum następujących funkcjonalności:
   a) zarządzać kontami uprzywilejowanymi w ramach organizacji,
   b) monitorować wykorzystanie kont uprzywilejowanych,
   c) nagrywać i archiwizować sesje zdalne,
   d) gwarantować skalowalność rozwiązania w przypadku dodawania nowych zasobów oraz nowych usług,
26) System PAM musi umożliwiać personalizację wyglądu aplikacji co najmniej po przez umieszczenie logo zamawiającego w głównym oknie aplikacji.

W ramach sprzedaży wykonawca musi wstępnie wdrożyć środowisko, oraz przeprowadzić warsztaty 5 godzin w zakresie:

1. zarządzanie użytkownikami

- utworzenie użytkownika lokalnego

- synchronizacja z AD

- włączenie autentykacji w AD

- dodawanie serwera autentykacji AD

- testowanie poprawności konfiguracji

- konfigurowanie synchronizacji grup dla użytkowników AD (administratorów, userów, approverów)

- przypisywanie uprawnień dla danych grup

2. dodawanie urządzeń

- dodawanie zasobów do połączeń: SSH, RDP

3. dodawanie poświadczeń

- dodawanie poświadczeń do zasobów opartych o połączenia SSH, RDP, HTTPS

4. Zarządzanie hasłami

- definiowanie typów haseł

- dodawanie polityki haseł

- włączanie zarządzania hasłem

- używanie pluginów i skryptów do zarządzania haseł

- ręczne wymuszenie zmian hasła

5. Zarządzanie dostępem i uprawnieniami

- tworzenie access group

- zarządzanie access grupą

6. Audytowanie poleceń

- automatyzacja kontroli użytkownika przez tworzenie audytu komend

7. Monitorowanie połączeń

- Testowanie połączeń RDP, SSH, HTTPS

8. Raporty

- weryfikacja dostępu do poświadczeń

- dostęp do podglądu haseł

- modyfikacje systemu

9. Ustalenie dostępu do MASTERKEY

- tworzenie polityki bezpieczeństwa dostępu do backupu

- włączanie 2FA

- pobieranie klucza do backupu

- procedura odtworzenia klucza

- odszyfrowanie backupu