20/W/2024

Wymagania techniczne systemu wieloskładnikowego uwierzytelniania dla 300 użytkowników infrastruktury OR POLATOM.

Dostawa licencji oraz usługi wdrożenia wraz ze szkoleniem pracowników:

- dostarczenie odpowiedniej ilości licencji wieczystych wraz z wsparciem na okres 5 lat na oferowane rozwiązanie;

Rozwiązanie nie może posiadać licencyjnych ograniczeń związanych z wymaganą funkcjonalnością dla 300 obsługiwanych użytkowników oraz 10 licencji na zaawansowane funkcje oferowane przez system bez ograniczeń czasowych na używanie systemu.

- wykonanie usługi uruchomienia systemu wraz z działem IT OR POLATOM w zakresie generowania jednorazowych kodów na telefonach komórkowych, uruchomienie dwuskładnikowego logowania do poczty przez stronę www (serwer Exchange wraz z OWA).

Zakres wymaganych prac związanych z wdrożeniem systemu:

- opracowanie harmonogramu wdrożenia systemu;
- przeprowadzenie instalacji i konfiguracji systemu;
- Integracja systemu z usługami AD oraz koncentratorem VPN;
- Integracja systemu z stroną poczty;
- przygotowanie i przeprowadzenie scenariuszy testowych weryfikujących wydajność i poprawność wdrożonego systemu w środowisku Zamawiającego.

- wykonanie usługi szkolenia z zakresu administracji, konfiguracji z systemem;

- wsparcie telefoniczne pracowników IT OR POLATOM przez okres 1 roku w rozwiązywaniu problemów.

Zaoferowane rozwiązanie musi być dostarczone w formie maszyny wirtualnej „virtual appliance”, jako obraz z wbudowanym systemem operacyjnym i preinstalowanym rozwiązaniem przez producenta do bezpośredniej instalacji w środowisku data center Zamawiającego na wymienionych platformach wirtualizacyjnych:

- Hyper-V Server 2016 lub późniejszy,
- VMware ESX 5.5 lub późniejszy.

Rozwiązanie musi mieć możliwość instalacji we własnej serwerowni oraz w środowisku chmurowym.

Wykonawca dostarczy dokumentację systemu, procedurę wykonywania i odtwarzania kopii bezpieczeństwa.

Rozwiązanie powinno obsługiwać użytkowników, których konta przechowywane są w:

- Active Directory Domain Services,
- LDAP (w tym OpenLDAP, OpenDJ),
- Microsoft SQL Server 2016.
- lokalnym repozytorium (baza danych wbudowana w system),

Rozwiązanie musi obsługiwać uwierzytelnianie do systemów:

- MS Windows (desktop i serwer również przez połączenie RDP)
- LINUX
- CentOS
- SUSE Linux Enterprise Server 15
- Red Hat Enterprise Linux Server 7, 8
- Debian 10
- Ubuntu 18
- Mac OS od wersji 10.3
- Microsoft Remote Desktop (mstsc)
- VMware Horizon Client v5

Rozwiązanie musi posiadać możliwość określania ról ograniczające zakres działalności użytkowników z podziałem co najmniej na role:

- administratorzy
- wsparcie w zakresie obsługi użytkowników w zakresie metod uwierzytelniających użytkowników (ang. helpdesk).
- Użytkownicy.

Rozwiązanie musi zapewniać pracę w trybie „multi tenant", tzn. pozwalać na definiowanie rozłącznych konfiguracji.

Rozwiązanie musi posiadać wbudowane mechanizmy wysokiej dostępności (HA) i zapewniać pracę w klastrze (HA). Udzielone licencje na zaproponowane rozwiązanie nie mogą ograniczać liczby zainstalowanych serwerów w infrastrukturze klienta.

- rozwiązanie musi pozwalać na rozbudowę poprzez dołączanie dodatkowych serwerów w klastrze (architektura klastrowa),
- dołączanie kolejnych serwerów nie wymaga przerwy w pracy systemu,
- całość rozwiązania musi współpracować w środowisku równoważenia ruchu http (ang. load balancers).

Rozwiązanie musi dostarczać mechanizm pomocy technicznej dla użytkowników w zakresie obsługi dostępnych dla nich metod uwierzytelniających, tzn.:

- zmiany istniejących,
- dopisywanie nowych

Zarządzanie metodami uwierzytelniającymi powinno mieć możliwość:

- realizacji samodzielnie przez użytkowników z opcją wyłączenia tej funkcjonalności przez administratora, być realizowane przez uprawnione osoby w imieniu użytkowników, za ich wiedzą, bez ich wiedzy,
- realizować przewidzianą przez RODO funkcję: „zapomnij mnie".

Rozwiązanie musi obsługiwać metody uwierzytelniania z wykorzystaniem dedykowanej aplikacji dostarczanej przez producenta dla Smartphone realizującej powiadomienie metodą Push i umożliwiającej potwierdzenie uwierzytelniania w aplikacji bez potrzeby wpisywania kodów i haseł jednorazowych. Aplikacja musi być dostępna na systemy Android i iOS.

- Apple Touch ID
- Urządzenie Bluetooth, które komunikuje się z komputerem, np. Smart Watch
- Karta zbliżeniowa RFID
- Trusted Platform Module z certyfikatem w komputerze
- Hasło jednorazowe wysyłane przez Email (Email OTP)
- Hasło awaryjne ustawione przez administratora w przypadku problemu z logowaniem użytkownika.
- Biometryka odcisk palca
- Token sprzętowy zgodny HOTP,
- Aplikacja generująca Token software zgodny z TOTP,
- Hasło LDAP
- OATH One Time Password
- Własne hasło
- PKI
- RADIUS Klient
- SAML Service Provider
- Pytania i odpowiedzi
- Hasło jednorazowe wysyłane SMS
- Urządzenia/Klucze zgodne Universal Two Factor, FIDO 2.0, U2F
- Hasło jednorazowe przekazywane głosowo (należy podać jakie wymagania Zamawiający musi spełnić, aby uruchomić tę funkcjonalność)
- Zewnętrzny Identity Provider OpenID Connect, OAUTH 2.0, SAML
- Windows Hello
- Bluetooth eSec

W ramach metody z wykorzystaniem aplikacji na Smartphone musi być możliwość realizacji uwierzytelnienia na podstawie lokalizacji GPS (położenia geograficznego) użytkownika. W rozwiązaniu musi być możliwość graficznego zaznaczenia obszaru na mapie z którego będą akceptowane uwierzytelnia za pomocą Smartphone.

Rozwiązanie musi umożliwiać konfiguracje sekwencji uwierzytelniania:

- składającego się z listy metod. Lista może zawierać jedną lub więcej metod.
- sekwencje muszą być kojarzone z użytkownikami na podstawie ich przynależności do wskazanych grup z systemu AD (Active Directory).
- każda sekwencja może być aktywna lub nieaktywna.
- sekwencja jest uznawana za spełnioną tylko wtedy, gdy wszystkie zawarte w niej metody zostały pozytywnie zrealizowane przez użytkownika.

Rozwiązanie musi pozwolić na definiowanie scenariuszy uwierzytelnienia.

Dla każdego scenariusza rozwiązanie musi pozwolić zdefiniować listę sekwencji, z których jedna musi być pomyślnie zrealizowana przez użytkownika, aby uznać proces uwierzytelnienia za skuteczny.

Rozwiązanie musi zapewniać obsługę oraz mieć możliwość budowy polityk zaawansowanego uwierzytelniania odnoszących się do następujących zdarzeń, systemów i aplikacji:

- login do systemu operacyjnego Windows
    - Windows w domenie AD
    - Windows poza domeną AD

- Możliwość uwierzytelnienia w trybie buforowanym (ang. „cache”), tzn. po pierwszym pełnym uwierzytelnieniu, kolejne będą wymagały tylko jednej metody (np. karta dotykowa) bez konieczności pamiętania i podawania hasła domenowego.

Możliwość uwierzytelnienia w trybie „off line” (gdy zamawiane rozwiązanie jest niedostępne dla użytkownika) pracującego na systemie Linux.

Możliwość ograniczenia logowania do domeny MS AD wyłącznie dla użytkowników logujących się przy użyciu zaawansowanych metod uwierzytelniania poprzez dostarczany wraz z oprogramowaniem AA mechanizm instalowany po stronie kontrolera domeny.

Portal logowania do konsoli zaawansowanego uwierzytelniania. Oddzielnie dla grup funkcjonalnych:

- administrowanie,
- raportowanie,
- zarządzanie urządzeniami obsługującymi kody jednokrotne,
- pozyskiwanie informacji o właścicielach kart,
- pomoc techniczna,
- samoobsługa.

Rozwiązanie musi zapewniać integrację oraz gotową obsługę dla:

- MS AD SSO z Kerberos
- Obsługę i plug in do Microsoft Network Policy Server (NPS)
- Obsługę i plug in do Microsoft Remote Desktop Gateway
- MS AZURE
- OFFICE 365
- GOGLE G Suite
- OAUTH2/ OpenID Connect
- SAML2

Rozwiązanie musi zapewniać obsługę RADIUS zarówno jako serwer jak i klient.

Rozwiązanie musi zapewniać obsługę aplikacji i urządzeń zintegrowanych przez Radius Server (np. VPN) przez wykorzystanie procesu uwierzytelniania, który wykorzystuje oddzielny kanał komunikacyjny od podstawowego kanału komunikacyjnego dla potwierdzenia i nawiązania wierzytelnego potwierdzenia Out-of-band (OOB).

Rozwiązanie musi zapewniać uwierzytelnianie aplikacji i urządzeń zintegrowanych przez Radius Server (np. VPN) w trybie Out-of-band (OOB) z wykorzystaniem portalu lub aplikacji i wymienionych metod:

- Dedykowanej aplikacji dostarczanej przez producenta systemu dla Smartphone realizującej powiadomienie metodą Push i umożliwiającej potwierdzenie uwierzytelniania w aplikacji bez potrzeby wpisywania kodów i haseł jednorazowych. Aplikacja musi być dostępna na systemy Android i iOS.
- Urządzenie Bluetooth, które komunikuje się z komputerem, np. Smart Watch.
- Karta zbliżeniowa RFID.
- Trusted Platform Module z certyfikatem w komputerze.
- Hasło jednorazowe wysyłane przez Email (Email OTP).
- Hasło awaryjne ustawione przez administratora w przypadku problemu z logowaniem użytkownika.
- Biometryka odcisk palca.

- Token sprzętowy zgodny HOTP.
- Aplikacja generująca Token software zgodny z TOTP.
- Hasło LDAP.
- OATH One Time Password.
- Własne hasło.
- PKI.
- Pytania i odpowiedzi.
- Hasło jednorazowe wysyłane SMS.
- Urządzenia/Klucze zgodne Universal Two Factor FIDO 2.0 U2F.
- Hasło jednorazowe przekazywane głosowo (Voice OTP – przy założeniu posiadania dodatkowego sprzętu/centrali).
- Windows Hello.

Rozwiązanie musi dostarczać funkcjonalne rozszerzenie dla serwisu Microsoft IIS pozwalające na zabezpieczanie serwowanych aplikacji i zasobów bez potrzeby ich modyfikowania, czyli zapewniać dodanie dodatkowego uwierzytelniania do dowolnych aplikacji działających na tym serwerze (np. Outlook Web Access).

Rozwiązanie musi dostarczać mechanizm jednokrotnego logowania (Single Sign On) dla zdalnego dostępu (Remote Desktop Server, Citrix for Active Directory Groups).

Rozwiązanie powinno mieć opcjonalną możliwość po wykupieniu stosownej licencji aktywacji mechanizmów obsługi ryzyka związanego z uwierzytelnianiem (aktualnie nie wymaganą).

Poziom ryzyka system powinien oceniać na podstawie:

- lokalizacji sieciowej użytkownika (adres IP, sieć IP),
- czasu (bieżącego, ostatniego logowania),
- innej zdefiniowanej w systemie.
- Czynniki oceny ryzyka powinny posiadać wagi pozwalające na globalne określenie ryzyka.

Stosownie do wagi ryzyka system powinien:

- zakończyć procedurę uwierzytelniania z wynikiem pozytywnym.
- zakończyć procedurę uwierzytelniania z wynikiem negatywnym i zablokować dostęp,
- kontynuować procedurę uwierzytelniania przez stosowanie kolejnych metod.

Z każdą sekwencją uwierzytelniania może być związany minimalny poziom ryzyka, przy którym sekwencja będzie miała zastosowanie.

Rozwiązanie musi prezentować raporty w zakresie uwierzytelnień z podaniem użytej sekwencji:

- udanych,
- nieudanych,
- wszystkich,
- przypisanych metod uwierzytelniania,
- podstawowe statystyki.

Rozwiązanie musi posiadać możliwość wykorzystania Google reCaptcha przy dostępie do konsoli, aby się bronić przed atakami robotów internetowych.

Rozwiązanie musi przechowywać informacje o zdarzeniach systemowych.

- Zdarzenia systemowe prezentowane są w ramach portalu administracyjnego,
- zdarzenia systemowe mogą być przekazywane do systemów SIEM, np. w formacie CEF.

Rozwiązanie musi umożliwiać tworzenie kopii bezpieczeństwa pozwalające szybko przywrócić system do ustawień organizacji. Przewrócenie kopii bezpieczeństwa nie może wymagać od użytkowników generowania nowych dostępów.

- Kopia bezpieczeństwa jest wykonywana na żądanie administratora przez wybranie stosownej funkcji w portalu administracyjnym,
- kopia bezpieczeństwa jest wykonywana regularnie bez udziału administratorów,
- kopia bezpieczeństwa jest szyfrowana,

Rozwiązanie musi generować zestaw informacji niezbędnych do zdiagnozowania problemu przez pomoc techniczną (plik do wysłania pomocy technicznej).

Komunikacja z systemem (administracja i użytkownicy) powinna odbywać się przy pomocy protokołu HTTPS z możliwością zmiany certyfikatu SSL.

Rozwiązanie musi posiadać centralną konsolę webową dostępną przy pomocy przeglądarek internetowych:

- Google Chrome 108 i powyżej,
- Mozilla Firefox 108 i powyżej,
- Safari 15 i powyżej,
- Microsoft Edge 109 i powyżej.

Rozwiązanie musi posiadać interfejs dla użytkownika i administratora dostępny w języku polskim. Użytkownicy muszą mieć możliwość logowania się własnymi poświadczeniami.

Rozwiązanie musi pozwalać na modyfikację interfejsu użytkownika poprzez zdefiniowanie własnego obrazka z logo oraz przez dostarczenie własnych arkuszy styli (CSS).

Rozwiązanie musi udostępnić bezpłatnie interfejs programistyczny (REST API) w celu umożliwienia integracji z innym oprogramowaniem.