Załącznik nr 6c

Opis Przedmiotu Zamówienia

Przedmiot zamówienia: Dostawa 35 licencji Microsoft 365 Buissness Premium w rocznej subskrypcji płatnej jednorazowo

W ramach zamówienia Wykonawca zrealizuje konfigurację systemu zarządzania urządzeniami (MDM), antywirusa defender oraz zabezpieczeń tożsamości w oparciu o posiadane przez Zamawiającego licencje Microsoft 365 Business Premium. Wdrożenie obejmie 35 użytkowników oraz ich stacje robocze pracujące w modelu w pełni chmurowym. Prace muszą obejmować następujące elementy:

1. Zabezpieczenie tożsamości i wymuszenie MFA (Entra ID)

• Uruchomienie logowania wieloskładnikowego (Multi-Factor Authentication – MFA) z wykorzystaniem aplikacji Microsoft Authenticator. – czy uzycza swoje kompy, czy klupic klucze

• Skonfigurowanie polityk dostępu warunkowego (Conditional Access) w celu globalnego wymuszenia MFA dla wszystkich użytkowników podczas logowania do usług firmowych, ze szczególnym uwzględnieniem bezwzględnej ochrony kont administracyjnych.

• Wdrożenie reguł blokowania ruchu na podstawie lokalizacji geograficznej (Geo-blocking) uniemożliwiających próby logowania do usług firmowych z krajów wysokiego ryzyka lub państw, w których Zamawiający nie prowadzi działalności.

2. Rejestracja i centralne zarządzanie (Entra ID & Intune)

• Podłączenie komputerów oraz telefonów użytkowników bezpośrednio do chmury.

• Automatyczne objęcie urządzeń zarządzaniem w konsoli Microsoft Intune.

3. Szyfrowanie stacji roboczych (BitLocker)

• Utworzenie i przypisanie polityki wymuszającej automatyczne szyfrowanie całych dysków twardych przy użyciu funkcji BitLocker na zarządzanych urządzeniach.

• Zapewnienie automatycznego zapisu (escrow) i bezpiecznego przechowywania kluczy odzyskiwania (Recovery Keys) dla każdej stacji w chmurowym portalu Entra ID.

4. Zarządzanie uprawnieniami (Windows LAPS)

• Konfiguracja chmurowej wersji rozwiązania Windows LAPS (Local Administrator Password Solution) poprzez polityki Intune.

• Utworzenie unikalnych, automatycznie rotowanych (zmienianych co zdefiniowany czas) haseł dla lokalnego konta administratora na każdej stacji roboczej. Hasła muszą być bezpiecznie składowane w Entra ID z dostępem wyłącznie dla autoryzowanych osób IT Zamawiającego.

5. Utwardzenie stacji (Hardening i Defender)

• Wdrożenie zalecanych polityk bazowych bezpieczeństwa (Security Baselines) w systemach Windows 11.

• Aktywacja i konfiguracja reguł zmniejszania powierzchni ataku (ASR – Attack Surface Reduction) w ramach posiadanych licencji.

6. Weryfikacja poprawności wdrożenia

• Weryfikacja na wszystkich stacjach, czy polityki zostały skutecznie zaaplikowane (poprawny status szyfrowania, pomyślne zaczytanie kluczy BitLocker oraz haseł LAPS do konsoli Entra ID).

• Pomoc użytkownikom w procesie pierwszej rejestracji MFA na telefonach służbowych.

• Przekazanie Zamawiającemu krótkiej instrukcji powykonawczej zawierającej m.in. procedurę dodawania nowych komputerów do systemu w przyszłości oraz sposób odzyskiwania hasła LAPS/BitLocker z konsoli.

7. Konfiguracja tenanta M365

- zmiana nazwy tenanata w url
- konfiguracja zalecanych ustawień podnoszących bezpieczeństwo