I - WYMAGANIA WDROŻENIA ACTIVEDIRECTORY ORAZ SZKOLENIE KADRY INFORMATYCZNEJ

1. CZĘŚĆ OPISOWA - Wdrożenie kontrolera domeny ActiveDirectory musi zostać przeprowadzone na serwerze zamawiającego oraz 18 stanowiskach komputerowych sieci Urzędu Gminy w Ciepłowodach. Zamawiający posiada niezbędną infrastrukturę sprzętową oraz posiada odpowiednie licencję umożliwiające wdrożenie usługi ActiveDirectory. Wdrożenie obejmować również będzie przeniesienie wszystkich danych i zainstalowanego oprogramowania w tym programów dziedzinowych takich jak: Płatnik (Baza SQL i ACCESS), Bestia (Baza SQL i ACCESS), FK 2000 (BAZA SQL) i inne oprogramowanie użytkowe zainstalowane lokalnie (PAKIET OFFICE, ACROBATE READER, CERTUM SMART SIGN, LEGISLATOR, CERTUM CARD READER, 7ZIP i inne).

2. W ramach wdrożenia usługi ActiveDirectory wykonawca:

2.1. przeprowadzi podłączenie do 18 komputerów do serwera ActiveDirectory

2.2. przeprowadzi migrację do 18 użytkowników lokalnych do serwera ActiveDirectory (wraz z wszystkimi danymi i oprogramowaniem)

2.3. skonfiguruje zabezpieczenia w serwerze ActiveDirectory zgodnie z wymaganiami UODO, KRI oraz normy ISO 27001

2.4. sporządzi dokumentację z przeprowadzonych prac wdrożeniowych.

3. Wykonawca do wdrożenia oferowanych rozwiązań musi posiadać następujące osoby z uprawnieniami:

3.1. jedną osobę posiadającą uprawnienia Audytora Wiodącego ISO 27001:2013

3.2. jedną osobę posiadającą uprawnienia Audytora Wewnętrznego ISO 27001:2013 i MCSA SQL Server 2012 i MCSA Windows Server 2012 lub uprawnienia równoważne.

4. W ramach wdrożenia wykonawca przeszkoli w Urzędzie kadrę informatyczną Urzędu z wdrożonych rozwiązań. Osoba szkoląca musi posiadać uprawnienia

Audytora Wiodącego ISO 27001:2013 lub uprawnienia równoważne.

5. W ramach wdrożenia wykonawca przekaże licencje na oprogramowanie, które musi umożliwiać migrację użytkowników lokalnych do serwera domenowego działającego w systemie Windows SERVER 2019 w wersji 64 bity professional z licencją na użytkowanie bezterminową umożliwiając przenoszenie do 18 użytkowników i musi realizować:

5.1. automatyczne przenoszenie profili i ustawień użytkownika z konta lokalnego do konta domenowego,

5.2. automatyczne przeniesienie dokumentów użytkownika z konta lokalnego do konta domenowego i nadanie odpowiednich uprawnień ACL,

5.3. automatyczne przenoszenie uprawnień plikowych i rejestru z konta lokalnego do konta domenowego,

5.4. automatyczne przeniesienie lokalnej skrzynki pocztowej Microsoft Outlook i Thunderbird z domyślnej lokalizacji w koncie lokalnym do konta domenowego.

II – WDROŻENIE OPROGRAMOWANIA SZYFRUJĄCEGO ORAZ SZKOLENIE KADRY PRACOWNIKÓW

1. CZĘŚĆ OPISOWA - wdrożenie oprogramowania do szyfrowania wiadomości email technologią END TO END z ochroną anty phishingową i okresem aktualizacji na 2 lata (18 stanowisk komputerowych). Dodatkowo dostawca przeprowadzi stacjonarne szkolenie kadry informatycznej Urzędu z obsługi wdrożonego oprogramowania oraz przeprowadzi dodatkowe szkolenie zdalne pracowników urzędu z tematyki cyberbezpieczeństwa, zagrożeń poczty email, przepisów prawnych w kontekście normy ISO 27001 przez Audytora Wiodącego ISO 27001 lub uprawnienia równoważne w okresie do 18 września 2023 r.

2. Licencje oprogramowania do szyfrowania wiadomości email technologią END TO END. Wsparcie techniczne i prawo do aktualizacji na 2 lata - bazy reguł, sygnatur i zagrożeń phishing.

3. Oprogramowanie musi zapewnić funkcjonalność:

3.1. szyfrowanie algorytmem AES256 treści wiadomości,

3.2. szyfrowanie algorytmem AES256 załączników,

3.3. szyfrowanie algorytmem AES256 plików,

3.4. szyfrowanie algorytmem AES256 katalogów,

3.5. do odszyfrowania treści wiadomości, plików, katalogów, załączników email nie wymagany jest dodatkowy płatny lub bezpłatny dostęp do usług internetowych, chmury, hostingu lub portalu internetowego.

3.6. do odszyfrowania treści wiadomości, plików, katalogów, załączników email nie wymagane jest połączenie Internetowe.

3.7. do odszyfrowania wiadomości nie jest potrzebne wysyłanie linków do oprogramowania deszyfrującego.

3.8. do odszyfrowania treści wiadomości nie jest wymagane instalowanie dodatkowego oprogramowania deszyfrującego.

3.9. odszyfrowanie treści wiadomości, plików, katalogów, załączników email musi być możliwe na popularnych systemach operacyjnych z środowiskiem graficznym: Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11, Ubuntu Desktop 20.04.3 ,Ubuntu Desktop 21.10, Linux Mint 20.2, Fedora Workstation 35, macOS 11, Android od wersji 6.0

3.10. szyfrowana zawartość wiadomości może zawierać nie tylko tekst ale również elementy graficzne takie jak: HTML i obrazki

3.11. generowania bezpiecznego hasła (litery, cyfry, znaki) o określonej minimalnej długości dla szyfrowania,

3.12. opieczętowania każdej wysłanej wiadomość sygnaturą, która jednoznacznie wskazuje na jej oryginalność,

3.13. zabezpieczenia każdego emaila dedykowanym unikalnym hasłem,

3.14. posiadania wewnętrznej bazy haseł, która umożliwia:

3.14.1. export haseł do pliku,

3.14.2. import haseł z pliku

3.14.3. generowania ponownie haseł w bazie

3.15. posiadania wewnętrznego raportu informującego administratora o szyfrowaniu email przy włączonej opcji generowania hasła dla każdej z nich,

3.16. posiadania wewnętrznego raportu z historią szyfrowanych plików i katalogów wraz z przypisanym hasłem szyfrującym,

3.17. posiadania menu kontekstowego do szybkiego wybierania szyfrowania wiadomości e-mailowych, plików i katalogów,

3.18. pracy i pomocy zdalnej użytkownikom poprzez przejęcie zdalnego pulpitu również poza siecią lokalną z użyciem jednorazowych wygenerowanych kodów autoryzacyjnych. Dodatkowo system pracy zdalnej musi działać niezależnie od włączonej funkcji UAC w systemie Windows.

3.19. integracji z komórką (Android, IOS, Windows Phone) umożliwiającą wygenerowanie sms-a z hasłem i opcją kontaktu sms-ową,

3.20. zabezpieczenia panelu ustawień oprogramowania poprzez hasło dostępowe,

3.21. wykrywania fałszywych e-maili - Antiphishing,

3.22. wykrywania prób podszycia się pod dowolnego adresata - mechanizm ANTISPOOFING,

3.23. wykrywania fałszywych linków i odsyłaczy w wiadomościach e-mailowych,

3.24. wykrywanie niebezpiecznych dokumentów MS Office,

3.25. wykrywanie niebezpiecznych rozszerzeń plików przesyłanych przez pocztę email,

3.26. definiowania alarmów informujących o niebezpiecznych mailach i załącznikach,

3.27. współpracę z serwerem producenta oprogramowania dostarczającym bazy reguł, sygnatur, zagrożeń phishingowych. Dostęp do tej bazy wymagany jest minimum na 2 lata.

3.28. współpracy z klientem Mozilla Thunderbird i Mozilla Thunderbird Portable dla systemów 32 i 64 Bit Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11.

4. Licencja na użytkowanie oprogramowania musi być wieczysta i nie może być uzależniona oraz powiązana z innym oprogramowaniem do bezpieczeństwa np. antywirusy.

6. Oprogramowanie musi działać samodzielnie i do poprawnej jego pracy nie może wymagać innych pakietów bezpieczeństwa np. antywirusy.

7. Oprogramowanie musi poprawnie działać z różnymi zainstalowanymi antywirusami.

8. Oprogramowanie nie może wyłączać domyślnego antywirusa systemowego Windows.

9. Przeprowadzenie stacjonarnego szkolenia kadry informatyczną Urzędu z obsługi wdrożonego oprogramowania. Osoba szkoląca musi posiadać uprawnienia Audytora Wiodącego ISO 27001:2013 lub uprawnienia równoważne.

10. Przeprowadzenie szkolenia zdalnego wszystkich pracowników Urzędu Gminy Ciepłowody z tematyki cyberbezpieczeństwa, zagrożeń poczty email, przepisów prawnych w kontekście normy ISO 27001 przez Audytora Wiodącego ISO 27001 lub uprawnienia równoważne w terminie do 18 września 2023 r.

INFORMACJE DODATKOWE

Serwis oprogramowania musi być realizowany przez producenta lub autoryzowanego partnera serwisowego producenta - wymagane oświadczenie Wykonawcy potwierdzające, że serwis będzie realizowany przez Producenta lub autoryzowanego partnera serwisowego producenta (należy dołączyć do oferty).