Znak postępowania: AIR.271.8.2025

Zał. nr 1C do SWZ

Część 3 - *Wzmocnienie cyberbezpieczeństwa w Gminie Pszów poprzez dostawę licencji na oprogramowanie szyfrujące pocztę elektroniczną*

OPIS PRZEDMIOTU ZAMÓWIENIA

Dostawa 60 szt. licencji na oprogramowanie do szyfrowania wiadomości email technologią end-to-end spełniającego wymagania, jak niżej:

Nazwa	**WYMAGANE MINIMALNE PARAMETRY**
Typ	Oprogramowanie do szyfrowania wiadomości email technologią end-to-end.
Zastosowanie	Zapewnienie szyfrowania end-to-end zabezpieczającego komunikację e-mailową, że tylko nadawca i odbiorca mają dostęp do treści wiadomości.
Licencja	Oprogramowanie posiada 2-letnią licencję z możliwością późniejszej kontynuacji na kolejne lata.
Ilość sztuk licencji	60 sztuk.
Okres wsparcia	Wsparcie techniczne i prawo do aktualizacji przez minimum 2 lata w tym dostęp do bazy reguł, sygnatur i zagrożeń phishing oraz bazy wycieków adresów, domen email.
Interfejs	Oprogramowanie posiada interfejs użytkownika w języku polskim.
Wsparcie techniczne	Wsparcie techniczne mailowe oraz telefoniczne w języku polskim.
Podstawowe funkcjonalności systemu	1. Oprogramowanie musi zapewnić funkcjonalność: 1.1. szyfrowanie algorytmem AES256 treści wiadomości, 1.2. szyfrowanie algorytmem AES256 załączników, 1.3. szyfrowanie algorytmem AES256 plików, 1.4. szyfrowanie algorytmem AES256 katalogów, 1.5. do odszyfrowania treści wiadomości, plików, katalogów, załączników email nie wymagany jest dodatkowy płatny lub bezpłatny dostęp do usług internetowych, chmury, hostingu lub portalu internetowego, 1.6. do odszyfrowania treści wiadomości, plików, katalogów, załączników email nie wymagane jest połączenie Internetowe, 1.7. do odszyfrowania wiadomości nie jest potrzebne wysyłanie linków do oprogramowania deszyfrującego, 1.8. do odszyfrowania treści wiadomości nie jest wymagane instalowanie dodatkowego oprogramowania deszyfrującego, 1.9. odszyfrowanie treści wiadomości, plików, katalogów, załączników email musi być możliwe na popularnych systemach operacyjnych z środowiskiem graficznym: Windows 8.1, Windows 10, Windows 11, macOS, Android od wersji 6.0, 1.10. szyfrowana zawartość wiadomości może zawierać nie tylko tekst ale również elementy graficzne takie jak: HTML, obrazki, 1.11. generowania bezpiecznego hasła (litery, cyfry, znaki) o określonej minimalnej długości dla szyfrowania, 1.12. opieczętowania każdej wysłanej wiadomość sygnaturą, która jednoznacznie wskazuje na jej oryginalność, 1.13. zabezpieczenia każdego emaila dedykowanym unikalnym hasłem, 1.14. posiadania wewnętrznej bazy haseł, która umożliwia: - export haseł do pliku, - import haseł z pliku - generowania ponownie haseł w bazie, 1.15. posiadania wewnętrznego raportu informującego administratora o szyfrowaniu email przy włączonej opcji generowania hasła dla każdej z nich, 1.16. posiadania wewnętrznego raportu z historią szyfrowanych plików i katalogów wraz z przypisanym hasłem szyfrującym, 1.17. posiadania menu kontekstowego do szybkiego wybierania szyfrowania wiadomości emailowych, plików i katalogów, 1.18. 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. 1.19. integracji z telefonem komórkowym (Android, IOS, Windows Phone) umożliwiającym wygenerowanie sms-a z hasłem i docelowym kontaktem sms-owym,

	1.20.	zabezpieczenia panelu ustawień oprogramowania poprzez hasło dostępowe,
	1.21.	wykrywania fałszywych emaili - Antiphishing,
	1.22.	wykrywania prób podszycia się pod dowolnego adresata - mechanizm ANTISPOOFING,
	1.23.	wykrywania fałszywych linków i odsyłaczy w wiadomościach emailowych,
	1.24.	wykrywanie niebezpiecznych dokumentów MS Office,
	1.25.	wykrywanie niebezpiecznych rozszerzeń plików przesyłanych przez pocztę email,
	1.26.	definiowania alarmów informujących o niebezpiecznych mailach i załącznikach,
	1.27.	współpracę z serwerem producenta oprogramowania dostarczającym bazy reguł, sygnatur, zagrożeń phishingowych. Dostęp do tej bazy wymagany jest minimum na 2 lata. Baza reguł, sygnatur i zagrożeń phishingowych powinna posiadać min. 1 500 000 wpisów. Producent musi umożliwiać wyświetlenie ilości wpisów na aktualny dzień poprzez stronę Internetową. Wpisy do bazy muszą być weryfikowane min. 2 razy w ciągu dnia,
	1.28.	alarmowanie o wybranych zagrożeniach phishingowych min. raz na miesiąc,
	1.29.	dostęp do bazy wycieków adresów i domen email. Dostęp do tej bazy wymagany jest minimum na 2 lata,
	1.30.	integrację z klientami MS Outlook i Mozilla Thunderbird oraz Mozilla Thunderbird Portable, która zapewni monitoring i wyświetlenie komunikatu dla użytkownika o wycieku adresów email wraz z decyzją czy dany email będzie szyfrowany technologią END-TO-END podczas wysłania wiadomości email,
	1.31.	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.
	2.	Licencja na użytkowanie oprogramowania musi być wieczysta i nie może być uzależniona oraz powiązana z innym oprogramowaniem do bezpieczeństwa np. antywirusy.
	3.	Oprogramowanie musi działać samodzielnie i do poprawnej jego pracy nie może wymagać innych pakietów bezpieczeństwa np. antywirusy.
	4.	Oprogramowanie musi poprawnie działać z różnymi zainstalowanymi antywirusami.
	5.	Oprogramowanie nie może wyłączać domyślnego antywirusa systemowego Windows.