**Załącznik numer 5 – załącznik po modyfikacji**

**Specyfikacja techniczna**

**Oprogramowanie do szyfrowania wiadomości email**

|  |  |
| --- | --- |
| Oprogramowanie- opis funkcjonalności | 1. Licencja na 150 użytkowników
2. Stosowanie aktualnego algorytmu szyfrującego AES256” „Oprogramowanie musi zapewnić funkcjonalność:
	1. szyfrowanie wiadomości,
	2. szyfrowanie załączników,
	3. szyfrowanie plików,
	4. szyfrowanie katalogów,
	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.
	6. do odszyfrowania wiadomości nie jest potrzebne wysyłanie linków do oprogramowania deszyfrującego.
	7. odszyfrowanie treści wiadomości, plików, katalogów, załączników email musi być możliwe na popularnych systemach operacyjnych z środowiskiem graficznym np. Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11, Android
	8. szyfrowana zawartość wiadomości może zawierać nie tylko tekst ale również elementy graficzne takie jak: HTML, obrazki
	9. generowania bezpiecznego hasła (litery, cyfry, znaki) o określonej minimalnej długości dla szyfrowania,
	10. posiadania wewnętrznej bazy haseł, która umożliwia:
		1. export haseł do pliku,
		2. import haseł z pliku
		3. generowania ponownie haseł w bazie
	11. zabezpieczenia panelu ustawień oprogramowania poprzez hasło dostępowe,
	12. wykrywania fałszywych emaili - Antiphishing,
	13. wykrywania prób podszycia się pod dowolnego adresata - mechanizm ANTISPOOFING,
	14. wykrywania fałszywych linków i odsyłaczy w wiadomościach emailowych,
	15. wykrywanie niebezpiecznych dokumentów MS Office,
	16. wykrywanie niebezpiecznych rozszerzeń plików przesyłanych przez pocztę email,
	17. definiowania alarmów informujących o niebezpiecznych mailach i załącznikach,
	18. ~~możliwość zdalnego zarządzania funkcjami szyfrowania i polityką dla poszczególnych stacji roboczych i użytkowników~~
	19. ~~Możliwość egzekwowania zasad szyfrowania, wydawania kluczy szyfrowania i ich unieważnianie, zapewniając bezpieczeństwo danych i zapobiegając utracie i wyciekowi poufnych informacji~~
	20. współpracę z serwerem producenta oprogramowania dostarczającym bazy reguł, sygnatur. Dostęp do tej bazy wymagany jest minimum na 2 lata.
	21. 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.
3. Oprogramowanie musi działać samodzielnie i do poprawnej jego pracy nie może wymagać innych pakietów bezpieczeństwa np. antywirusy.
4. Oprogramowanie nie może wyłączać domyślnego antywirusa systemowego Windows.
5. Wsparcie techniczne i prawo do aktualizacji na 2 lata. Bazy reguł, sygnatur i zagrożeń na 2 lata.
 |