Załącznik nr 2 do Zapytania ofertowego nr WO.271.4.2022 z dnia 18.05.2022

OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ)

60 licencji na oprogramowanie do szyfrowania wiadomości e-mail technologią END TO END wraz ze wsparciem technicznym i prawem do aktualizacji oprogramowania oraz baz reguł, sygnatur i zagrożeń phishing na 2 lata zgodne z poniższymi wymaganiami i funkcjonalnościami:

1. Oprogramowanie musi zapewnić funkcjonalność:
   1) szyfrowania algorytmem AES256 treści wiadomości;
   2) szyfrowania algorytmem AES256 załączników;
   3) szyfrowania algorytmem AES256 plików;
   4) szyfrowania algorytmem AES256 katalogów;
   5) do odszyfrowania treści wiadomości, plików, katalogów, załączników e-mail nie jest wymagana dodatkowa płatna lub bezpłatna licencja (oprogramowanie, usługa, chmura, hosting) lub dostęp do portalu internetowego;
   6) do odszyfrowania treści wiadomości, plików, katalogów, załączników e-mail nie jest wymagane połączenie Internetowe;
   7) odszyfrowanie treści wiadomości, plików, katalogów, załączników e-mail musi być możliwe na popularnych systemach operacyjnych ze środowiskiem graficznym: Windows, Linux, macOS, Android;
   8) generowania bezpiecznego hasła (litery, cyfry, znaki) o określonej minimalnej długości dla szyfrowania;
   9) opieczętowania każdej wysłanej wiadomość sygnaturą, która jednoznacznie wskazuje na jej oryginalność;
   10) zabezpieczenia każdego e-maila dedykowanym unikalnym hasłem;
   11) posiadania wewnętrznej bazy haseł, która umożliwia:
      a) eksport haseł do pliku,
      b) import haseł z pliku
      c) generowania ponownie haseł w bazie
   12) posiadania wewnętrznego raportu informującego administratora o szyfrowaniu e-mail przy włączonej opcji generowania hasła dla każdej z nich;
   13) posiadania wewnętrznego raportu z historią szyfrowanych plików i katalogów wraz z przypisanym hasłem szyfrującym;
   14) posiadania menu kontekstowego do szybkiego wybierania szyfrowania wiadomości e-mailowych, plików i katalogów;
   15) 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;
   16) integracji z komórką (Android, IOS, Windows Phone) umożliwiającą wygenerowanie SMS-a z hasłem i docelowym kontaktem SMS-owym;
   17) zabezpieczenia panelu ustawień oprogramowania poprzez hasło dostępowe;
   18) wykrywania fałszywych e-maili – funkcja Antiphishing;
   19) wykrywania prób podszycia się pod dowolnego adresata -mechanizm ANTISPOOFING;
   20) wykrywania fałszywych linków i odsyłaczy w wiadomościach e-mailowych;
   21) wykrywanie niebezpiecznych dokumentów przesyłanych przez pocztę e-mail;
   22) wykrywanie niebezpiecznych rozszerzeń plików przesyłanych przez pocztę e-mail,

23) definiowania alarmów informujących o niebezpiecznych mailach i załącznikach;
24) współpracę z serwerem producenta oprogramowania dostarczającym bazy reguł, sygnatur, zagrożeń phishingowych. Dostęp do tej bazy wymagany jest minimum na 2 lata;
25) współpracy z klientem Mozilla Thunderbird i Mozilla Thunderbird Portable.

2. Licencje na użytkowanie oprogramowania muszą być wieczyste i nie mogą być uzależnione oraz powiązane z innym oprogramowaniem do bezpieczeństwa np. antywirusem.
3. Oprogramowanie musi działać samodzielnie i do poprawnej jego pracy nie mogą być wymagane inne pakiety bezpieczeństwa np. antywirusy.
4. Oprogramowanie musi poprawnie działać z różnymi zainstalowanymi antywirusami.
5. Przeprowadzenie cyklicznych zdalnych szkoleń minimum raz w roku z tematyki cyberbezpieczeństwa, zagrożeń poczty e-mail, przepisów prawnych w kontekście normy ISO 27001 przez Audytora Wiodącego ISO 27001 lub uprawnienia równoważne przez 2 lata.