Załącznik nr 1

Opis przedmiotu zamówienia

I. Oprogramowanie do szyfrowania wiadomości email technologią END TO END, zdalny pulpit. Wsparcie techniczne i prawo do aktualizacji na 2 lata. Bazy reguł, sygnatur i zagrożeń phishing na 2 lata.

Oprogramowanie musi zapewnić funkcjonalność:

1. szyfrowanie algorytmem AES256 treści wiadomości,
2. szyfrowanie algorytmem AES256 załączników,
3. szyfrowanie algorytmem AES256 plików,
4. szyfrowanie algorytmem AES256 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 treści wiadomości, plików, katalogów, załączników email nie wymagane jest połączenie Internetowe.
7. do odszyfrowania wiadomości nie jest potrzebne wysyłanie linków do oprogramowania deszyfrującego.
8. do odszyfrowania treści wiadomości nie jest wymagane instalowanie dodatkowego oprogramowania deszyfrującego.
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
10. szyfrowana zawartość wiadomości może zawierać nie tylko tekst ale również elementy graficzne takie jak: HTML, obrazki
11. generowania bezpiecznego hasła (litery, cyfry, znaki) o określonej minimalnej długości dla szyfrowania,
12. opieczętowania każdej wysłanej wiadomość sygnaturą, która jednoznacznie wskazuje na jej oryginalność,
13. zabezpieczenia każdego emaila dedykowanym unikalnym hasłem,
14. posiadania wewnętrznej bazy haseł, która umożliwia:
    - export haseł do pliku,
    - import haseł z pliku
    - generowania ponownie haseł w bazie
15. posiadania wewnętrznego raportu informującego administratora o szyfrowaniu email przy włączonej opcji generowania hasła dla każdej z nich,
16. posiadania wewnętrznego raportu z historią szyfrowanych plików i katalogów wraz z przypisanym hasłem szyfrującym,
17. posiadania menu kontekstowego do szybkiego wybierania szyfrowania wiadomości email, plików i katalogów,
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.

19. integracji z komórką (Android, IOS, Windows Phone) umożliwiającą wygenerowanie sms-a z hasłem i docelowym kontaktem sms-owym,
20. zabezpieczenia panelu ustawień oprogramowania poprzez hasło dostępowe,
21. wykrywania fałszywych emaili - Antiphishing,
22. wykrywania prób podszycia się pod dowolnego adresata - mechanizm ANTISPOOFING,
23. wykrywania fałszywych linków i odsyłaczy w wiadomościach emailowych,
24. wykrywanie niebezpiecznych dokumentów MS Office,
25. wykrywanie niebezpiecznych rozszerzeń plików przesyłanych przez pocztę email,
26. definiowania alarmów informujących o niebezpiecznych mailach i załącznikach,
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,
28. alarmowanie o wybranych zagrożeniach phishingowych min. raz na miesiąc,
29. 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.
30. Licencja na użytkowanie oprogramowania musi być wieczysta i nie może być uzależniona oraz powiązana z innym oprogramowaniem do bezpieczeństwa np. antywirusy.
31. Oprogramowanie musi działać samodzielnie i do poprawnej jego pracy nie może wymagać innych pakietów bezpieczeństwa np. antywirusy.
32. Oprogramowanie musi poprawnie działać z różnymi zainstalowanymi antywirusami.
33. Oprogramowanie nie może wyłączać domyślnego antywirusa systemowego Windows.

II. Serwer z oprogramowaniem do zarządzania komputerami poprzez kontroler domeny wraz z serwerem zapasowym

Serwer główny:

1. Obudowa: RACK 1U
2. Procesor: Jeden procesor czterordzeniowy z obsługą instrukcji 64 bitowych umożliwiający osiągnięcie wyniku min. 6800 punktów w teście PassMark CPU Benchmarks dostępnym na stronie http://www.cpubenchmark.net/high_end_cpus.html. Procesor z obsługą wirtualizacji.
3. Pamięć: min. 32GB dedykowane do pracy serwerowej
4. 4 kieszenie HotSwap SATA3
5. 1 dysk systemowy o poj. min. 1TB zamontowany w kieszeni HotSwap
6. 3 dyski na dane o poj. min. 2TB zamontowane w kieszeniach HotSwap.
7. Obsługa sieci: min. 2 karty sieciowe LAN RJ45 10/100/1000 Mb/s
8. Wsparcie KVM przez LAN
9. Panel przedni chroniący kluczem dostępu do dysków
10. Czujnik otwarcia obudowy
11. Komplet szyn montażowych w zestawie
12. Gwarancja: 2 lata gwarancji producenta.

Serwer zapasowy:

1. Obudowa: RACK 1U
2. Procesor: Jeden procesor czterordzeniowy z obsługą instrukcji 64 bitowych umożliwiający

osiągnięcie wyniku min. 6800 punktów w teście PassMark CPU Benchmarks dostępnym na stronie http://www.cpubenchmark.net/high_end_cpus.html. Procesor z obsługą wirtualizacji.

3. Pamięć: min. 32GB dedykowane do pracy serwerowej
4. 4 kieszenie HotSwap SATA3
5. 1 dysk systemowy o poj. min. 1TB zamontowany w kieszeni HotSwap
6. 3 dyski na dane o poj. min. 2TB zamontowane w kieszeniach HotSwap.
7. Obsługa sieci: min. 2 karty sieciowe LAN RJ45 10/100/1000 Mb/s
8. Wsparcie KVM przez LAN
9. Panel przedni chroniący kluczem dostępu do dysków
10. Czujnik otwarcia obudowy
11. Komplet szyn montażowych w zestawie
12. Gwarancja: 2 lata gwarancji producenta.

Funkcjonalności oprogramowania:

1. Oprogramowanie dostarczone razem z serwerem musi zapewnić możliwość zarządzania systemem i konfiguracją przez przeglądarkę WEB, zapewniając funkcjonalność:
   - 1.1. interfejs obsługi serwera musi być realizowany przez najnowszą przeglądarkę internetową i być w standardzie Windows METRO,
   - 1.2. system powinien przed zalogowaniem do panelu zarządzającego informować w czasie rzeczywistym administratora o obciążeniu: całego systemu, procesora, pamięci oraz interfejsu sieciowego na dynamicznych wykresach. Wskazując myszką dane na wykresie powinny pokazywać wartość obciążenia. Informacje o obciążeniu całego systemu, procesora, pamięci oraz interfejsu sieciowego powinny być archiwizowane w serwerze i dostępne przez system raportujący dla okresów: godzinowy, dzienny, tygodniowy i miesięczny,
   - 1.3. serwer musi umożliwiać realizowanie usług (FTP, FTP z opcją szyfrowania SSL/TLS, TFTP, NFS),
   - 1.4. musi posiadać system antywirusowy,
   - 1.5. możliwość zarządzania serwerem poprzez protokół SNMP w wersji 1/2/3,
   - 1.6. musi umożliwiać dostęp administratorów przez przeglądarkę WEB,
   - 1.7. wbudowany firewall zarządzany przez przeglądarkę WEB,
   - 1.8. przed zalogowaniem administratora do interfejsu serwera WEB, powinien bez autoryzacji odczytywać parametry obciążenia serwera pokazywane na dynamicznych wykresach w przeglądarce WEB,
   - 1.9. system musi umożliwiać generowanie certyfikatów SSL przez przeglądarkę WEB,
   - 1.10. system powinien posiadać możliwość importowania zewnętrznych certyfikatów SSL przez przeglądarkę WEB,
2. W zakresie obsługi domeny, dostarczone oprogramowanie musi zapewnić funkcjonalność:
   - 2.1. zarządzania do min. 50 użytkowników, grup,
   - 2.2. zarządzanie do min. 50 komputerów,
   - 2.3. zarządzanie do min. 50 urządzeń,
   - 2.4. zarządzania polisami GPO,
   - 2.5. obsługę profili użytkowników oraz profili mobilnych,
   - 2.6. obsługę do min. 85 jednoczesnych podłączeń do serwera domeny,
   - 2.7. zarządzania użytkownikami, grupami, komputerami podpiętymi do kontrolera domenowego przez przeglądarkę WEB,
   - 2.8. możliwość tworzenia użytkowników i grup w kontrolerze domeny przez przeglądarkę

WEB,

2.9. nadawania haseł dla użytkowników w kontrolerze domeny przez przeglądarkę WEB,
2.10. wyszukiwania po nazwie użytkownika, grupy i komputera przez przeglądarkę WEB,
2.11. listy użytkowników, którym wygasła ważność konta dostępna w przeglądarce WEB,
2.12. listy zablokowanych kont w kontrolerze domeny dostępna w przeglądarce WEB,
2.13. wszystkie operacje zakładania i modyfikacji oraz usuwania kont, grup, komputerów w kontrolerze domenowym przez przeglądarkę WEB powinny być raportowane w centralnym repozytorium systemowym,
2.14. możliwość wyświetlenia oraz akceptowania polityki bezpieczeństwa przed zalogowaniem użytkowników do serwera domenowego,
2.15. administrator podłączający się do kontrolera domeny musi mieć możliwość autoryzacji i logowania się do serwera domenowego przy pomocy jednego dostarczonego do serwera urządzenia sprzętowego token wykorzystujący port USB,
2.16. Administrator zanim dokona logowania do kontrolera domeny przy pomocy urządzenia sprzętowego token może wyświetlić wewnętrzną politykę bezpieczeństwa informacji Urzędu. Administrator Bezpieczeństwa Informacji ma możliwość zarządzania treścią, która jest wyświetlana i akceptowana w procesie logowania do systemu operacyjnego lub kontrolera domeny.
2.17. Administrator wyciągając urządzenie autoryzacyjne token z portu USB będzie miał blokowany system operacyjny.
2.18. Zastosowane urządzenie sprzętowe token powinno umożliwiać przypisywanie konkretnego komputera (wraz z logowaniem administrator do kontrolera domeny) do urządzenia sprzętowego token,
2.19. Pamięć urządzenia sprzętowego token musi umożliwiać zdefiniowania do 20 uwierzytelnień do systemu operacyjnego i kontrolera domeny,
2.20. Urządzenie sprzętowe token musi wykorzystywać tylko jeden port USB w wersji 2.0 lub 3.0,
2.21. Urządzenie sprzętowe token w celu uwierzytelnienia musi wymagać stosowania min. 6 znakowego PIN-u,
2.22. współpracy z klientami Windows 7,8,8.1,10,11 w wersji professional.

3. Licencja kontrolera domeny dla zamawianego serwera głównego i zapasowego musi umożliwiać:
   3.1. łatwe przenoszenie i uruchomienie kontrolera domeny pomiędzy zamawianym serwerem głównym i zapasowym,
   3.2. łatwe uruchomienie kontrolera domeny w trybie awaryjnym (w ograniczonej funkcjonalności) na dowolnym serwerze posiadanego przez zamawiającego na czas naprawy zamówionego serwera głównego lub zapasowego.
4. Oprogramowanie musi umożliwiać wirtualizację dowolnych systemów operacyjnych i musi realizować:
   4.1. obsługę minimum cztero-rdzeniowego procesora,
   4.2. obsługę minimum 32GB RAM-u,
   4.3. obsługę vmware VMDK,
   4.4. obsługę minimum 10 instancji środowisk wirtualnych,
   4.5. zapis stanu maszyny wirtualnej tzw. snapshot,
   4.6. kopii stanu maszyny wirtualnej,
   4.7. emulacji wielu urządzeń np. kart sieciowych, kontrolerów SAS,
   4.8. dynamicznej alokacji pamięci na kontener danych

4.9. współpracy z kontrolerami SATA, SCSI,
4.10. tryb pracy sieciowej min NAT, tunel UD, Bridge oraz wielu interfejsów sieci,
4.11. zarządzanie poprzez przeglądarkę WEB,
4.12. archiwizacje uruchomionych maszyn wirtualnych.

5. Oprogramowanie musi również umożliwiać migrację użytkowników lokalnych do serwera domenowego działającego w systemie Windows Vista,7,8,8.1,10,11 w wersji 32 i 64 bity w wersji professional z licencją na użytkowanie bezterminową umożliwiając przenoszenie do 85 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.

III. 50 szt. urządzeń autoryzacyjnych do systemu operacyjnego lub serwera kontrolera domeny sprzętowy TOKEN. Wsparcie techniczne i prawo do aktualizacji na 2 lata.

Wymagane funkcjonalności:

1. Uwierzytelnienie użytkowników do systemu operacyjnego lub serwera kontrolera domeny przy pomocy dedykowanego urządzenia sprzętowego , monitorowania logów uwzględniające:
   - logowanie do systemu (kto, kiedy)
   - wylogowanie/zablokowanie systemu (kto, kiedy)
2. Użytkownik zanim dokona logowania do systemu operacyjnego przy pomocy urządzenia sprzętowego może wyświetlić zdefiniowaną przez administratora wewnętrzną PBI. Administrator Bezpieczeństwa Informacji ma możliwość zarządzania treścią, która jest wyświetlana i akceptowana w procesie logowania do systemu operacyjnego lub kontrolera domeny.
3. Użytkownik, który opuszcza stanowisko pracy będzie miał blokowany system operacyjny przez urządzenie sprzętowe.
4. Pamięć urządzenia sprzętowego musi umożliwiać zdefiniowania do 20 uwierzytelnień do systemu operacyjnego.
5. Możliwość autoryzacji do systemu operacyjnego lub kontrolera domeny dedykowanym PIN-em.
6. Możliwość nadawania indywidualnego kodu PIN do urządzenia autoryzacyjnego TOKEN dla konta użytkownika w systemie operacyjnym lub kontrolerze domeny.
7. Zastosowane urządzenie sprzętowe powinno umożliwiać przypisywanie konkretnego komputera do urządzenia sprzętowego.
8. Narzędzie sprzętowe musi wykorzystywać tylko jeden port USB w wersji 2.0 lub 3.0
9. Urządzenie sprzętowe w celu uwierzytelnienia musi wymagać stosowania min. 6 znakowego PIN-u,
10. Współpraca z klientami Windows 7, 8, 8.1, 10, 11
11. Wdrożenie i szkolenie z oprogramowania i urządzeń autoryzacyjnych musi być realizowane przez certyfikowanych inżynierów z uprawnieniami wystawionymi przez producenta.