Zapytanie o informację (RFI)

I. Przedmiot i cel Zapytania o informację

1. Zakład Ubezpieczeń Społecznych rozważa dokonanie zakupu polegającego na **Zakup wsparcia dla posiadanego przez Zamawiającego systemu antywirusowego opartego na oprogramowaniu firmy Symantec albo dostarczenie i wdrożenie rozwiązania równoważnego**. Szczegółowy opis zapytania stanowi **Załącznik nr 1** do Zapytania o informację.
2. Celem niniejszego Zapytania o informację jest pozyskanie przez Zakład Ubezpieczeń Społecznych od podmiotów zajmujących się profesjonalnie określonym zakresem, danych dotyczących szacunkowego kosztu realizacji.

II. Ogólne informacje o charakterze formalnym

1. Niniejsze Zapytanie o informację **nie stanowi oferty zawarcia umowy w rozumieniu przepisów *ustawy z dnia 23 kwietnia 1964 r.- Kodeks cywilny*.** Udzielenie odpowiedzi na niniejsze Zapytanie o informację nie będzie uprawniało do występowania z jakimikolwiek roszczeniami w stosunku do Zakładu Ubezpieczeń Społecznych.
2. Niniejsze Zapytanie o informację **nie jest elementem jakiegokolwiek postępowania o udzielenie zamówienia, w rozumieniu *ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych***, jak również nie jest elementem jakiegokolwiek procesu zakupowego prowadzonego w oparciu o wewnętrzne regulacje Zakładu Ubezpieczeń Społecznych.
3. Złożenie odpowiedzi na niniejsze Zapytanie o informację jest jednoznaczne z wyrażeniem zgody przez podmiot składający taką odpowiedź na nieodpłatne wykorzystanie przez Zakład Ubezpieczeń Społecznych wszystkich lub części przekazanych informacji.

III. Termin i sposób złożenia odpowiedzi na Zapytanie o informację

1. Odpowiedź na Zapytanie o informację należy przygotować w oparciu o formularz stanowiący **Załącznik nr 2** do Zapytania o informację.
2. W przypadku, gdy informacje zawarte w odpowiedzi na Zapytanie o informację stanowią tajemnicę przedsiębiorstwa w rozumieniu przepisów ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji, podmiot składający taką odpowiedź winien to wyraźnie zastrzec w odpowiedzi. Brak przedmiotowego zastrzeżenia, Zakład Ubezpieczeń Społecznych będzie traktował przekazane informacje jako informacje, które nie stanowią tajemnicy przedsiębiorstwa.
3. **W przypadku zaproponowania rozwiązania równoważnego, należy przedstawić dodatkowe informacje tj.: nazwa oprogramowania, producenta, sposób licencjonowania/subskrypcji.**
4. Odpowiedź na Zapytanie o informację należy przesłać w terminie do **12 lipca 2018 r. do godziny 12:00** na adres e-mail: **rfi-urzadzenia-windows@zus.pl**

Załącznik nr 1 - Szczegółowy opis Zapytania o informację

I. Przedmiot zapytania został podzielony na dwa warianty

Wariant I – 36 miesięczna usługa wsparcia dla systemu antywirusowego (dalej: „System") opartego na oprogramowaniu firmy Symantec będącego w użytkowaniu przez Zamawiającego. Szczegółowy opis przedmiotu zapytania został zawarty **w Rozdziale II.**

Wariant II – dostarczenie i wdrożenie rozwiązania równoważnego z zapewnieniem 36 miesięcznego wsparcia. Szczegółowy opis przedmiotu zapytania został zawarty **w Rozdziale III.**

W zakres Wariantu II wchodzą :

Wymagania rozwiązania równoważnego dotyczące serwerów oraz poczty:

1. Antywirus
2. Firewall
3. Ochrona przed włamaniami
4. Ochrona systemu operacyjnego
5. Ochrona integralności systemu
6. Architektura
7. Moduł centralnego zarządzania
8. Dystrybucja elementów systemu ochrony
9. Ochrona środowisk wirtualnych
10. Ochrona systemu poczty elektronicznej
    1) Ochrona systemu pocztowego na styku z Internetem (bramka pocztowa)
    2) ochrona serwerów Exchange:

Wymagania rozwiązania równoważnego dotyczące Stacji roboczych

1. Antywirus
2. Firewall
3. Ochrona przed włamaniami
4. Ochrona systemu operacyjnego
5. Ochrona integralności systemu
6. Architektura
7. Moduł centralnego zarządzania
8. Dystrybucja elementów systemu ochrony
9. Ochrona środowisk wirtualnych
10. Warunki wsparcia

II. **Wariant I** - Przedmiotem zapytania jest usługa wsparcia dla systemu antywirusowego (dalej: „System") opartego na oprogramowaniu firmy Symantec będącego w użytkowaniu przez Zamawiającego.

Usługa wsparcia świadczona będzie w okresie 3 lat, nie wcześniej niż od dnia 08.09.2018.

Oprogramowanie firmy Symantec posiadane przez ZUS:

- Symantec Endpoint Protection - 2000 serwerów
- minimum 52.000 stacji roboczych
- Symantec Mail Security for Microsoft Exchange - 50000 skrzynek
- Symantec Mesaging Gateway - 2 x Symantec 8360:
  - Symantec Antyspam
  - Symantec Antywirus
  - Symantec Premium Content Control
  - Software Updates

1. Wykonawca w dniu zawarcia umowy przekaże Zamawiającemu wykaz pracowników upoważnionych do rozwiązywania problemów i współpracy z Zamawiającym w celu realizacji umowy. Wszystkie ww. osoby winny komunikować się w zakresie koordynacji i realizacji przedmiotu zamówienia z Zamawiającym w języku polskim (w mowie i piśmie). W przypadku osób nie władających językiem polskim Wykonawca zobowiązany jest zapewnić tłumacza na język polski.
2. Wykonawca zapewni aktualizacje baz sygnatur wirusów, oprogramowania, lub inne rozwiązanie stosowane przez producenta oprogramowania gwarantujące skuteczną ochronę antywirusową, przez cały okres obowiązywania umowy. Wykonawca zapewni pełne wsparcie dla dwóch fizycznych urządzeń Symantec 8360.
3. Wykonawca w ramach usługi wsparcia zagwarantuje czas pracy inżyniera do dyspozycji Zamawiającego w ilości 100 godzin przez 3 lata, od poniedziałku do piątku, z wyłączeniem świąt ustawowych, w godzinach w godz. 8.00 – 16.00, od momentu rozpoczęcia świadczenia usług.
   Po każdorazowym zakończeniu pracy inżyniera będzie sporządzany protokół z wykorzystania godzin.
   Ponadto Wykonawca, w ramach wsparcia, zapewni Zamawiającemu e-mail`owe i telefoniczne konsultacje w zakresie oprogramowania Symantec oraz jego współpracy z platformami, na których jest osadzone, od poniedziałku do piątku, z wyłączeniem świąt ustawowych, w godzinach w godz. 8.00 – 16.00.
4. Wykonawca gwarantuje świadczenie usługi wsparcia i możliwość zgłaszania problemów poprzez HP Service Manager oraz drogą telefoniczną, faksową lub elektroniczną, 7 dni w tygodniu i 24 godz. na dobę. Obsługę trudnych do zdiagnozowania i usunięcia problemów, na miejscu u Zamawiającego. Usługa wsparcia nie pomniejsza ilości godzin z czasu pracy inżyniera.

5. W przypadku awarii oprogramowania Wykonawca zapewni czas naprawy lub zastosowanie obejścia oraz przywrócenia pełnej funkcjonalności, w przeciągu 24 godzin roboczych (dni od poniedziałku do piątku, z wyłączeniem świąt ustawowych, w godzinach w godz. 8.00 – 16.00.) od chwili zgłoszenia.

   W przypadku urządzeń fizycznych Symantec 8360 wykonawca zapewni gwarantowany czas naprawy w przeciągu 24 godzin roboczych (dni od poniedziałku do piątku, z wyłączeniem świąt ustawowych oraz dni wolnych Zamawiającego, w godzinach w godz. 8.00 – 16.00), od chwili zgłoszenia awarii.

   W przypadku, gdy naprawa nie może być wykonana w terminie 24 godzin od momentu zgłoszenia, Wykonawca dostarczy, uruchomi i skonfiguruje urządzenie zastępcze wyprodukowane nie wcześniej niż wymieniane, wykonane w tej samej technologii, o nie gorszych parametrach technicznych i o nie większych kosztach eksploatacji, przez cały okres użytkowania sprzętu przez Zamawiającego. Urządzenie zastępcze nie będzie powodowało wzrostu kosztów utrzymania pozostałych urządzeń posiadanych przez Zamawiającego. Koszty dostawy i wymiany urządzenia ponosi Wykonawca. Urządzenie zastępcze będzie uruchomione na okres nie dłuższy niż 60 dni. Po tym terminie Wykonawca jest zobowiązany do dostarczenia naprawionego sprzętu. W przypadku, gdy Wykonawca nie zwróci naprawianego urządzenia w powyższym terminie lub umowa wygaśnie przed upływem 60 dni od dostarczenia urządzenia zastępczego urządzenie zastępcze przechodzi na własność Zamawiającego;

6. W ramach wsparcia Wykonawca będzie dokonywał comiesięcznych weryfikacji poprawności działania Systemu w siedzibie Zamawiającego, świadczył pomoc przy określaniu jego optymalnej konfiguracji oraz współpracy z innym, używanym w ZUS oprogramowaniem firmy Microsoft. Weryfikacja poprawności działania Systemu powinna być wykonywana raz w miesiącu, przez okres 3 lat, od momentu rozpoczęcia świadczenia usług, w terminie do 10 dnia każdego miesiąca.

   Comiesięczna weryfikacja powinna co najmniej obejmować :

   a. Analizę problemów wynikających z raportu poprzedniego,
   b. Wykaz wykonanych prac podczas wizyty,
   c. Raport stanu definicji wirusów,
   d. Zestawienie niezaktualizowanych klientów SEP z poprzedniego i bieżącego raportu,
   e. Stan definicji Symantec Mail Security,

f. Stan definicji Symantec Message Gateway,

g. Zestawienie wersji komponentów oprogramowania dostępnego w ramach aktualizacji z wersjami używanymi przez Zamawiającego,

h. Zalecenia naprawcze dotyczące wykrytych nieprawidłowości,

i. Ewentualne sugestie zmian konfiguracji ochrony przed złośliwym oprogramowaniem mające na celu zwiększenie bezpieczeństwa.

Po przeprowadzeniu comiesięcznej weryfikacji poprawności działania systemu sporządzony zostanie protokół. Protokół zostanie podpisany przez przedstawicieli Wykonawcy i Zamawiającego.

7. Usługa wsparcia świadczona przez Wykonawcę będzie realizowana w Centrali ZUS, Warszawa.

III. **Wariant II** – Przedmiotem zapytania jest dostarczenie i wdrożenie rozwiązania równoważnego z zapewnieniem 36 miesięcznego wsparcia.

Rozwiązanie musi spełniać następujące warunki dla serwerów, poczty elektronicznej oraz stacji roboczych.

1. Oferta musi obejmować zaprojektowanie i wdrożenie w siedzibie Zamawiającego systemu ochrony przed wszelkim szkodliwym oprogramowaniem (w tym wirusami, spamem, oprogramowaniem np. typu malware, adware, spyware, rootkit itp.) dla:
   - minimum 2.000 serwerów
   - poczty elektronicznej (minimum 50.000 skrzynek użytkowników)
   - minimum 52.000 stacji roboczych

   z prawem bezterminowego korzystania z dostarczonego rozwiązania.

2. Koszty zaoferowanego rozwiązania równoważnego powinny uwzględniać wykonanie migracji obecnie istniejącego systemu na nowy (wraz z przeniesieniem konfiguracji) i muszą obejmować:
   a. przygotowanie projektu wdrożenia, harmonogramu uwzględniającego instruktarze/warsztaty, określającego końcowy termin realizacji zamówienia. Zakończenie wdrożenia, uruchomienie ochrony na stacjach i serwerach oraz przygotowanie dokumentacji musi nastąpić w ciągu maksymalnie 2 miesięcy od dnia podpisania umowy,
   b. przygotowanie szczegółowych procedur opisujących czynności niezbędne do wykonania podczas wdrożenia,
   c. pełne wdrożenie rozwiązania przez wykonawcę. Przez wdrożenie rozumiemy przeniesienie obecnego rozwiązania na nowe, w tym:
      - Instalacja i konfiguracja serwerów zarządzających oraz integracja z domeną „zus.ad”,
      - Przeniesienie kont administratorów do nowego rozwiązania, wraz z odpowiednimi uprawnieniami,
      - Przeniesienie konfiguracji środowiska z uwzględnieniem obecnego podziału na kontenery, wraz odpowiednio przypisanymi uprawnieniami, regułami i wykluczeniami, dla poszczególnych grup serwerów i stacji roboczych,
      - Uruchomienie rozwiązania antyspamowego, integracja z domeną „zus.ad”, przeniesienie konfiguracji z obecnego rozwiązania antyspamowego na nowe, z zachowaniem obecnej konfiguracji sieciowej (również adresów IP) wraz z kontami administratorów, ich uprawnieniami, niezbędnymi regułami antyspamowymi i wyjątkami stworzonymi na potrzeby ZUS , w tym:
        - lokalnych polityk reputacji,
        - lokalnych polityk spamu,

  - lokalnych polityk filtrowania kontentu maila (na podstawie header, body, attachement),
  - mechanizmów rozpoznania nadawcy (SPF,DKIM,DMARC),
  - zainstalowanych i obsługiwanych certyfikatów,
  - szyfrowania TLS dla wybranych domen,
- Uruchomienie ochrony dla poczty elektronicznej na Serwerach z MS Exchange wraz z przeniesieniem dotychczasowej konfiguracji,
- Uruchomienie ochrony na serwerach w Centrali i w Oddziałach,
- Uruchomienie ochrony na stacjach roboczych w Centrali i w Oddziałach,

d. przygotowanie szczegółowej dokumentacji powykonawczej,
e. przygotowanie procedur opisujących okresowe czynności administracyjne (np. dotyczące uruchomienia ochrony na nowym serwerze, aktualizacji komponentów ochrony, przygotowania uniwersalnego obrazu systemu zawierającego preinstalowane komponenty ochrony,
f. przygotowanie procedur awaryjnych (tj. odzyskanie środowiska po awarii, przywrócenie wcześniejszej konfiguracji),
g. przygotowanie końcowego raportu określającego liczbę i stan komponentów rozwiązania,
h. przygotowanie procedur instalacji, konfiguracji i aktualizacji sygnatur dla serwerów autonomicznych (z dostępem i bez dostępu do internetu),
i. dostarczenie dokumentu potwierdzającego prawo do aktualizowania dla dostarczonego systemu przez okres trwania umowy oraz do bezterminowego korzystania z systemu ochrony,
j. koszty instruktarzy/warsztatów w języku polskim z dostarczonego rozwiązania dla 35 administratorów serwerów oraz 18 administratorów stacji roboczych, wraz z przejazdem i zakwaterowaniem i wyżywieniem.

3. Instruktarze/warsztaty dla administratorów powinny spełniać następujące warunki:
   a. Instruktarze/warsztaty dla administratorów systemu mają być przeprowadzone nie wcześniej niż po zakończeniu wdrożenia,
   b. mają odbyć się w siedzibie lub w jednym z ośrodków szkoleniowych Zamawiającego,
   c. zakres warsztatów powinien obejmować zagadnienia dotyczące funkcjonalności systemu, a także administracji i eksploatacji wdrożonego rozwiązania,
   d. minimum 5-dniowe (40 godzin) warsztaty dla 35 administratorów serwerów oraz 18 administratorów stacji roboczych (serwerów, systemu pocztowego, stacji roboczych i pozostałych elementów ochrony t.j np. antyspam),
   e. Instruktarze/warsztaty muszą zostać zakończone w ciągu 1 miesiąca od dnia po zakończonym wdrożeniu,

f. Ewentualne koszty, związane z dojazdem, zakwaterowaniem oraz wyżywieniem administratorów ponosi Zamawiający.

4. Przejście na nowe rozwiązanie nie może spowodować przerwy w funkcjonowaniu środowiska.

Oferowane rozwiązanie równoważne powinno spełniać poniższe minimalne wymagania:

1. pochodzić od jednego producenta i stanowić kompletne rozwiązanie ochrony przed szkodliwym oprogramowaniem dla systemów operacyjnych serwerów oraz systemu poczty elektronicznej
2. umożliwiać centralne śledzenie i zarządzanie ochroną całego przedsiębiorstwa, zarządzanie administratorami systemu ochrony przed szkodliwym oprogramowaniem, śledzenie działań administratorów, a także dystrybucję konfiguracji, aktualizacji i baz wirusów poprzez sieć teletransmisyjną.
3. umożliwiać administrowanie ochroną przed szkodliwym oprogramowaniem na wolnostojących serwerach łączących się z internetem.
4. umożliwiać instalację i okresową aktualizację dostarczonego rozwiązania oraz baz sygnatur ochrony na autonomicznych serwerach nie posiadających dostępu do Internetu.

System antywirusowy powinien wspierać następujące platformy systemowe będące w posiadaniu Zamawiającego:

- Windows Server 2008 (32-bitowy, 64-bitowy) i nowsze,
- MS Exchange 2010 i nowsze,
- VMware 5.5 i nowsze.
- Windows 10 (32-bitowy, 64-bitowy),
- Windows 8.1 (32-bitowy, 64-bitowy),
- Windows 7 (32-bitowy, 64-bitowy),

Ponadto w poszczególnych zakresach oferowane rozwiązanie dla <u>serwerów oraz poczty</u> powinno spełniać poniższe minimalne wymagania:

1. Antywirus:

1) Usuwanie wirusów, makrowirusów, robaków internetowych oraz koni trojańskich (oraz wirusów i robaków z plików skompresowanych oraz samo rozpakowujących się) lub kasowanie zainfekowanych plików. Ochrona przed oprogramowaniem typu „spyware" i „adware", włącznie z usuwaniem zmian wprowadzonych do systemu przez szkodliwe oprogramowanie.
2) Wykrywanie wirusów, makro-wirusów, robaków internetowych, koni trojańskich, spyware, adware i dialerów ma być realizowane w pojedynczym systemie skanującym.
3) Określanie obciążenia CPU dla zadań skanowania zaplanowanego oraz skanowania na żądanie.

4) Skanowanie plików pobranych z Internetu wraz ze skryptami umieszczonymi w sieci internet oraz plików skompresowanych.
5) Zapewnienie stałej ochrony wszystkich zapisywanych, odczytywanych, a także uruchamianych plików przez mechanizm skanujący pracujący w tle wraz z metodą heurystyczną wyszukiwania wirusów (na życzenie); pliki te mogą być skanowane:
   a) Na dyskach twardych,
   b) W boot sektorach,
   c) Na płytach CD/DVD,
   d) Na zewnętrznych dyskach twardych (np. podłączonych przez port USB).
6) Możliwość samodzielnego pobierania aktualizacji z Internetu do serwera.
7) Możliwość zablokowania funkcji zmiany konfiguracji klienta lub ukrycie interfejsu użytkownika klienta.
8) Scentralizowaną obsługę wirusów polegającą na przekazywaniu nieodwracalnie zainfekowanych plików do bezpiecznego miejsca w postaci centralnej kwarantanny na centralnym serwerze, w celu przeprowadzenia dalszych badań.
9) Wbudowana w dostarczone rozwiązanie funkcja do wysyłania podejrzanych lub zainfekowanych nowymi wirusami plików do producenta w celu uzyskania szczepionek.
10) Wyszukiwanie i usuwanie wirusów w plikach skompresowanych (także zagnieżdżonych wewnątrz innych plików skompresowanych), w szczególności w plikach typu ZIP, GNU, LZH/LHA, BinHex, HTTP, ARJ, RAR, MIME/UU, TAR, kontenerach CAB, UUE, Rich Text Format, ArcManager, MS-TNEF.
11) Aktualizacja definicji wirusów nie może wymagać zatrzymania procesu skanowania na jakimkolwiek systemie.
12) Mikrodefinicje wirusów - przyrostowe, scentralizowane aktualizowanie klientów jedynie o nowe definicje wirusów i mechanizmy skanujące.
13) Możliwość cofnięcia procesu aktualizacji definicji wirusów i mechanizmów skanujących – powrót do poprzedniego zastawu definicji wirusów bez konieczności reinstalacji komponentów systemu, systemu operacyjnego czy też restartu serwerów.
14) Możliwość natychmiastowego wymuszenia aktualizacji definicji wirusów na serwerach.
15) Aktualizacja bazy definicji wirusów oraz mechanizmów skanujących, co najmniej 1 raz dziennie.
16) Możliwość aktualizacji bazy definicji wirusów średnio, co 1 godzinę.
17) Heurystyczna technologia do wykrywania nowych, nieznanych wirusów.
18) Moduł analizy zachowań aplikacji do wykrywania nowych, nieznanych zagrożeń typu robak internetowy, koń trojański, keylogger.
19) Automatyczna rejestracja w dzienniku zdarzeń wszelkich nieautoryzowanych prób zmian rejestru dokonywanych przez użytkownika.
20) Automatyczne ponowne uruchomianie skanowania w czasie rzeczywistym, jeśli zostało wyłączone przez użytkownika mającego odpowiednie uprawnienia na z góry określony czas.
21) Automatyczne wymuszanie na kliencie programu pobrania zaktualizowanych definicji wirusów, jeśli aktualnie przechowywane pliki są przestarzałe.
22) Aktualizacje definicji wirusów muszą posiadać podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione.
23) Skanowanie poczty klienckiej (na komputerze klienckim).

2. Firewall powinien zapewniać:

1) Pełne zabezpieczenie serwerów przed atakami hakerów oraz nieautoryzowanymi próbami dostępu do komputerów i skanowaniem portów.
2) możliwość monitorowania i kontroli, jakie aplikacje łączą się poprzez interfejsy sieciowe.
3) Możliwość definiowania przez Administratora połączenia, które serwer może inicjować i odbierać.
4) Możliwość konfigurowania dostępu serwera do protokołów rozszerzonych innych niż ICMP,UDP czy TCP np.: IGMP, GRE, OSPFIGP, L2TP, Lite-UDP.
5) Aktualizacje definicji sygnatur ataków posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione.
6) Możliwość zdefiniowania indywidualnych komputerów lub całych zakresów adresów IP, które są traktowane, jako: całkowicie bezpieczne lub niebezpieczne.
7) Możliwość wykrywania próby wyszukiwania przez hakerów luk w zabezpieczeniach systemu w celu przejęcia nad nim kontroli.
8) Konfigurację zezwalanego i zabronionego ruchu, która ma się odbywać w oparciu o takie informacje jak: interfejs sieciowy, protokół, host docelowy, aplikacja, godzina komunikacji.
9) Konfigurację serwera, która ma się odbywać poprzez określenie: Adresu MAC, numeru IP, zakresu numerów IP, wskazanie podsieci, nazwy DNS (FQDN) lub domeny DNS.
10) Możliwość nagrywania komunikacji spełniającej wskazane wymagania.
11) Konfigurowalną funkcjonalność powiadamiania użytkownika o zablokowanych aplikacjach. Ma istnieć możliwość dodania własnego komunikatu.
12) W przypadku wykrycia zdefiniowanego ruchu, firewall ma umożliwiać wysyłanie wiadomości do administratora.
13) Uniemożliwianie określenia systemu operacyjnego i rodzaju przeglądarki internetowej serwera przez serwery www.
14) Uniemożliwienie określenia systemu operacyjnego poprzez analizę pakietów sieciowych wysyłanych przez serwer.
15) Uniemożliwienie przejęcia sesji poprzez losowo generowane numery sekwencji TCP.
16) Domyślne reguły zezwalające na ruch DHCP, DNS.

3. Ochrona przed włamaniami:

1) Ma zawierać bibliotekę ataków i podatności (sygnatur) stosowanych przez produkt, dostarczoną przez Producenta rozwiązania. Administrator ma mieć możliwość uaktualniania tej biblioteki poprzez konsolę zarządzającą.
2) Ma mieć możliwość tworzenia własnych wzorców włamań (sygnatur), korzystając z semantyki Snort'a.
3) Ma umożliwiać wykrywanie skanowania portów.
4) Ma umożliwiać ochronę przed atakami typu odmowa usług (Denial of Service).
5) Ma umożliwiać blokowanie komunikacji z serwerami z podmienionymi MAC adresami (spoofed MAC).
6) Ma umożliwiać wykrywanie trojanów i generowanego przez nie ruchu.
7) Ma umożliwiać wykrywanie prób nawiązania komunikacji za pośrednictwem zaufanych aplikacji, przez inne oprogramowanie.

8) Ma umożliwiać blokowanie komunikacji z węzłami uznanymi za wrogie na zdefiniowany przez administratora czas. Ma istnieć możliwość definiowania wyjątków.

4. Ochrona systemu operacyjnego:

1) Ma umożliwiać uruchamianie i blokowanie wskazanych aplikacji.
2) Ma umożliwiać ładownie modułów lub bibliotek DLL.
3) Ma umożliwiać kontrolę odczytywania i zapisywania na systemie plików przez wskazane aplikacje.
4) Ma umożliwiać rozróżnianie aplikacji poprzez nazwę i sygnaturę cyfrową.
5) Ma umożliwiać blokowanie wskazanego typu urządzeń przed dostępem użytkownika – urządzenia muszą być identyfikowane po ich numerze seryjnym.
6) Ma umożliwiać kontrolę dostępu do rejestru systemowego.
7) Ma umożliwiać logowanie plików wgrywanych na urządzenia zewnętrzne.
8) Polityki ochrony mają mieć możliwość pracy w dwóch trybach, testowym i produkcyjnym. W trybie testowym aplikacje i urządzenia nie są blokowane, ale jest tworzony wpis w logu.

5. Ochrona integralności systemu:

1) musi umożliwiać wykonywanie szerokiego zakresu testów integralności systemu pod kątem zgodności z polityką bezpieczeństwa, w tym: programów antywirusowych, poprawek firmy Microsoft, dodatków Service Pack firmy Microsoft, zapór ogniowych.
2) Testy integralności mają być przeprowadzane cyklicznie, co zdefiniowany okres czasu.
3) Powyższe szablony muszą być automatycznie aktualizowane ze strony producenta.
4) Dostarczone rozwiązanie musi umożliwiać wykonanie niestandardowego testu integralności komputera, posiadać zaawansowaną składnie If…Then…Else.
5) W przypadku niestandardowego testu integralności musi istnieć dostępność następujących testów:
   a) Wpisy rejestru systemu operacyjnego - istnienie, określona wartość, inne,
   b) Pliki - istnienie, data, rozmiar, suma kontrolna,
   c) Wiek, data, rozmiar pliku sygnatury systemu antywirusowego,
   d) Zainstalowane poprawki,
   e) Uruchomiony proces, wersja systemu operacyjnego,
   f) Własny skrypt VisualBasic, wsh, itp.
   g) Własna aplikacja,
6) W przypadku niezgodności serwera z testem integralności, musi być możliwość ustawienia akcji naprawczej na poziomie pojedynczego testu. Jako możliwe operacje do wykonania musi istnieć możliwość:
   a) Uruchamianie dowolnego/własnego skryptu lub programu,
   b) Logowanie zdarzenia,
   c) Ukazanie okienka z wiadomością,
   d) Pobieranie oraz uruchamianie instalacji,
7) Ma istnieć możliwość wskazania czasu oczekiwania na wykonanie akcji naprawczych.
8) Możliwość wymuszenia instalacji dowolnej aplikacji.

9) W wypadku niezgodności własnego systemu, dostarczone rozwiązanie musi umożliwić zaaplikowanie dowolnego innego zestawu konfiguracji, w szczególności polityki firewallowej (zdefiniowanej bardzo restrykcyjnie), polityki antywirusowej, polityki pobierania aktualizacji, polityki kontroli uruchamianych aplikacji i polityki kontroli urządzeń.
10) Musi być możliwe, nieuwzględnianie wyniku poszczególnego testu na wynik końcowy integralności komputera.
11) Musi istnieć możliwość stwierdzenia, że na komputerze znaleziono zagrożenie i nie można było takiego zagrożenia usunąć – na ten czas komputer powinien znaleźć się w kwarantannie.

6. Architektura:

1) Rozwiązanie ma mieć architekturę trójwarstwową. Węzły mają być zarządzane przez serwery, a konfiguracja rozwiązania ma być zapewniona poprzez graficzną konsolę administratora.
2) Rozwiązanie ma zapewniać wysoką skalowalność i odporność na awarie.
3) Komunikacja pomiędzy agentami i serwerem ma być szyfrowana.
4) Numery portów używane do komunikacji mają mieć możliwość konfiguracji przez użytkownika końcowego.
5) Agent ma się przełączać do innego serwera zarządzającego w przypadku niedostępności przypisanego serwera.
6) Serwery zarządzające muszą móc replikować pomiędzy sobą informacje o agentach, ich konfiguracji oraz logi. Musi istnieć możliwość zdefiniowania kierunku replikacji logów (jednostronna lub dwustronna).
7) Musi istnieć możliwość zdefiniowania dowolnego klienta, jako lokalnego dostarczyciela aktualizacji – możliwość konfiguracji ilości przetrzymywanych aktualizacji, zajętości na dysku oraz konfiguracji prędkości ich pobierania z serwera zarządzającego.
8) Definiowanie lokalnego repozytorium musi zawierać warunki, jakie muszą być zachowane by dany komputer mógł stać się lokalnym repozytorium – warunkami muszą być przynajmniej: wersja systemu operacyjnego, adres komputera, nazwa komputera (z możliwością podania jej ze znakami specjalnymi, np.: komputer*), określonego wpisu w rejestrze.

7. Moduł centralnego zarządzania:

1) Centralna instalacja, konfiguracja w czasie rzeczywistym, zarządzanie, raportowanie i administrowanie dostarczonym rozwiązaniem z graficznej konsoli.
2) Centralna aktualizacja ochrony antywirusowej, zapory ogniowej i systemu wykrywania włamań przez administratora.
3) Produkt ma wykrywać i raportować nieautoryzowane zmiany w konfiguracji produktu na serwerze. Ma istnieć możliwość blokowania takich zmian.
4) Produkt ma zapewniać zarządzanie poprzez graficzną konsolę. Dostęp do konsoli ma być możliwy po wcześniejszej weryfikacji użytkownika. Produkt ma mieć możliwość definiowania wielu spersonalizowanych kont administracyjnych i niezależną konfigurację uprawnień.

5) Możliwość definiowania wielu niezależnych organizacji na jednym serwerze zarządzającym – informacje dostarczone do serwera zarządzającego nie będą dostępne pomiędzy organizacjami.
6) Integracja z Microsoft ActiveDirectory w celu importu użytkowników, listy maszyn, struktury jednostek organizacyjnych.
7) Konta administracyjne mają być tworzone na poziomie serwerów zarządzających i na poziomie organizacji definiowanych na serwerze.
8) Uprawnienia administratorów mają być ustawiane niezależnie dla każdego kontenera wewnątrz organizacji.
9) Możliwość utworzenia kont administratorów z uprawnieniami tylko do odczytu.
10) Konfiguracja agentów ma mieć strukturę drzewa, z mechanizmami dziedziczenia.
11) Uwierzytelnianie administratorów ma się odbywać w oparciu o wewnętrzną bazę danych lub z użyciem Microsoft Active Directory. Produkt ma mieć możliwość wykorzystania wieloelementowego uwierzytelniania (np. z wykorzystaniem tokenów, certyfikatów itp.).
12) Dostęp do interfejsu produktu i listy funkcji dostępnych dla użytkownika ma być konfigurowany z poziomu centralnej konsoli zarządzającej.
13) Paczki instalacyjne produktu mają pozwalać na dodanie własnej konfiguracji.
14) Pełna funkcjonalność ma być zawarta w jednym pliku instalacyjnym.
15) Nowe wersje dostarczonego rozwiązanie mają być automatycznie dystrybuowane na serwery w postaci różnicy między aktualnie zainstalowaną wersją na kliencie a nową wersją.
16) Produkt ma automatycznie wykrywać wszystkie urządzenia przyłączone do sieci komputerowej.
17) Produkt ma zapewniać graficzne raportowanie.
18) Wbudowane raporty maja pokazywać:
    a) Stan dystrybucji sygnatur antywirusowych oraz IDS/IPS,
    b) Wersje zainstalowanych klientów,
    c) Inwentaryzacje serwerów,
    d) Wykrytych wirusów, zdarzeń sieciowych, integralności komputerów.
19) Moduł raportowania ma pokazywać stan wykonywanych poleceń na węzłach.
20) Możliwość zaplanowanego tworzenia raportów i przesyłania ich na wybrane adresy poczty elektronicznej.
21) Możliwość zdefiniowania alertów administracyjnych zawierających zdarzenia:
    a) Błędnej autoryzacji do systemu zarządzania,
    b) Dostępności nowych wersji komponentów systemu antywirusowego,
    c) Pojawienia się nowego komputera,
    d) Zdarzeń powiązanych z infekcjami wirusów,
    e) Stanu serwerów zarządzających,
22) Pełna polska wersja językowa dostarczonego rozwiązania dla systemu zarządzania i klientów, wraz z dokumentacją.

8. Dystrybucja elementów systemu ochrony:

1) Paczka instalacyjna agenta do zarządzania instalowana na komputerze musi być nie większa niż 200MB.
2) Agent musi mieć możliwość określenia, z jaką przepustowością ma pobierać paczki instalacyjne (musi być też możliwość zdefiniowania, że ograniczenie pasma obowiązuje, jeżeli pasmo jest niższe niż określone).
3) Musi istnieć możliwość przekształcenia dowolnego agenta w taki sposób by lokalnie mógł dostarczać paczki instalacyjne dla danej grupy agentów – agenci sami wybiorą sobie dla nich najbliższe repozytorium paczek instalacyjnych.
4) Musi istnieć możliwość zdefiniowania, z jaką przepustowością agent przekształcony w lokalne repozytorium ma pobierać paczki instalacyjne – konfiguracja ta ma być niezależna od konfiguracji pozostałych agentów.
5) Musi istnieć możliwość dowolnego grupowania agentów oraz możliwość importu skonfigurowanych grup z Active Directory.
6) Agent musi, zupełnie niezależnie, mieć możliwość naprawy instalacji komponentów dostarczonego rozwiązania, dostarczenia nowych definicji wirusów, dokonanie audytu wykorzystywanych komponentów systemu antywirusowego (w szczególności wykorzystywanych wersji).
7) Agent musi mieć możliwość wykonania prostych komend na komputerze opartych o języki skryptowe.

9. Ochrona środowisk wirtualnych:

1) Produkt musi umożliwiać identyfikacje środowiska wirtualnego, w którym działa, informacja na ten temat musi być widoczna w konsoli. Minimalnie identyfikowane środowiska to: Microsoft, VMware.
2) Produkt musi umożliwiać w wypadku skanowania w czasie rzeczywistym oraz przy skanowaniu zaplanowanym, wykluczenie w środowisku wirtualnym wszystkich plików z tzw. bazowego obrazu (Gold Image) - nie będą one nigdy poddawane skanowaniu.
3) Produkt musi umożliwiać współdzielenie wyników skanowania zaplanowanego i na żądanie pomiędzy instancjami wirtualnymi - znalezienie już raz przeskanowanego tego samego pliku powoduje nieskanowanie go na systemie pytającym.
4) Produkt musi umożliwiać przeskanowanie plików *.vmdk w poszukiwaniu zagrożeń.

10. Ochrona systemu poczty elektronicznej:

1) Ochrona systemu pocztowego na styku z Internetem (bramka pocztowa):

Wymagania systemowe:

- Dedykowane redundantne rozwiązanie (appliance).
- Integracja z LDAP: min. Active Directory, MS Exchange.
- Rozwiązanie dostarczone przez Wykonawcę musi być odpowiednio wydajne, redundantne, zapewniać wsparcie dla mechanizmów HA oraz musi spełniać następujące wymagania:
    - rozwiązanie musi być dedykowane do obsługi dużych organizacji – min. 50 000 jednoczesnych użytkowników, z możliwością rozbudowy, bez konieczności wymiany lub reinstalacji,

  - konfiguracja rozwiązania musi zapewniać ciągłość działania dostarczonego systemu ochrony w przypadku awarii jednego z appliance-ów,
  - rozwiązanie musi umożliwiać konfigurację min. 2 niezależnych portów 1 Gb/s Ethernet,
  - rozwiązanie musi dodatkowo umożliwiać gromadzenie logów przez okres minimum dwóch lat.
- W przypadku zaoferowania urządzeń fizycznych, sprzętowe elementy rozwiązania muszą być fabrycznie nowe, muszą być nie starsze jak 3 miesiące, licząc od dnia podpisania umowy, zamontowane
  w szafie rack 19" zamawiającego, zajmować nie więcej jak 1U. Dodatkowo muszą spełniać następujące wymagania:
  - urządzenia muszą zawierać co najmniej podwójne zasilacze umożliwiające wymianę każdego z nich w trakcie pracy urządzenia,
  - urządzenia muszą zawierać min 2 porty 1 Gb/s Ethernet,
  - urządzenia muszą zawierać min. 2 dyski pracujące w trybie zapewniającym odporność na awarię dowolnego z nich i umożliwiające ich wymianę i odbudowę struktury danych w trakcie pracy urządzenia,
  - pojemność dysków musi dodatkowo umożliwiać gromadzenie logów przez okres minimum dwóch lat.

Funkcjonalność rozwiązania:

- Zintegrowane rozwiązanie antywirusowe, antyspamowe i filtrowania treści.
- Praca, jako bramka pocztowa.
- Blokowanie spamu w oparciu o lokalne polityki, silnik skanujący i bazy. Poczta nie jest przekierowana na serwer usługodawcy.
- Rozwiązanie antyspamowe ma mieć skuteczność nie mniejszą niż 98%. Równocześnie rozwiązanie ma charakteryzować się współczynnikiem fałszywych alarmów na poziomie 1 na milion, potwierdzonym przez niezależne testy.
- Do wykrywania spamu, system ma wykorzystywać bazy o numerach IP lub nazwach domen wykorzystywanych przez spamerów.
- System ma zapewnić routing wiadomości pocztowych w oparciu o domenę i adres odbiorcy.
- System ma mieć możliwość zmiany domeny i nazwy użytkownika w wiadomości przychodzącej i wychodzącej dla odbiorcy i nadawcy odpowiednio dla ruchu przychodzącego i wychodzącego.
- System ma umożliwiać tworzenie aliasów dla grup użytkowników.
- System ma zapewnić dopisywanie domyślnej nazwy domeny dla nadawcy wiadomości.
- System ma zapewnić ochronę przed skanowaniem serwera pocztowego w poszukiwaniu istniejących (prawidłowych) adresów pocztowych.
- Usuwanie nagłówków Received z wysyłanych wiadomości.

- Wiadomości z systemów próbujących atakować spamem serwer pocztowy, mają być automatycznie odrzucane przez określony czas, jeśli zostanie przekroczona wartość graniczna (ilość wiadomości zaklasyfikowanych, jako spam z jednego IP w danym przedziale czasu).
- Wiadomości z systemów próbujących atakować wirusami serwer pocztowy, mają być automatycznie odrzucane przez określony czas, jeśli zostanie przekroczona wartość graniczna (ilość wiadomości zaklasyfikowanych, jako wirusy z jednego IP w danym przedziale czasu).
- Połączenia z systemów próbujących atakować spamem serwer pocztowy, mają być automatycznie odrzucane przez określony czas, jeśli zostanie przekroczona wartość graniczna (ilość wiadomości zaklasyfikowanych, jako spam z jednego IP w danym przedziale czasu).
- Administrator ma mieć możliwość definiowania domen i adresów pocztowych, z którymi wymiana wiadomości będzie się zawsze odbywać.
- Administrator ma mieć możliwość definiowania domen i adresów pocztowych, z którymi wymiana wiadomości będzie zawsze blokowana.
- Niezależnie konfigurowane polityki dla wiadomości przychodzących i wychodzących.
- Funkcja ograniczająca dostępne pasmo dla maszyn/domen przesyłających spam, ale nieblokująca w całości komunikacji z tymi maszynami/domenami.
- Aktualizacje sygnatur spamu nie rzadziej, niż co 1 min.
- Aktualizacje sygnatur antywirusowych nie rzadziej, niż co 1 godzina.
- Rozwiązanie antywirusowe ma skanować skompresowane załączniki do 10 poziomów zagnieżdżeń w głąb i ma być odporna na złośliwie spreparowane załączniki („załączniki bomby”).
- Wiadomości z wirusami typu mass-mailer mają być w całości odrzucane, bez podejmowania dodatkowych akcji takich jak np. powiadomienie.
- Wykrywanie fałszywych URL-i w wiadomościach.
- Wykorzystanie technologii znakowania załączników dla odróżnienia ich treści.
- Wykorzystanie technologii analizy html mających na celu przeciwdziałanie metodom utrudniającym analizę treści wiadomości (np.: losowo generowane ciągi, nieprawidłowe kody formatujące).
- Detekcja języka, w którym została napisana wiadomość i możliwość użycia tej informacji, jako kryterium przy przetwarzaniu wiadomości.
- Kontrola treści w oparciu o słowa kluczowe lub słowniki definiowana przez administratora, w tym sprawdzanie zawartości skompresowanych archiwów.
- Możliwość dodawania do wysyłanych wiadomości zdefiniowanego tekstu.
- Nakładanie polityk na załączniki w oparciu o ich rozmiar, typ MIME, nazwę pliku lub jego rozszerzenie – w tym identyfikację prawdziwego rozszerzenia pliku.
- Wiadomości sklasyfikowane, jako spam można:
    - Usunąć

  - Dodać nagłówek wiadomości.
  - Zmodyfikować – dodać informację dla odbiorcy
  - Zarchiwizować
  - BCC – wysłać blind carbon copy na inny adres pocztowy
  - Bounce – odpowiedzieć nadawcy wiadomością z modyfikowalnym NDR
  - Wyczyścić, jeśli wiadomość zawierała wirusa
  - Dostarczyć bez modyfikacji
  - Przekierować na inny adres pocztowy
  - Zmodyfikować temat wiadomości
  - Wrzucić wiadomość do centralnej kwarantanny
  - Przesłać powiadomienie na wybrany adres
  - Usunąć załącznik z wiadomości
- Możliwość wysłania wiadomości spam niewykrytych przez rozwiązanie do producenta, w celu ich analizy.
- Rozróżnienie kategorii wiadomości na:
  - Normalne wiadomości bez spamu i wirusów,
  - Spam,
  - Podejrzane o spam,
  - Biuletyn (tzw. newsletter),
  - Wiadomość marketingowa,
  - Wiadomość z podejrzanym adresem URL,
  - Wirusy masowe,
  - Wiadomości zawierające wirusy,
  - Wiadomości, których nie można przeskanować,
  - Wiadomości od blokowanych nadawców,
  - Wiadomości zablokowane na podstawie filtrów przygotowanych przez administratora.
- Wsparcie dla Transport Layer Security (TLS) – definiowane per domena lub polityka, Sender Policy Framework (SPF), Sender ID.
- Import bazy użytkowników poprzez LDAP.
- Administrator ma mieć możliwość w ingerencję czułości rozwiązania.
- Rozwiązanie ma posiadać serwer kwarantanny, Serwer ma być dostępny dla poszczególnych użytkowników końcowych. Serwer ma przesyłać okresowe powiadomienia o zawartości kwarantanny. Powiadomienia mają mieć wbudowane mechanizmy do zarządzania zawartością kwarantanny (przesłanie dalej, podgląd, zalogowanie do kwarantanny).
- Na serwer kwarantanny można nałożyć ograniczenia dla poszczególnych użytkowników jak i całego serwera wg ilości przechowywanych wiadomości, ilości zajętego miejsca.
- Użytkownik końcowy rozwiązania ma mieć możliwość definiowania własnych list blokowanych i przepuszczanych nadawców wiadomości, ingerencje w zachowanie

systemu detekcji języka i możliwość wysłania do producenta systemu źle sklasyfikowanych wiadomości.

- Komunikacja pobierania uaktualnień ma być szyfrowana.
- Komunikacja w celu zarządzania systemem ma być szyfrowana.
- Rozwiązanie ma być centralnie zarządzane z wbudowanymi mechanizmami raportowania. Jedna konsola ma umożliwić zarządzania kilkoma współpracującymi urządzeniami. Wykonywane raporty mają uwzględniać dane zebrane ze wszystkich współpracujących urządzeń.
- System ma posiadać zestaw wbudowanych (predefiniowanych) raportów. Wykonanie raportów można zaplanować w dzienniku. Gotowe raporty można przesłać do skrzynki pocztowej wyznaczonych odbiorców.
- System ma umożliwiać tworzenie wielu kont administracyjnych z różnymi poziomami uprawnień, w tym możliwość zdefiniowania użytkowników mających dostęp do różnych kwarantann.
- System ma umożliwiać definiowanie poziomu logowania o swojej aktywności.
- System ma powiadamiać wybranych administratorów o nieprawidłowej pracy komponentów.
- System ma umożliwiać wykonywanie zaplanowanych kopii bezpieczeństwa konfiguracji i baz kwarantanny oraz możliwość odtworzenia konfiguracji z tak wykonanej kopii.
- Ograniczony zestaw poleceń dostępny z konsoli systemu operacyjnego.
- System ma umożliwiać graficzne śledzenie wiadomości, w tym informacje, co stało się z wiadomością.
- System ma posiadać wewnętrzną bazę reputacji, śledzącą adresy IP serwerów pocztowych.
- System ma umożliwiać zapytanie o adres IP do wewnętrznej i globalnej bazy reputacji.
- System ma umożliwiać stworzenie odpowiednio obsługiwanych kolejek z punktu widzenie reputacji danego adresu IP – ograniczając taki adres do ilości wysyłanych wiadomości, ilości nawiązywanych połączeń w określonym czasie.
- System ma mieć możliwość zdefiniowania osobnej kwarantanny dla poczty naruszającej reguły zgodności z polityką określającą rodzaj przesyłanych treści.
- System musi umożliwiać skorzystania z predefiniowanych polityk i wzorców.
- System ma umożliwiać rozpatrywanie incydentów skojarzonych z naruszeniem polityk, w tym definiowanie ważności incydentu.
- System ma posiadać ochronę przed atakami wirusów typu Day Zero, oraz zdefiniowaną kwarantannę dla złapanych w ten sposób wirusów z możliwością ustawienia czasu, przez który zatrzymane maile mają w niej pozostawać.
- System ma dodatkowo posiadać możliwość wysyłania alertów SNMP.
- System ma umożliwiać integracje z UPS-em.

- System musi wspierać autentykację DomainKeys Identified Mail (DKIM).
- System musi wspierać autentykację SMTP.

2) ochrona serwerów Exchange:

Wymagania systemowe:

- Wspierane systemy operacyjne:
  - Windows Server 2008/2008 R2 Standard/Enterprise/Data Center,
  - Windows 2012/2012 R2 i nowsze.
- Wersje Exchange:
  - Exchange Server 2010 (CAS, Hub Transport, Mailbox) i nowsze,
- Wspierane technologie wirtualizacyjne: VMWare oraz Hyper-V.

Funkcje dostarczonego rozwiązania:

- Zintegrowane rozwiązanie antywirusowe i antyspamowe.
- Możliwość zdefiniowania precyzyjnej polityki skanowania poczty elektronicznej.
- Możliwość tworzenia własnych raportów i ich automatycznego uruchamiania się.
- Zawiera zintegrowane narzędzie raportujące służące do raportowania statystyk związanym ze spamem i antywirusem.
- Możliwość tworzenia zaplanowanego skanowania zasobów.
- Skanowanie wiadomości przesyłanych przez serwer (routed messages)
- Możliwość wyboru pojedynczych skrzynek roboczych i folderów publicznych do skanowania zaplanowanego.
- Możliwość ustalenia czasu, w którym zaplanowane skanowanie ma się odbywać (okno czasowe). W przypadku, gdy skanowanie nie zostanie zakończone, następne skanowanie rozpocznie się w miejscu zakończenia poprzedniego.
- Aktualizacja definicji wirusów, co 1 godzinę.
- Wykorzystanie VS API 2.5.
- Wbudowana heurystyka.
- Usuwanie załączników o niepożądanym rozszerzeniu, także w archiwach spakowanych.
- Blokowanie wysyłania załączników dla grup użytkowników (integracja z Active Directory), dla wiadomości przychodzących czy wychodzących.
- Blokowanie wysyłania wiadomości z uwagi na treść dla grup użytkowników (integracja z Active Directory), dla wiadomości przychodzących czy wychodzących.
- Monitorowanie pracy systemu AV na serwerze Exchange'a, w celu wykrycia problemów z komunikacją system AV – Exchange.
- Konfiguracja przesyłanych powiadomień w zależności od rodzaju wykrytego zagrożenia.

- Możliwość usuwania całych wiadomości w przypadku wykrycia wirusa.
- Możliwość ciągłego skanowania Information Store w czasie rzeczywistym.
- Możliwość korzystania z centralnego serwera kwarantanny.
- Powiadamianie administratora o zmasowanym ataku wirusów.
- Funkcja usuwania poczty masowej automatycznie (Mass-Mailer Cleanup) eliminuje nie tylko załączniki, lecz całe wiadomości zainfekowane przez robaki rozsyłające się masowo za pomocą poczty elektronicznej.
- Niestandardowe reguły filtrowania.
- Filtrowanie oparte na regułach zapobiega przedostawaniu się do sieci niepożądanych treści, a także wydostawaniu się z niej poufnych informacji.
- Centralne zarządzanie za pomocą jednej konsoli obsługującej wiele serwerów, umożliwiające jednoczesną aktualizację ustawień wszystkich serwerów Microsoft® Exchange w całym przedsiębiorstwie.
- Zawiera narzędzie do zwalczania nowych „nieznanych" wirusów.
- Możliwość definiowania reguł dla plików zaszyfrowanych.
- Możliwość eksportowania i importowania ustawień konfiguracyjnych.
- System ma umożliwiać identyfikacje prawdziwego typu pliku niezależnie od jego rozszerzenia.
- Zintegrowane rozwiązanie antywirusowe i antyspamowe, jedna, graficzna konsola zarządzająca.
- Blokowanie spamu w oparciu o lokalne polityki, silnik skanujący i bazy. Poczta nie jest przekierowana na serwer usługodawcy.
- Definiowalne reguły filtrowania oraz funkcje obsługi czarnych list i białych list w czasie rzeczywistym.
- Rozwiązanie antyspamowe ma mieć skuteczność nie mniejszą niż 97%.Równocześnie rozwiązanie ma charakteryzować się współczynnikiem fałszywych alarmów na poziomie 1 na milion, potwierdzonym przez niezależne testy.
- Do wykrywania spamu, system ma wykorzystywać bazy o numerach IP lub nazwach domen wykorzystywanych przez spamerów.
- Aktualizacje sygnatur spamu nie rzadziej, niż co 10 min.
- Możliwość definiowania reguł dotyczących wiadomości podejrzanych o spam i uznanych za spam.
- Automatyczny sposób uaktualniania definicji antywirusów i antyspamu.
- Integracja z funkcjami określania poziomu wiarygodności poczty przychodzącej (Spam Confidence Level) oraz inteligentnego filtrowania wiadomości (Intelligent Message Filter) firmy Microsoft.
- System ma posiadać wewnętrzną bazę reputacji, śledzącą adresy IP serwerów pocztowych.

Oferowane rozwiązanie dla <u>stacji roboczych</u> powinno spełniać poniższe minimalne wymagania:

1. Antywirus:

1) Usuwanie wirusów, makrowirusów, robaków internetowych oraz koni trojańskich (oraz wirusów i robaków z plików skompresowanych oraz samo rozpakowujących się) lub kasowanie zainfekowanych plików. Ochrona przed oprogramowaniem typu „spyware" i „adware", włącznie z usuwaniem zmian wprowadzonych do systemu przez szkodliwe oprogramowanie.
2) Wykrywanie wirusów, makro-wirusów, robaków internetowych, koni trojańskich, spyware, adware i dialerów ma być realizowane w pojedynczym systemie skanującym.
3) Skanowanie plików pobranych z Internetu
4) Zapewnienie stałej ochrony wszystkich zapisywanych, odczytywanych, a także uruchamianych plików przez mechanizm skanujący pracujący w tle wraz z metodą heurystyczną wyszukiwania wirusów (na życzenie); pliki te mogą być skanowane:
   a) Na dyskach twardych,
   b) W boot sektorach,
   c) Na płytach CD/DVD,
   d) Na zewnętrznych dyskach twardych (np. podłączonych przez port USB).
5) Możliwość pobierania aktualizacji z Internetu do stacji.
6) Możliwość zablokowania funkcji zmiany konfiguracji klienta lub ukrycie interfejsu użytkownika klienta.
7) Wyszukiwanie i usuwanie wirusów w plikach skompresowanych (także zagnieżdżonych wewnątrz innych plików skompresowanych).
8) Aktualizacja definicji wirusów nie może wymagać zatrzymania procesu skanowania na jakimkolwiek systemie.
9) Mikro definicje wirusów - przyrostowe, scentralizowane aktualizowanie klientów jedynie o nowe definicje wirusów i mechanizmy skanujące.
10) Możliwość cofnięcia procesu aktualizacji definicji wirusów i mechanizmów skanujących – powrót do poprzedniego zestawu definicji wirusów bez konieczności reinstalacji komponentów systemu, systemu operacyjnego.
11) Możliwość natychmiastowego wymuszenia aktualizacji definicji wirusów.
12) Aktualizacja bazy definicji wirusów na bieżąco
13) Możliwość aktualizacji bazy definicji wirusów średnio, co 2 godziny.
14) Heurystyczna technologia do wykrywania nowych, nieznanych wirusów.
15) Moduł analizy zachowań aplikacji do wykrywania nowych, nieznanych zagrożeń typu robak internetowy, koń trojański, keylogger.
16) Automatyczne ponowne uruchomianie skanowania w czasie rzeczywistym, jeśli zostało wyłączone przez użytkownika mającego odpowiednie uprawnienia na z góry określony czas.
17) Automatyczne wymuszanie na kliencie programu pobrania zaktualizowanych definicji wirusów, jeśli aktualnie przechowywane sygnatury są przestarzałe.

18) Aktualizacje definicji wirusów muszą posiadać podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione.
19) Możliwość skanowania sieci w poszukiwaniu niezabezpieczonych stacji roboczych.
20) Blokowanie zewnętrznych urządzeń z możliwością tworzenia i konfiguracji zasad dla podłączanych nośników danych.
21) Możliwość zabezpieczenia programu antywirusowego przed deinstalacją i zmianą konfiguracji przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora. Przy próbie deinstalacji program musi pytać o hasło zabezpieczające instalację.
22) Możliwość ochrony przeglądarki internetowej przed zagrożeniami typu phishing,
23) Możliwość Skanowanie poczty klienckiej (na komputerze klienckim).

2. Firewall powinien zapewniać:

1) Pełne zabezpieczenie przed nieautoryzowanymi próbami dostępu do komputerów i skanowaniem portów.
2) Możliwość monitorowania i kontroli, jakie aplikacje łączą się poprzez interfejsy sieciowe.
3) Aktualizacje definicji sygnatur ataków posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione. Możliwość wykrywania próby wyszukiwania luk w zabezpieczeniach systemu w celu przejęcia nad nim kontroli.
4) Konfigurację zezwalanego i zabronionego ruchu, która ma się odbywać w oparciu o takie informacje jak: interfejs sieciowy, protokół, host docelowy, aplikacja, godzina komunikacji.
5) Uniemożliwienie określenia systemu poprzez maskowanie niepowtarzalnego identyfikatora systemu operacyjnego.
6) Domyślne reguły zezwalające na ruch DHCP, DNS.

3. Ochrona przed włamaniami:

1) Ma zawierać bibliotekę ataków i podatności (sygnatur) stosowanych przez produkt, dostarczoną przez Producenta rozwiązania. Administrator ma mieć możliwość uaktualniania tej biblioteki poprzez konsolę zarządzającą.
2) Ma mieć możliwość tworzenia własnych wzorców włamań (sygnatur), korzysta z analizy ruchu sieciowego do detekcji ataków.
3) Ma umożliwiać wykrywanie skanowania portów.
4) Ma umożliwiać ochronę przed atakami typu odmowa usług (Denial of Service).
5) Ma umożliwiać blokowanie komunikacji z serwerami z podmienionymi MAC adresami (spoofed MAC).
6) Ma umożliwiać blokowanie komunikacji z adresami ip atakującego.

4. Ochrona systemu operacyjnego:

1) Ma umożliwiać uruchamianie i blokowanie wskazanych aplikacji.
2) Ma umożliwiać tworzenie niestandardowych reguł kontroli aplikacji
3) Ma umożliwiać jednoznaczne rozróżnianie aplikacji.

4) Ma umożliwiać blokowanie wskazanego typu urządzeń przed dostępem użytkownika – urządzenia muszą być jednoznacznie identyfikowane.
5) Ma umożliwiać kontrolę dostępu do rejestru systemowego.
6) Polityki ochrony mają mieć możliwość pracy w dwóch trybach, testowym i produkcyjnym. W trybie testowym aplikacje i urządzenia nie są blokowane, ale jest tworzony wpis w logu.

5. Ochrona integralności systemu:

1) Musi umożliwiać wykonywanie testów integralności systemu pod kątem zgodności z polityką bezpieczeństwa, w tym: programów antywirusowych, poprawek firmy Microsoft, dodatków Service Pack firmy Microsoft, zapór ogniowych.
2) Testy integralności systemu mają być przeprowadzane cyklicznie, co zdefiniowany okres czasu.
3) W wypadku niezgodności własnego systemu, dostarczone rozwiązanie musi umożliwić zaaplikowanie dowolnego innego zestawu konfiguracji, w szczególności polityki firewallowej (zdefiniowanej bardzo restrykcyjnie), polityki antywirusowej, polityki pobierania aktualizacji, polityki kontroli uruchamianych aplikacji i polityki kontroli urządzeń.
4) Musi być możliwe, nieuwzględnianie wyniku poszczególnego testu na wynik końcowy integralności komputera.
5) Musi istnieć możliwość stwierdzenia, że na komputerze znaleziono zagrożenie i nie można było takiego zagrożenia usunąć – na ten czas komputer powinien znaleźć się w kwarantannie.

6. Architektura:

1) Rozwiązanie ma mieć architekturę trójwarstwową. Węzły mają być zarządzane przez serwery, a konfiguracja rozwiązania ma być zapewniona poprzez graficzną konsolę administratora.
2) Rozwiązanie ma zapewniać wysoką skalowalność i odporność na awarie.
3) Komunikacja pomiędzy agentami i serwerem ma być szyfrowana.
4) Numery portów używane do komunikacji mają mieć możliwość konfiguracji przez użytkownika końcowego.
5) Agent ma się przełączać do innego serwera zarządzającego w przypadku niedostępności przypisanego serwera.
6) Musi istnieć możliwość zdefiniowania dowolnego klienta, jako lokalnego dostarczyciela aktualizacji – możliwość konfiguracji ilości przetrzymywanych aktualizacji, zajętości na dysku oraz konfiguracji prędkości ich pobierania z serwera zarządzającego.

7. Moduł centralnego zarządzania:

1) Centralna instalacja, konfiguracja w czasie rzeczywistym, zarządzanie, raportowanie i administrowanie dostarczonym rozwiązaniem z pojedynczej konsoli.
2) Centralna aktualizacja ochrony antywirusowej, zapory ogniowej i systemu wykrywania włamań przez administratora.

3) Produkt ma zapewniać zarządzanie poprzez konsolę. Dostęp do konsoli ma być możliwy po wcześniejszej weryfikacji użytkownika. Produkt ma mieć możliwość definiowania wielu spersonalizowanych kont administracyjnych i niezależną konfigurację uprawnień.
4) Integracja z Microsoft Active Directory w celu importu użytkowników, listy maszyn, struktury jednostek organizacyjnych.
5) Konta administracyjne mają być tworzone na poziomie serwerów zarządzających i na poziomie organizacji definiowanych na serwerze.
6) Uprawnienia administratorów mają być ustawiane niezależnie dla każdego kontenera wewnątrz organizacji.
7) Możliwość utworzenia kont administratorów z uprawnieniami tylko do odczytu.
8) Konfiguracja agentów ma mieć strukturę drzewa, z mechanizmami dziedziczenia.
9) Uwierzytelnianie administratorów ma się odbywać w oparciu o wewnętrzną bazę danych lub z użyciem Microsoft Active Directory. Produkt ma mieć możliwość wykorzystania wieloelementowego uwierzytelniania (np. z wykorzystaniem tokenów, certyfikatów itp.).
10) Dostęp do interfejsu produktu i listy funkcji dostępnych dla użytkownika ma być konfigurowany z poziomu centralnej konsoli zarządzającej.
11) Paczki instalacyjne produktu mają pozwalać na dodanie własnej konfiguracji.
12) Pełna funkcjonalność ma być zawarta w jednym pliku instalacyjnym.
13) Produkt ma automatycznie wykrywać urządzenia przyłączone do sieci komputerowej.
14) Produkt ma zapewniać graficzne raportowanie.
15) Wbudowane raporty maja pokazywać:
    a) Stan dystrybucji sygnatur antywirusowych
    b) Wersje zainstalowanych klientów,
    c) Inwentaryzacje klientów,
    d) Wykrytych wirusów, zdarzeń sieciowych, integralności komputerów.
16) Moduł raportowania ma pokazywać stan wykonywanych poleceń.
17) Możliwość zaplanowanego tworzenia raportów i przesyłania ich na wybrane adresy poczty elektronicznej.
18) Możliwość zdefiniowania alertów administracyjnych.
19) Produkt powinien umożliwiać instalacji/deinstalacji poprzez System SCCM będące w posiadaniu zamawiającego (wersja SCCM 2012 R2).
20) Pełna polska wersja językowa dostarczonego rozwiązania dla systemu zarządzania i klientów, wraz z dokumentacją.
21) Możliwość zdefiniowania indywidualnych komputerów lub całych zakresów adresów IP, które są traktowane, jako: całkowicie bezpieczne lub niebezpieczne.

8. Dystrybucja elementów systemu ochrony:

1) Paczka instalacyjna agenta do zarządzania instalowana na komputerze musi być nie większa niż 200MB.
2) Produkt powinien umożliwiać instalacje agenta w wersji z sygnaturami i bez sygnatur (czysty agent).

3) Agent musi mieć możliwość określenia, z jaką przepustowością ma pobierać paczki instalacyjne (musi być też możliwość zdefiniowania, że ograniczenie pasma obowiązuje, jeżeli pasmo jest niższe niż określone).
4) Musi istnieć możliwość konfiguracji agenta w taki sposób by lokalnie mógł dostarczać paczki instalacyjne dla danej grupy agentów – agenci sami wybiorą sobie dla nich najbliższe repozytorium paczek instalacyjnych.
5) Musi istnieć możliwość zdefiniowania, z jaką przepustowością agent przekształcony w lokalne repozytorium ma pobierać paczki instalacyjne – konfiguracja ta ma być niezależna od konfiguracji pozostałych agentów.
6) Musi istnieć możliwość dowolnego grupowania agentów oraz możliwość importu skonfigurowanych grup z Active Directory.
7) Rozwiązanie musi, zupełnie niezależnie, mieć możliwość naprawy instalacji komponentów dostarczonego rozwiązania, dostarczenia nowych definicji wirusów, dokonanie audytu wykorzystywanych komponentów systemu antywirusowego (w szczególności wykorzystywanych wersji).
8) Agent musi mieć możliwość wykonania prostych komend na komputerze opartych o języki skryptowe.

9. Ochrona środowisk wirtualnych:

1) Produkt musi umożliwiać identyfikacje środowiska wirtualnego, w którym działa, informacja na ten temat musi być widoczna w konsoli. Minimalnie identyfikowane środowiska to: Microsoft, VMware.
2) Produkt musi umożliwiać w wypadku skanowania w czasie rzeczywistym oraz przy skanowaniu zaplanowanym, wykluczenie w środowisku wirtualnym wszystkich plików z tzw. bazowego obrazu (Gold Image) - nie będą one nigdy poddawane skanowaniu.
3) Produkt musi umożliwiać współdzielenie wyników skanowania zaplanowanego i na żądanie pomiędzy instancjami wirtualnymi - znalezienie już raz przeskanowanego tego samego pliku powoduje nieskanowanie go na systemie pytającym.
4) Produkt musi umożliwiać przeskanowanie plików .vmdk w poszukiwaniu zagrożeń.

10. Warunki wsparcia:

Dostarczone rozwiązanie musi być objęte 36 miesięczną gwarancją na poniższych warunkach.

1) Wykonawca w dniu zawarcia umowy przekaże Zamawiającemu wykaz pracowników upoważnionych do rozwiązywania problemów i współpracy z Zamawiającym w celu realizacji umowy. Wszystkie ww. osoby winny komunikować się w zakresie koordynacji i realizacji przedmiotu zamówienia z zamawiającym w języku polskim (w mowie i piśmie). W przypadku osób nie władających językiem polskim Wykonawca zobowiązany jest zapewnić tłumacza na język polski.
2) Wykonawca zapewni aktualizacje baz sygnatur wirusów, oprogramowania, lub inne rozwiązanie stosowane przez producenta oprogramowania gwarantujące skuteczną ochronę antywirusową, przez cały okres obowiązywania umowy. W przypadku awarii Wykonawca zapewni czas naprawy lub zastosowanie obejścia oraz przywrócenia pełnej funkcjonalności, w przeciągu 24 godzin roboczych (dni

od poniedziałku do piątku, z wyłączeniem świąt ustawowych, w godzinach w godz. 8.00 – 16.00.) od chwili zgłoszenia.

3) Wykonawca zapewni pełne wsparcie dla dostarczonych urządzeń (w zakresie pełnej obsługi sprzętu i oprogramowania, przez cały okres obowiązywania umowy). W przypadku awarii Wykonawca zapewni czas naprawy lub wymiany urządzenia na inne, wolne od wad (o parametrach nie gorszych od posiadanego przez zamawiającego) oraz przywrócenia pełnej funkcjonalności, w przeciągu 24 godzin roboczych (dni od poniedziałku do piątku, z wyłączeniem świąt ustawowych, w godzinach w godz. 8.00 – 16.00.) od chwili zgłoszenia awarii.
4) Wykonawca w czasie realizacji umowy zagwarantuje czas pracy inżyniera do dyspozycji Zamawiającego w ilości 100 godzin przez 3 lata, od poniedziałku do piątku, z wyłączeniem świąt ustawowych, w godzinach w godz. 8.00 – 16.00, od momentu rozpoczęcia świadczenia usług.
5) Po każdorazowym zakończeniu pracy inżyniera będzie sporządzany protokół z wykorzystania godzin.
6) Ponadto Wykonawca, w ramach gwarancji, zapewni Zamawiającemu e-mail`owe i telefoniczne konsultacje w zakresie dostarczonego systemu oraz jego współpracy z platformami, na których jest osadzone w dni robocze, od poniedziałku do piątku, z wyłączeniem świąt ustawowych, w godzinach w godz. 8.00 – 16.00.
7) Wykonawca gwarantuje świadczenie usługi gwarancyjnych i możliwość zgłaszania problemów drogą elektroniczną na dedykowany adres email, 7 dni w tygodniu i 24 godz. na dobę. Wykonawca gwarantuje obsługę trudnych do zdiagnozowania i usunięcia problemów, na miejscu u Zamawiającego w dni robocze, od poniedziałku do piątku, z wyłączeniem świąt ustawowych, w godzinach w godz. 8.00 – 16.00.
8) W przypadku urządzeń fizycznych wykonawca zapewni gwarantowany czas naprawy w przeciągu 24 godzin roboczych (dni od poniedziałku do piątku, z wyłączeniem świąt ustawowych oraz dni wolnych Zamawiającego, w godzinach w godz. 8.00 – 16.00), od chwili zgłoszenia awarii..
9) W przypadku, gdy naprawa nie może być wykonana w terminie 24 godzin od momentu zgłoszenia, Wykonawca dostarczy, uruchomi i skonfiguruje urządzenie zastępcze wyprodukowane nie wcześniej niż wymieniane, wykonane w tej samej technologii, o nie gorszych parametrach technicznych i o nie większych kosztach eksploatacji, przez cały okres użytkowania sprzętu przez Zamawiającego. Urządzenie zastępcze nie będzie powodowało wzrostu kosztów utrzymania pozostałych urządzeń posiadanych przez Zamawiającego. Koszty dostawy i wymiany urządzenia ponosi Wykonawca. Urządzenie zastępcze będzie uruchomione na okres nie dłuższy niż 60 dni. Po tym terminie Wykonawca jest zobowiązany do dostarczenia naprawionego sprzętu. W przypadku, gdy Wykonawca nie zwróci naprawianego urządzenia w powyższym terminie lub umowa wygaśnie przed upływem 60 dni od dostarczenia urządzenia zastępczego urządzenie zastępcze przechodzi na własność Zamawiającego
10) W ramach gwarancji Wykonawca będzie dokonywał comiesięcznych weryfikacji poprawności działania systemu w siedzibie Zamawiającego, świadczył pomoc przy określaniu jego optymalnej konfiguracji oraz współpracy z innym, używanym w ZUS oprogramowaniem firmy Microsoft. Weryfikacja poprawności działania systemu powinna być wykonywana raz w miesiącu, przez okres 3 lat, od momentu rozpoczęcia świadczenia usług, w terminie do 10 dnia każdego miesiąca. Raport z weryfikacji poprawności działania systemu powinien zawierać m.in.:
    a) Analizę problemów wynikających z raportu poprzedniego,

b) Wykaz wykonanych prac podczas wizyty,
c) Raport stanu definicji wirusów,
d) Zestawienie niezaktualizowanych klientów z poprzedniego i bieżącego raportu,
e) Zestawienie wersji komponentów oprogramowania dostępnego w ramach aktualizacji z wersjami używanymi przez Zamawiającego,
f) Zalecenia naprawcze dotyczące wykrytych nieprawidłowości,
g) Ewentualne sugestie zmian konfiguracji ochrony przed złośliwym oprogramowaniem mające na celu zwiększenie bezpieczeństwa.

11) Po przeprowadzeniu comiesięcznej weryfikacji poprawności działania systemu sporządzony zostanie protokół. Protokół zostanie podpisany przez przedstawicieli Wykonawcy i Zamawiającego.
12) Usługa gwarancji świadczona przez Wykonawcę będzie realizowana w Centrali ZUS, Warszawa.

Załącznik nr 2 – Formularz odpowiedzi na zapytanie

Dane podmiotu	……*
Adres Wykonawcy: kod, miejscowość, ulica, nr lokalu	……*
Nr telefonu	……*
E-mail	……*

Zakład Ubezpieczeń Społecznych

ul. Szamocka 3, 5

01-748 Warszawa

FORMULARZ ODPOWIEDZI NA ZAPYTANIE O INFORMACJĘ

1. W odpowiedzi na Zapytanie o informację dotyczące ***Zakup wsparcia dla posiadanego przez Zamawiającego systemu antywirusowego opartego na oprogramowaniu firmy Symantec albo dostarczenie i wdrożenie rozwiązania równoważnego*** przedstawiam poniższe informacje.

2. Poniższe informacje (**wybrać właściwe**):
   - *zawierają informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji i nie mogą być ujawniane innym podmiotom.
   - *nie zawierają informacji stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji i mogą być ujawniane innym podmiotom.

   UWAGA: w przypadku gdy Wykonawca nie zaznaczy żadnej z ww. opcji, ZUS przyjmie, że Wykonawca nie zastrzega przekazanych informacji jako stanowiących tajemnicę przedsiębiorstwa, co w konsekwencji oznaczać będzie, że takie informacje będą udostępnianie przez ZUS w trybie dostępu do informacji publicznej, na stosowny wniosek innych podmiotów.

3. Przedstawione informacje dotyczące szacunkowych kosztów (**wybrać właściwe*):
   - *zawierają upusty na poziome ….% od „cen katalogowych".
   - *nie zawierają upustów od „cen katalogowych" i ZUS może uzyskać upust na poziome ….% od poniżej przedstawionych kosztów.

4. Przedstawione informacje dotyczą (**wybrać właściwe*):
   - ***Wariantu I** – 36 miesięczna usługa wsparcia dla systemu antywirusowego opartego na oprogramowaniu firmy Symantec będącego w użytkowaniu przez Zamawiającego.
   - ***Wariantu II** – dostarczenie i wdrożenie rozwiązania równoważnego z zapewnieniem 36 miesięcznego wsparcia.
5. Wszelką korespondencję dotyczącą przedmiotowej odpowiedzi na zapytanie o informację należy kierować na:

Imię i Nazwisko	……*
Nazwa podmiotu	……*
Adres	……*
Nr telefonu	……*

Nr faksu	……*
Adres e-mail	……*

Zakup wsparcia dla posiadanego przez Zamawiającego systemu antywirusowego opartego na oprogramowaniu firmy Symantec albo dostarczenie i wdrożenie rozwiązania równoważnego

Specyfikacja zaoferowanego rozwiązania

Funkcjonalność	Zaproponowane rozwiązanie
Rozwiązanie dotyczące serwerów oraz poczty:	
1. Antywirus	
2. Firewall	
3. Ochrona przed włamaniami	
4. Ochrona systemu operacyjnego	
5. Ochrona integralności systemu	
6. Architektura	
7. Moduł centralnego zarządzania	
8. Dystrybucja elementów systemu ochrony	
9. Ochrona środowisk wirtualnych	
10. Ochrona systemu poczty elektronicznej	
1) Ochrona systemu pocztowego na styku z Internetem (bramka pocztowa)	
2) ochrona serwerów Exchange	
Rozwiązania dotyczące stacji roboczych	
1. Antywirus	
2. Firewall	
3. Ochrona przed włamaniami	
4. Ochrona systemu operacyjnego	
5. Ochrona integralności systemu	
6. Architektura	
7. Moduł centralnego zarządzania	

Formularz cenowy

	1	5	8	9
Lp.	**Produkt**	**Stawka podatku VAT w %**	**Razem w PLN (bez VAT)**	**Razem w PLN (z VAT)**
1	System antywirusowy	……*	……*	……*
2	… Inne elementy oddzielnie wyceniane*	……*	……*	……*
3	Warsztaty	……*	……*	……*
4	36 miesięczna Usługa wsparcia	……*	……*	……*
Razem				

* wypełnia Oferent

Nazwisko i imię osoby (osób) uprawnionej(-ych)	Podpis(-y) osoby(osób) uprawnionej(-ych)