POWIATOWY URZĄD PRACY W ROPCZYCACH

ul. Najświętszej Marii Panny 2, 39-100 Ropczyce tel. 17 22-31-660; fax 17 22-27-569
rzro@praca.gov.pl *www.bip.pup-ropczyce.pl*

Ropczyce, dnia 28.06.2016r.

WA.2510.1.107.2016.AK

Zaproszenie do składania ofert

Powiatowy Urząd Pracy w Ropczycach zaprasza do składania ofert cenowych na
dostawę oprogramowania antywirusowego
dla Powiatowego Urzędu Pracy w Ropczycach

Zamówienie o wartości netto **poniżej 30 000** €.

1. Zamawiający:

Powiatowy Urząd Pracy w Ropczycach
Ul. Najświętszej Marii Panny 2
39 – 100 Ropczyce

Osobami ze strony Zamawiającego upoważnionymi do kontaktowania się z Wykonawcami są:

1. Witold Cesarz tel. 17 22 31 684 e-mail wcesarz@pup-ropczyce.pl
2. Aneta Kubik tel. 17 22-31-661 e-mail akubik@pup-ropczyce.pl

2. Opis przedmiotu zamówienia:

2.1

Dostawa 75 licencji oprogramowania antywirusowego ESET Endpoint Antivirus NOD32 Suite dla stacji roboczych i serwerów plików z konsolą administracyjną, lub równoważny spełniający poniższe kryteria.

Wymagania w zakresie ochrony stacji roboczych:

1. Pełne wsparcie dla systemu Windows Vista/Windows 7/Windows8/Windows 8.1/10 w wersji 32 i 64 bitowej
2. Wersja programu dla stacji roboczych oraz pomoc i dokumentacja dostępne w języku polskim.
3. Skuteczność programu potwierdzona nagrodami VB100 i co najmniej jedną inną niezależną organizacje taką jak AV-comparatives lub AV-test
4. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
5. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
6. Wbudowana technologia do ochrony przed rootkitami.
7. Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
8. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików, możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.

9. System ma oferować administratorowi możliwość definiowania zadań w harmonogramie w taki sposób, aby zadanie przed wykonaniem sprawdzało czy komputer pracuje na zasilaniu bateryjnym i jeśli tak – nie wykonywało danego zadania.
10. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (w tym: co godzinę, po zalogowaniu i po uruchomieniu komputera). Każde zadanie ma mieć możliwość uruchomienia z innymi ustawieniami (czyli metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania).
11. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
12. Możliwość określania poziomu obciążenia procesora podczas skanowania „na żądanie” i według harmonogramu.
13. Możliwość skanowania dysków sieciowych i dysków przenośnych, skanowanie plików spakowanych i skompresowanych.
14. Możliwość definiowania listy rozszerzeń plików, które mają być skanowane (w tym z uwzględnieniem plików bez rozszerzeń).
15. Możliwość umieszczenia na liście wyłączeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
16. Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu.
17. Brak konieczności ponownego uruchomienia komputera po instalacji programu.
18. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 min lub do ponownego uruchomienia komputera.
19. W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji.
20. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera.
21. Możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.
22. Skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP w czasie rzeczywistym, zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
23. Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
24. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.
25. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.
26. Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. Program musi umożliwić blokowanie danej strony internetowej po podaniu na liście całej nazwy strony lub tylko wybranego słowa występującego w nazwie strony.
27. Możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron ustalonej przez administratora.
28. Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.

29. Program ma zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.
30. Możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika w celu analizy przez laboratorium producenta.
31. Administrator ma mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego.
32. Program musi posiadać funkcjonalność która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
33. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania na żądanie oraz przez moduły ochrony w czasie rzeczywistym.
34. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego.
35. W przypadku gdy stacja robocza nie będzie posiadała dostępu do sieci Internet ma odbywać się skanowanie wszystkich procesów również tych, które wcześniej zostały uznane za bezpieczne.
36. Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej i/lub obu metod jednocześnie.
37. Możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie, oraz czy próbki zagrożeń mają być wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika.
38. Do wysłania próbki zagrożenia do laboratorium producenta aplikacja nie może wykorzystywać klienta pocztowego wykorzystywanego na komputerze użytkownika.
39. Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.
40. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
41. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
42. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy komputerze przy próbie dostępu do konfiguracji był proszony o podanie hasła.
43. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora. Przy próbie deinstalacji program musi pytać o hasło.
44. Program ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika i administratora wraz z listą niezainstalowanych aktualizacji.
45. Program ma mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zwykle oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu.

46. Po instalacji programu, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu wirusów.
47. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku.
48. Program ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie brak dostępu do podłączanego urządzenia.
49. Program ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
50. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.
51. Użytkownik ma posiadać możliwość takiej konfiguracji programu aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika
52. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).
53. Program musi być wyposażona w mechanizm ochrony przed exploitami w popularnych aplikacjach np. czytnikach PDF, aplikacjach JAVA itp.
54. Program ma być wyposażony we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesach i połączeniach.
55. Program ma oferować funkcję, która aktywnie monitoruje i skutecznie blokuje działania wszystkich plików programu, jego procesów, usług i wpisów w rejestrze przed próbą ich modyfikacji przez aplikacje trzecie.
56. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń dostępna z Internetu.
57. Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami.
58. Możliwość określenia maksymalnego czasu ważności dla bazy danych sygnatur, po upływie czasu i braku aktualizacji program zgłosi posiadanie nieaktualnej bazy sygnatur.
59. Program musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji.
60. Program musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji za pomocą wbudowanego w program serwera http
61. Program musi być wyposażona w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji w celu ich późniejszego przywrócenia.
62. Program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
63. Aplikacja musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełno ekranowym, w momencie wykrycia trybu pełno ekranowego aplikacja ma wstrzymać wyświetlanie wszelkich powiadomień związanych ze swoją pracą oraz wstrzymać swoje zadania znajdujące się w harmonogramie zadań aplikacji.

64. Użytkownik ma mieć możliwość skonfigurowania programu tak aby automatycznie program włączał powiadomienia oraz zadania pomimo pracy w trybie pełnoekranowym po określonym przez użytkownika czasie.
65. Program ma być wyposażony w dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, kontroli stron Internetowych i kontroli urządzeń, skanowania na żądanie i według harmonogramu, dokonanych aktualizacji baz wirusów i samego oprogramowania.
66. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.
67. Program musi posiadać możliwość aktywacji poprzez podanie klucza licencyjnego oraz możliwość aktywacji programu offline.

Wymagania w zakresie ochrony serwera plików Windows

1. Wsparcie dla systemów: Microsoft Windows Server 2008, 2008 R2, 2012, 2012 R2.
2. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
3. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
4. Wbudowana technologia do ochrony przed rootkitami i exploitami.
5. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
6. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
7. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu. Każde zadanie może być uruchomione z innymi ustawieniami (metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania).
8. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
9. System antywirusowy ma mieć możliwość określania poziomu obciążenia procesora podczas skanowania „na żądanie” i według harmonogramu.
10. System antywirusowy ma mieć możliwość wykorzystania wielu wątków skanowania w przypadku maszyn wieloprocesorowych.
11. Użytkownik ma mieć możliwość zmiany ilości wątków skanowania w ustawieniach systemu antywirusowego.
12. Możliwość skanowania dysków sieciowych i dysków przenośnych.
13. Skanowanie plików spakowanych i skompresowanych.
14. Możliwość definiowania listy rozszerzeń plików, które mają być skanowane (z uwzględnieniem plików bez rozszerzeń).
15. Możliwość umieszczenia na liście wyłączeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
16. Program musi posiadać funkcjonalność pozwalającą na ograniczenie wielokrotnego skanowania plików w środowisku wirtualnym za pomocą mechanizmu przechowującego informacje o przeskanowanym już obiekcie i współdzieleniu tych informacji z innymi maszynami wirtualnymi.
17. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).
18. Program powinien oferować możliwość skanowania dysków sieciowych typu NAS.
19. Aplikacja musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.

20. Aplikacja musi posiadać funkcjonalność, która automatycznie uzupełni elementy wymagane dla tworzenia reguł w oparciu o informacje dostępne z aktualnie podłączonego nośnika.
21. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.
22. System antywirusowy ma automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
23. Zainstalowanie na serwerze nowych usług serwerowych ma skutkować automatycznym dodaniem kolejnych wyłączeń w systemie ochrony.
24. Dodanie automatycznych wyłączeń nie wymaga restartu serwera.
25. Automatyczne wyłączenia mają być aktywne od momentu wykrycia usług serwerowych.
26. Administrator ma mieć możliwość wglądu w elementy dodane do wyłączeń i ich edycji.
27. W przypadku restartu serwera – usunięte z listy wyłączeń elementy mają być automatycznie uzupełnione.
28. Brak konieczności ponownego uruchomienia komputera po instalacji systemu antywirusowego.
29. System antywirusowy ma mieć możliwość zmiany konfiguracji oraz wymuszania zadań z poziomu dedykowanego modułu CLI .
30. Możliwość przeniesienia zainfekowanych plików w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.
31. Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej i/lub obu metod jednocześnie.
32. Możliwość skanowania wyłącznie z zastosowaniem algorytmów heurystycznych tj. wyłączenie skanowania przy pomocy sygnatur baz wirusów.
33. Aktualizacje modułów analizy heurystycznej.
34. Możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie, oraz czy próbki zagrożeń będą wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika.
35. Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.
36. Wysyłanie zagrożeń do laboratorium ma być możliwe z serwera zdalnego zarządzania i lokalnie z każdej stacji roboczej w przypadku komputerów mobilnych.
37. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
38. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
39. Interfejs programu ma oferować funkcję pracy w trybie bez grafiki gdzie cały interfejs wyświetlany jest w formie formatek i tekstu.

40. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy serwerze przy próbie dostępu do konfiguracji systemu antywirusowego był proszony o podanie hasła.
41. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program ma pytać o hasło.
42. System antywirusowy ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika wraz z listą niezainstalowanych aktualizacji.
43. System antywirusowy ma mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zwykle oraz aktualizacje o niskim priorytecie. Program ma także posiadać opcję dezaktywacji tego mechanizmu.
44. System antywirusowy ma oferować funkcję, która aktywnie monitoruje i skutecznie blokuje działania wszystkich plików programu, jego procesów, usług i wpisów w rejestrze przed próbą ich modyfikacji przez aplikacje trzecie.
45. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń.
46. Aktualizacja dostępna z Internetu, lokalnego zasobu sieciowego, nośnika CD, DVD lub napędu USB, a także przy pomocy protokołu HTTP z dowolnej stacji roboczej lub serwera (program antywirusowy z wbudowanym serwerem HTTP).
47. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.
48. Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami (serwer aktualizacyjny, ustawienia sieci, autoryzacja).
49. Do każdego zadania aktualizacji można przypisać dwa różne profile z innym ustawieniami (serwer aktualizacyjny, ustawienia sieci, autoryzacja). Przykładowo, domyślny profil aktualizuje z sieci lokalnej a w przypadku jego niedostępności wybierany jest profil rezerwowy pobierający aktualizację z Internetu.
50. System antywirusowy wyposażony w tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
51. Aplikacja musi posiadać możliwość wykluczania ze skanowania procesów.
52. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania.
53. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.

Wymagania w zakresie administracji zdalnej

1. Serwer administracyjny musi oferować możliwość instalacji na systemach Windows Server 2008, 2012 oraz systemach Linux.
2. Musi istnieć możliwość pobrania ze strony producenta serwera zarządzającego w postaci gotowej maszyny wirtualnej w formacie OVA (Open Virtual Appliance).
3. Serwer administracyjny musi oferować możliwość wykorzystania już istniejącej bazy danych MS SQL lub MySQL użytkownika.
4. Administrator musi posiadać możliwość pobrania wszystkich wymaganych elementów serwera centralnej administracji i konsoli w postaci jednego pakietu instalacyjnego lub każdego z modułów oddzielnie bezpośrednio ze strony producenta.
5. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW niezależnie od platformy sprzętowej i programowej.

6. Narzędzie musi być kompatybilne z protokołami IPv4 oraz IPv6.
7. Komunikacja z konsolą powinna być zabezpieczona się za pośrednictwem protokołu SSL.
8. Narzędzie do administracji zdalnej musi posiadać moduł pozwalający na wykrycie niezarządzanych stacji roboczych w sieci.
9. Serwer administracyjny musi posiadać mechanizm instalacji zdalnej oprogramowania antywirusowego na stacjach roboczych.
10. Serwer administracyjny musi oferować możliwość instalacji modułu do zarządzania urządzeniami mobilnymi.
11. Serwer administracyjny musi oferować możliwość instalacji serwera http proxy pozwalającego na pobieranie aktualizacji baz sygnatur oraz pakietów instalacyjnych na stacjach roboczych bez dostępu do Internetu.
12. Serwer http proxy musi posiadać mechanizm zapisywania w pamięci podręcznej najczęściej pobieranych elementów.
13. Centralna administracja musi pozwalać na zarządzanie programami zabezpieczającymi na stacjach roboczych z systemami Windows, Linux oraz serwerach Windows.
14. Centralna administracja musi pozwalać na zarządzanie programami zabezpieczającymi na urządzeniach mobilnych z systemem Android.
15. Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware'ową, zaporą osobistą i kontrolą dostępu do stron internetowych zainstalowanymi na stacjach roboczych w sieci.
16. Serwer administracyjny musi posiadać możliwość pobrania listy zainstalowanego oprogramowania firm trzecich na stacji roboczej z możliwością jego odinstalowania.
17. W przypadku braku zainstalowanego klienta na urządzeniu mobilnym musi istnieć możliwość jego pobrania ze sklepu Google Play.
18. Administrator musi posiadać możliwość utworzenia listy zautoryzowanych urządzeń mobilnych, które mogą zostać podłączone do serwera centralnej administracji.
19. Serwer administracyjny musi oferować możliwość zablokowania, odblokowania, wyczyszczenia zawartości, zlokalizowania oraz uruchomienia syreny na zarządzanym urządzaniu mobilnym. Funkcjonalność musi wykorzystywać połączenie internetowe, nie komunikację za pośrednictwem wiadomości SMS.
20. Serwer administracyjny musi oferować możliwość utworzenia polityk konfiguracji dla aplikacji zabezpieczającej na urządzeniu mobilnym.
21. Administrator musi posiadać możliwość utworzenia dodatkowych użytkowników/administratorów Serwer centralnego zarządzania do zarządzania stacjami roboczymi.
22. Administrator musi posiadać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli zarządzającej
23. Dwu fazowa autoryzacja musi się odbywać za pomocą wiadomości SMS lub haseł jednorazowych generowanych na urządzeniu mobilnym za pomocą dedykowanej aplikacji.
24. Administrator musi posiadać możliwość utworzenia użytkownika wbudowanego lub zintegrowanego z grupą z usługi Active Directory.
25. Serwer administracyjny musi oferować możliwość utworzenia zestawów uprawnień dotyczących zarządzania poszczególnymi grupami komputerów, politykami, raportowania, zarządzania licencjami, zadaniami, itp.
26. Serwer administracyjny musi posiadać możliwość konfiguracji czasu bezczynności po jakim użytkownik zostanie automatycznie wylogowany.

27. Serwer administracyjny musi w przejrzysty sposób informować administratora o elementach zadań jakie są wymagane do jego uruchomienia a w przypadku jego braku wskazywać brakujące elementy konfiguracji.
28. Instalacja zdalna programu zabezpieczającego musi odbywać się z repozytorium producenta lub z pakietu dostępnego w Internecie lub zasobie lokalnym.
29. Serwer administracyjny musi oferować możliwość wyboru parametrów pakietu instalacyjnego zależnych od systemu operacyjnego oraz licencji na program zabezpieczający.
30. Serwer administracyjny musi oferować możliwość deinstalacji programu zabezpieczającego firm trzecich lub jego niepełnej instalacji podczas instalacji nowego pakietu.
31. Serwer administracyjny musi oferować możliwość wysłania komunikatu lub polecenia na stacje kliencką.
32. Serwer administracyjny musi oferować możliwość utworzenia jednego zadania dla kilku klientów lub grupy.
33. Serwer administracyjny musi oferować możliwość uruchomienia zadania automatycznie zgodnie z harmonogramem, po wystąpieniu nowego dziennika zdarzeń lub umieszczeniu nowego klienta w grupie dynamicznej.
34. Serwer administracyjny musi oferować możliwość utworzenia grup statycznych i dynamicznych komputerów.
35. Grupy dynamiczne tworzone na podstawie szablonu określającego warunki jakie musi spełnić klient aby zostać umieszczony w danej grupie. Przykładowe warunki: Adresy sieciowe IP, Aktywne zagrożenia, Stan funkcjonowania/ochrony, Wersja systemu operacyjnego, itp.
36. Serwer administracyjny musi oferować możliwość utworzenia polityk dla programów zabezpieczających i modułów serwera centralnego zarządzania.
37. Serwer administracyjny musi oferować możliwość przypisania polityki dla pojedynczego klienta lub dla grupy komputerów. Serwer administracyjny musi oferować możliwość przypisania kilku polityk z innymi priorytetami dla jednego klienta.
38. Edytor konfiguracji polityki musi być identyczny jak edytor konfiguracji ustawień zaawansowanych w programie zabezpieczającym na stacji roboczej.
39. Serwer administracyjny musi oferować możliwość nadania priorytetu „Wymuś” dla konkretnej opcji w konfiguracji klienta. Opcja ta nie będzie mogła być zmieniona na stacji klienckiej bez względu na zabezpieczenie całej konfiguracji hasłem lub w przypadku jego braku.
40. Serwer administracyjny musi oferować możliwość ukrycia graficznego interfejsu użytkownika na stacji klienckiej i jego uruchomienia tylko przez administratora.
41. Serwer administracyjny musi umożliwiać wyświetlenie polityk do których przynależy dana stacja robocza oraz ich edycję z poziomu właściwości samego klienta
42. Serwer administracyjny musi oferować możliwość utworzenia własnych raportów lub skorzystanie z predefiniowanych wzorów.
43. Serwer administracyjny musi oferować możliwość utworzenia raportów zawierających dane zebrane ze stacji roboczej i serwer centralnego zarządzania.
44. Serwer administracyjny musi oferować możliwość wyboru formy przedstawienia danych w raporcie w postaci tabeli, wykresu lub obu elementów jednocześnie.
45. Serwer administracyjny musi oferować możliwość określenia danych jakie powinny znajdować się w poszczególnych kolumnach tabeli lub na elementach wykresu oraz ich odfiltrowania i posortowania.
46. Serwer administracyjny musi być wyposażona w mechanizm importu oraz eksportu szablonów raportów.

47. Serwer administracyjny musi oferować możliwość wygenerowania raportu na żądanie, zgodnie z harmonogramem lub umieszczenie raportu na Panelu kontrolnym dostępnym z poziomu interfejsu konsoli WWW.
48. Raport generowany okresowo może zostać wysłany za pośrednictwem wiadomości email lub zapisany do pliku w formacie PDF, CSV.
49. Serwer administracyjny musi oferować możliwość skonfigurowania czasu automatycznego odświeżania raportu na panelu kontrolnym oraz umożliwiać jego odświeżenie na żądanie.
50. Serwer administracyjny musi oferować możliwość tworzenia wielu zakładek panelu, w których będą widoczne wybrane przez administratora elementy monitorujące.
51. Serwer administracyjny musi oferować możliwość maksymalizacji wybranego elementu monitorującego.
52. Raport na panelu kontrolnym musi być w pełni interaktywny pozwalając przejść do zarządzania stacją/stacjami, której raport dotyczy.
53. Serwer administracyjny musi oferować możliwość utworzenia własnych powiadomień lub skorzystanie z predefiniowanych wzorów.
54. Administrator musi posiadać możliwość wysłania powiadomienia za pośrednictwem wiadomości email .
55. Serwer administracyjny musi oferować możliwość konfiguracji własnej treści komunikatu w powiadomieniu.
56. Serwer administracyjny musi oferować możliwość dodania licencji do serwera zarządzania na podstawie klucza licencyjnego lub pliku offline licencji.
57. Serwer administracyjny musi oferować możliwość weryfikacji identyfikatora publicznego licencji, ilości wykorzystanych stanowisk, czasu wygaśnięcia, wersji produktu, na który jest licencja oraz jej właściciela.
58. Narzędzie administracyjne musi być wyposażone w mechanizm wyszukiwania zarządzanych komputerów na podstawie co najmniej nazwy komputera, adresu IPv4 i IPv6 lub wyszukania konkretnej nazwy zagrożenia.
59. Administrator musi mieć możliwość określenia zakresu czasu w jakim dane zadanie będzie wykonywane (sekundy, minuty, godziny, dni, tygodnie).

Czas trwania licencji 3 lata. Ochronie podlegać będzie co najmniej 5 serwerów plików Windows. Zamawiający posiada obecnie 68 licencji ESET Endpoint Antivirus NOD32 Suite ważnych do 31.07.2016. **W przypadku zaoferowania oprogramowania równoważnego konieczne jest jego wdrożenie w infrastrukturze zamawiającego obejmujące instalację na stacjach roboczych, instalację i konfiguracje serwera zdalnej administracji oraz min. 2 dniowe szkolenie jednego pracownika obejmujące wszystkie funkcje oprogramowania. Wdrożenie i szkolenie musi być przeprowadzone najpóźniej do 31.07.2016r.**

2.2 Pozostałe warunki realizacji zamówienia:

2.2.1 Zamówienie należy zrealizować w formie jednorazowej dostawy.

2.2.2 Wykonawca zobowiązany będzie dostarczyć przedmiot zamówienia do siedziby Zamawiającego **na swój koszt**.

2.2.3 Odbiór przedmiotu zamówienia nastąpi w siedzibie Powiatowego Urzędu Pracy w Ropczycach.

2.2.4 Złożenie oferty niezgodnej z opisem przedmiotu zamówienia określonym przez Zamawiającego skutkuje odrzuceniem oferty z postępowania. Za niezgodną z przedmiotem zamówienia uznaje się również ofertę, nie uwzględniającą pełnego zakresu przedmiotu zamówienia, lub ofertę zawierającą przedmiot zamówienia niezgodny z warunkami niniejszego zamówienia.

3. Termin i miejsce składania ofert:

do 08.07.2016r. godz. 12.00

Oferty należy składać na adres Zamawiającego:

POWIATOWY URZĄD PRACY w ROPCZYCACH
39-100 Ropczyce
ul. Najświętszej Marii Panny 2
I piętro pok. nr 12 – kancelaria

4. Termin wykonania zamówienia:

Termin realizacji zamówienia: **do 10 dni od podpisania umowy z Wykonawcą**.

5. Warunki udziału w postępowaniu i wykaz dokumentów na potwierdzenie ich spełniania:

Zamawiający nie precyzuje warunków udziału w postępowaniu.

6. Opis sposobu przygotowania oferty:

6.1 Zaleca się złożenie oferty na formularzu ofertowym przygotowanym przez Zamawiającego – wg wzoru stanowiącego załącznik nr **1 do zaproszenia.** W przypadku przygotowania oferty na innym formularzu Wykonawca umieści w nim wszelkie informacje i oświadczenia zawarte w formularzu ofertowym przygotowanym przez Zamawiającego.

6.2 Wykonawca zamieści ofertę w zamkniętej nieprzeźroczystej kopercie z napisem:

Oferta na dostawę oprogramowania antywirusowego
dla Powiatowego Urzędu Pracy w Ropczycach

nie otwierać przed 8 lipca 2016 r. – godz. 12^{30} WA.2510.1.107.2016.AK

6.3 Oferta powinna być czytelna i złożona w języku polskim.
Wszelkie zmiany w tekście oferty (przekreślenia, poprawki dopiski) powinny być podpisane lub parafowane przez Wykonawcę, w przeciwnym wypadku nie będą uwzględniane.

6.4 Ofertę podpisuje osoba lub osoby uprawnione do reprezentowania i składania oświadczeń woli w imieniu Wykonawcy. Jeżeli ofertę w imieniu Wykonawcy podpisuje pełnomocnik Wykonawcy, do oferty należy dołączyć **pełnomocnictwo**.

6.5 Oferta nie podpisana zostanie odrzucona w postępowaniu.

6.6 Na ofertę składają się następujące dokumenty:

6.6.1 **Wypełniony formularz ofertowy** – zgodnie z załącznikiem **nr 1**.

6.6.2 ***Pełnomocnictwo – jeżeli dotyczy***.

6.7 Termin związania ofertą wynosi 30 dni. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.

6.8 Wszelkie koszty związane przygotowaniem i złożeniem oferty ponosi Wykonawca.

6.9 Zamawiający nie dopuszcza składania ofert częściowych.

6.10 Zamawiający nie dopuszcza składania ofert wariantowych.

7. Otwarcie ofert nastąpi w dniu 08.07.2016r. godzina 12.30.

8. Opis sposobu obliczenia ceny oferty:

8.1 Przy wyliczaniu wartości ceny poszczególnych elementów należy ograniczyć się do dwóch miejsc po przecinku na każdym etapie wyliczenia ceny.
Jeżeli trzecia cyfra po przecinku jest mniejsza niż 5 to przy zaokrągleniu drugiej cyfry nie zmienia się, jeżeli trzecia cyfra po przecinku jest równa 5 lub większa, to drugą cyfrę należy zaokrąglić w górę.

8.2 Cena podana w ofercie musi obejmować wszystkie koszty związane z wykonaniem przedmiotu zamówienia w pełnym zakresie, w tym koszty dostawy oraz warunkami stawianymi przez Zamawiającego. **W przypadku zaoferowania rozwiązania równoważnego w cenie oferty Wykonawca uwzględni wdrożenie oprogramowania w infrastrukturze zamawiającego obejmujące instalację na stacjach roboczych, instalację i konfiguracje serwera zdalnej administracji oraz min. 2 dniowe szkolenie jednego pracownika obejmujące wszystkie funkcje oprogramowania.**

8.3 Rozliczenia pomiędzy Zamawiającym a Wykonawcą dokonywane będą w walucie „złoty polski".

8.4 Wykonawcy zobowiązani są podać w tabeli zawartej w formularzu ofertowym ilość, cenę jednostkową netto, cenę jednostkową brutto, stawkę VAT oraz wartości brutto. Ogólna cena brutto oferty winna być podana także słownie.

8.5 Cena określona przez Wykonawcę w tabeli cenowej obowiązuje na okres ważności oferty i umowy i nie może ulec zmianie.

9. Kryteria oceny ofert:

CENA – 100 %

Punktacja w tym kryterium zostanie obliczona wg wzoru:

Z = (Cn : Co) x 100

gdzie:

Cn – cena najniższa wśród ofert

Co – cena danego Wykonawcy

Obliczenia zostaną dokonane z dokładnością do dwóch miejsc po przecinku.

9.1 Ocenie podlegają wyłącznie oferty spełniające wymagania określone przez Zamawiającego w niniejszym zaproszeniu.

9.2 O wyborze najkorzystniejszej oferty zadecyduje największa ilość punktów uzyskanych przez Wykonawcę w kryterium cena.

9.3 Jeżeli nie będzie można dokonać wyboru oferty najkorzystniejszej ze względu na to, że dwie lub więcej ofert uzyskają taką samą liczbę punktów, Zamawiający wezwie Wykonawców, którzy złożyli te oferty, do złożenia, w wyznaczonym terminie, ofert dodatkowych. Zamawiający zastrzega, że Wykonawcy, składający oferty, nie mogą zaoferować cen wyższych niż zaoferowane w złożonych ofertach. Złożenie oferty dodatkowej zawierającej wyższą ceną skutkować będzie odrzuceniem oferty z postępowania.

10. Zawarcie umowy.

10.1 Zawarcie umowy nastąpi w terminie wyznaczonym przez Zamawiającego wg projektu stanowiącego załącznik nr 2 do zaproszenia. Przed podpisaniem umowy Zamawiający może żądać od Wykonawcy przedstawienia aktualnego odpisu z właściwego rejestru (KRS) lub centralnej ewidencji i informacji o działalności gospodarczej a w przypadku wykonawców wspólnie ubiegających się o zamówienie, umowy regulującej współpracę wykonawców.

11. Unieważnienie postępowania:

11.1 Zamawiający unieważni postępowanie o udzielenie zamówienia publicznego, jeżeli:
11.1.1 nie złożono żadnej oferty niepodlegającej odrzuceniu,
11.1.2 cena najkorzystniejszej oferty przewyższa kwotę, którą zamawiający może przeznaczyć na sfinansowanie zamówienia, chyba, że Zamawiający może zwiększyć tę kwotę do kwoty oferty najkorzystniejszej;
11.1.3 wystąpiła istotna zmiana okoliczności powodująca, że prowadzone postępowanie lub wykonanie zamówienia nie leży w interesie publicznym, czego nie można było wcześniej przewidzieć,
11.1.4. postępowanie obarczone jest wadą uniemożliwiającą zawarcie ważnej umowy w sprawie zamówienia,
11.1.5 z ważnych przyczyn, których nie można było wcześniej przewidzieć.

12. Ogłoszenie wyników prowadzonego postępowania

Zamawiający powiadomi e-mailowo lub faksem Wykonawców biorących udział w postępowaniu o wynikach oraz zamieści stosowną informacje na swojej stronie internetowej.

Uwagi: Ze względu na szacunkową wartość usługi (do 30 tys. euro) postępowanie prowadzone jest z wyłączeniem przepisów ustawy Prawo zamówień publicznych (Dz. U. z 2015 poz. 2164).

Załączniki:
1. Formularz ofertowy.
2. Projekt umowy.