**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA DLA CZĘŚCI IV**

|  |
| --- |
| **Parametry wymagane** |
| **Aktualizacja oprogramowania antywirusowego ESET Endpoint Protection Standard lub oprogramowanie równoważne – 725 szt.**  |
| 1 | **Zakres zamówienia.**Przedmiot zamówienia obejmuje aktualizację oprogramowania antywirusowego (odnowienie licencji dla ochrony 725 stacji roboczych oraz serwerów plików) i bazy danych sygnatur wirusów oprogramowania obecnie eksploatowanego w Warmińsko-Mazurskim Urzędzie Wojewódzkim w Olsztynie oraz w Delegaturach Urzędu w Elblągu i Ełku - ESET Endpoint Protection Standard w sieci komputerowej wraz z konsolą do zarządzania dla kompleksowej ochrony systemów komputerowych, z aktualizacją roczną. Rozpoczęcie usługi będzie liczone od dnia następującego po ostatnim dniu upływu okresu świadczenia aktualnie obowiązującej usługi, tj. w okresie od dnia 19.12.2020 r. do dnia 18.12.2021 r., lub krótszą – w zależności od dnia zawarcia umowy i terminu jej wykonania, lub dostarczenie oprogramowania równoważnego w ilości 725 szt. Rozpoczęcie usługi musi być liczone od dnia następującego po ostatnim dniu upływu okresu świadczenia aktualnie obowiązującej usługi. |
| 2 | **Równoważność oprogramowania antywirusowego** **w stosunku do oprogramowania określonego w specyfikacji istotnych warunków zamówienia**. Przez równoważność oprogramowania należy rozumieć spełnienie następujących wymagań:1. oferowane oprogramowanie musi spełniać wymagania określone w punkcie 3 zawierającym specyfikację wymagań funkcjonalnych oraz zapewniać osiągnięcie poziomu zabezpieczeń nie mniejszego niż oferowane przez mechanizmy wdrożonego u zamawiającego oprogramowania ESET Endpoint Protection Standard,
2. wykonawca wdroży oprogramowanie równoważne w terminie wskazanym w ofercie, przy czym okres od deinstalacji dotychczas funkcjonującego oprogramowania do wdrożenia zaproponowanego oprogramowania równoważnego nie może być dłuższy niż 3 dni robocze. Czynności wykonywane będą w godzinach pracy zamawiającego tj. od godz. 7:30 do godz. 15:30, od poniedziałku do piątku z wyjątkiem dni ustawowo wolnych od pracy,
3. wykonawca przeszkoli personel techniczny (6 osób) w zakresie używania, zarządzania oraz administrowania programem,
4. wykonawca przygotuje i przekaże zamawiającemu wersję elektroniczną instrukcji obsługi interfejsu użytkownika oprogramowania zainstalowanego na komputerze,
5. wykonawca dokona pełnej deinstalacji istniejącego oprogramowania w liczbie 725 licencji w następujących lokalizacjach: Olsztyn, Elbląg, Ełk, Grzechotki, Bezledy, Gronowo, Gołdap, łącznie z usunięciem wpisów w rejestrach systemowych,
6. wykonawca dokona zainstalowania oprogramowania na komputerach w liczbie zgodnej z liczbą wymaganych licencji.
 |
| 3 | **Specyfikacja wymagań funkcjonalnych.**1. **Wymagania ogólne:**
2. pełne wsparcie dla systemu Windows 7/Windows8/Windows 8.1/Windows 8.1 Update/Windows 10/Windows Server/Android,
3. wsparcie dla 32- i 64-bitowej wersji systemu Windows,
4. wersja programu dla stacji roboczych Windows dostępna w języku polskim,
5. pomoc w programie (help) i dokumentacja do programu dostępna w języku polskim,
6. skuteczność programu potwierdzona nagrodami VB100 i co najmniej dwie inne niezależne organizacje takie jak ICSA labs lub Check Mark.
7. **Ochrona antywirusowa i antyspyware:**
8. pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami,
9. program musi oferować funkcję samo ochrony,
10. wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.,
11. skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików,
12. możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu,
13. 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,
14. możliwość skanowania dysków sieciowych i dysków przenośnych,
15. skanowanie plików spakowanych i skompresowanych,
16. możliwość definiowania listy rozszerzeń plików, które mają być skanowane (w tym z uwzględnieniem plików bez rozszerzeń),
17. możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach,
18. możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu,
19. brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu,
20. 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,
21. skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Windows Mail,
22. możliwość definiowania różnych portów dla POP3 i IMAP, na których ma odbywać się skanowanie,
23. możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail,
24. skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie,
25. możliwość automatycznego wysyłania powiadomienia o wykrytych zagrożeniach do dowolnej stacji roboczej w sieci lokalnej,
26. w przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e‑mail,
27. możliwość definiowania różnych portów dla HTTP, na których ma odbywać się skanowanie,
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 uruchomienia zdalnego skanowania wybranych stacji roboczych z opcją wygenerowania raportu ze skanowania i przesłania do konsoli zarządzającej,
31. możliwość sprawdzenia z centralnej konsoli zarządzającej stanu ochrony stacji roboczej (aktualnych ustawień programu, wersji programu i bazy wirusów, wyników skanowania skanera na żądanie i skanerów rezydentnych),
32. możliwość sprawdzenia z centralnej konsoli zarządzającej podstawowych informacji dotyczących stacji roboczej: adresów IP, adresów MAC, wersji systemu operacyjnego oraz domeny, do której dana stacja robocza należy, ostatnio zalogowanego użytkownika,
33. możliwość centralnej aktualizacji stacji roboczych z serwera w sieci lokalnej lub Internetu,
34. możliwość skanowania sieci z centralnego serwera zarządzającego w poszukiwaniu niezabezpieczonych stacji roboczych,
35. dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe,
36. możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta,
37. możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy komputerze przy próbie dostępu do konfiguracji był proszony o podanie hasła,
38. 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,
39. hasło do zabezpieczenia konfiguracji programu oraz deinstalacji musi być takie samo,
40. 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,
41. 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,
42. 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,
43. 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,
44. automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń dostępna z Internetu,
45. możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami,
46. program musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji,
47. program musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji za pomocą wbudowanego w program serwera http,
48. program ma być wyposażony w dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, pracy zapory osobistej, modułu antyspamowego, kontroli stron Internetowych i kontroli urządzeń, skanowania na żądanie i według harmonogramu, dokonanych aktualizacji baz wirusów i samego oprogramowania,
49. wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.
50. **Administracja zdalna:**
51. serwer administracyjny musi oferować możliwość instalacji na systemach min. Windows Server 2012 oraz systemach Linux,
52. serwer administracyjny musi wspierać instalację w oparciu o co najmniej bazy danych MS SQL lub MySQL,
53. serwer administracyjny musi oferować możliwość wykorzystania już istniejącej bazy danych MS SQL lub MySQL użytkownika,
54. serwer administracyjny musi oferować możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy,
55. centralna administracja musi pozwalać na zarządzanie programami zabezpieczającymi na stacjach roboczych z systemami Windows, Mac OS X oraz Linux,
56. centralna administracja musi pozwalać na zarządzanie programami zabezpieczającymi na urządzeniach mobilnych z systemem Android,
57. centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware’ową, zaporą osobistą i kontrolą dostępu do stron internetowych zainstalowanymi na stacjach roboczych w sieci,
58. zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta,
59. administrator musi posiadać możliwość zarządzania za pomocą dedykowanego agenta stacjami nie posiadającymi zainstalowanego programu zabezpieczającego,
60. agent musi przekazywać informacje na temat stanu systemu operacyjnego do Serwer administracyjna zarządzającego,
61. instalacja agenta nie może wymagać określenia typu systemu (32 lub 64 – bitowy) oraz jego rodzaju (Windows, Mac, itp) a dobór odpowiedniego pakietu musi być w pełni automatyczny,
62. instalacja zdalna programu zabezpieczającego za pośrednictwem agenta musi odbywać się z repozytorium producenta lub z pakietu dostępnego w Internecie lub zasobie lokalnym,
63. serwer administracyjny musi oferować możliwość wyboru parametrów pakietu instalacyjnego zależnych od systemu operacyjnego oraz licencji na program zabezpieczający,
64. serwer administracyjny musi oferować możliwość deinstalacji programu zabezpieczającego firm trzecich lub jego niepełnej instalacji podczas instalacji nowego pakietu,
65. serwer administracyjny musi oferować możliwość wysłania komunikatu lub polecenia na stacje kliencką,
66. serwer administracyjny musi oferować możliwość utworzenia jednego zadania dla kilku klientów lub grupy,
67. serwer administracyjny musi oferować możliwość uruchomienia zadania automatycznie zgodnie z harmonogramem, po wystąpieniu nowego dziennika zdarzeń lub umieszczeniu nowego klienta w grupie dynamicznej,
68. serwer administracyjny musi oferować możliwość utworzenia grup statycznych i dynamicznych komputerów,
69. 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.,
70. serwer administracyjny musi oferować możliwość utworzenia polityk dla programów zabezpieczających i modułów serwera centralnego zarządzania,
71. 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,
72. edytor konfiguracji polityki musi być identyczny jak edytor konfiguracji ustawień zaawansowanych w programie zabezpieczającym na stacji roboczej,
73. 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,
74. serwer administracyjny musi umożliwiać wyświetlenie polityk do których przynależy dana stacja robocza oraz ich edycję z poziomu właściwości samego klienta,
75. serwer administracyjny musi oferować możliwość utworzenia własnych raportów lub skorzystanie z predefiniowanych wzorów,
76. serwer administracyjny musi oferować możliwość utworzenia raportów zawierających dane zebrane przez agenta ze stacji roboczej i serwer centralnego zarządzania,
77. serwer administracyjny musi oferować możliwość wygenerowania raportu na żądanie, zgodnie z harmonogramem lub umieszczenie raportu na Panelu kontrolnym dostępnym z poziomu interfejsu konsoli WWW,
78. raport generowany okresowo może zostać wysłany za pośrednictwem wiadomości email lub zapisany do pliku w formacie PDF, CSV lub PS,
79. serwer administracyjny musi oferować możliwość skonfigurowania czasu automatycznego odświeżania raportu na panelu kontrolnym oraz umożliwiać jego odświeżenie na żądanie,
80. serwer administracyjny musi oferować możliwość tworzenia wielu zakładek panelu, w których będą widoczne wybrane przez administratora elementy monitorujące,
81. serwer administracyjny musi oferować możliwość weryfikacji identyfikatora publicznego licencji, ilości wykorzystanych stanowisk, czasu wygaśnięcia, wersji produktu, na który jest licencja oraz jej właściciela,
82. 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,
83. administrator musi mieć możliwość określenia zakresu czasu w jakim dane zadanie będzie wykonywane (sekundy, minuty, godziny, dni, tygodnie).
 |