Sąd Rejonowy w Puławach

Oferta cenowa na dostawę programów antywirusowych.

Oferta cenowa na dostawę programów antywirusowych.

Metadane

Data wytworzenia : 12.06.2017
Data publikacji : 12.06.2017
Rejestr zmian

Podmiot udostępniający informację:
Sąd Rejonowy w Puławach

Osoba wytwarzająca/odpowiadająca za informację:
Iwona Wójcik

Osoba udostępniająca informację:
Arek Illek

Poprzedni Strona
Następny Strona

DYREKTOR
Sądu Rejonowego
w Puławach

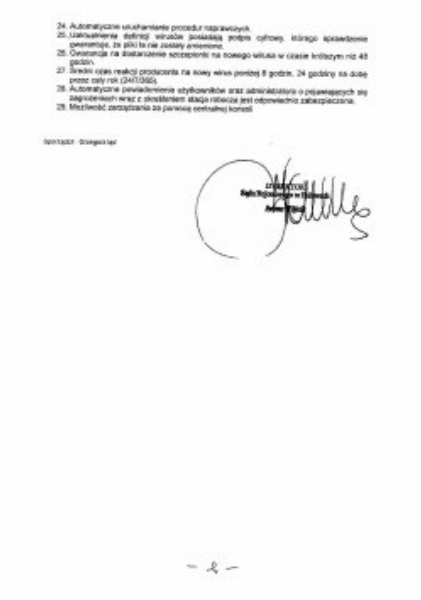
WYKONAWCY
WSZYSCY

Zapytanie Iwona Wójcik

Sąd Rejonowy
w Puławach
SĄD REJONOWY
ul. Lubelska 7
24-100 Puławy

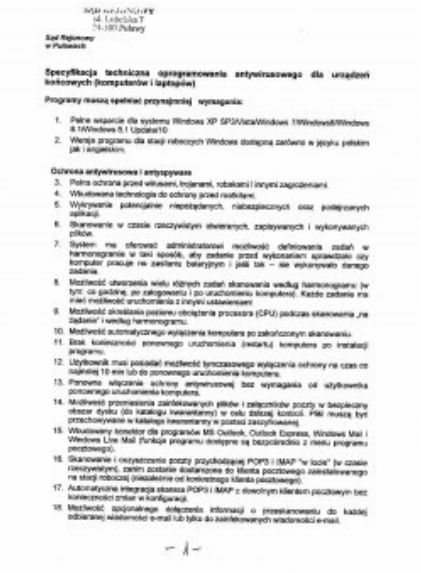
Specyfikacja techniczna oprogramowania antywirusowego dla serwerów

Serwer1 Iwona Wójcik



24. Automatyczne uruchamianie procedur naprawczych.
25. Uaktualnienia definicji wirusów posiadają podpis cyfrowy, który sprawdzenie gwarantuje, że pliki te nie zostały zmienione.
26. Gwarancja na dostarczenie szczepionki na nowego wirusa w czasie krótszym niż 48 godzin.
27. Średni czas reakcji producenta na nowy wirus poniżej 8 godzin. 24 godziny na dobę przez cały rok (24/7/365).
28. Automatyczne powiadomienie użytkowników oraz administratorów o pojawiających się zagrożeniach wraz z określeniem stacji roboczej jest odpowiednio zabezpieczona.
29. Możliwość zarządzania za pomocą centralnej konsoli

Serwer2 Iwona Wójcik



Sąd Rejonowy
w Pułtusku

Specyfikacja techniczna oprogramowania antywirusowego dla urządzeń końcowych (komputerów i laptopów)

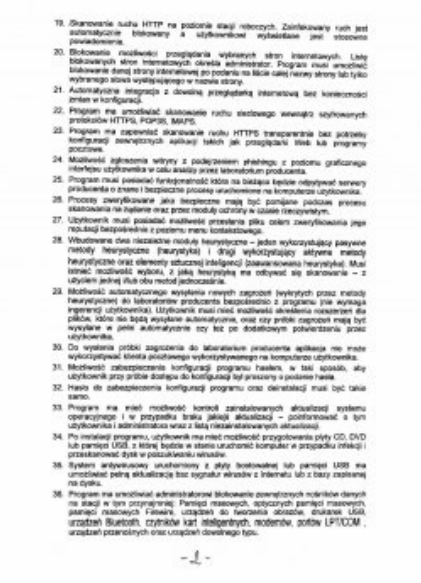
Programy muszą spełniać przynajmniej wymagania:

1. Pełne wsparcie dla systemu Windows XP SP3/Vista/Windows 7/Windows8/Windows 8.1/Windows 8.1 Update/10
2. Wersja programu dla stacji roboczych Windows dostępna zarówno w języku polskim jak i angielskim.

Ochrona antywirusowa i antyspyware

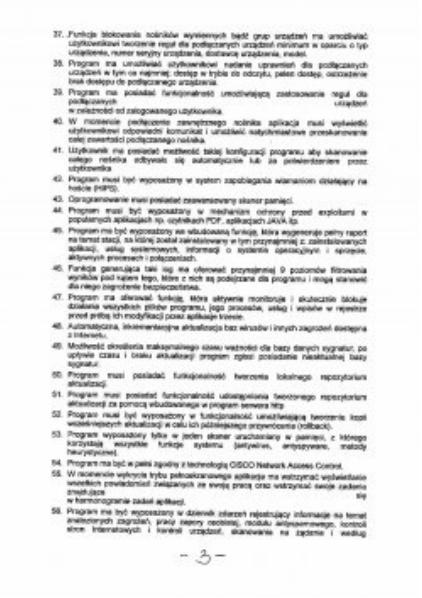
3. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
4. Wbudowana technologia do ochrony przed rootkitami.
5. Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
6. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
7. 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.
8. 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
9. Możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania („na żądanie" i według harmonogramu).
10. Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu.
11. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu.
12. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 15 min lub do ponownego uruchomienia komputera.
13. Ponowne włączanie ochrony antywirusowej bez wymagania od użytkownika ponownego uruchomienia komputera.
14. 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.
15. Wbudowany konektor dla programów MS Outlook, Outlook Express, Windows Mail i Windows Live Mail (funkcje programu dostępne są bezpośrednio z menu programu pocztowego).
16. Skanowanie i oczyszczenie poczty przychodzącej POP3 i IMAP "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
17. Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
18. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.

Komputer1 Iwona Wójcik



19. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.
20. 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.
21. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
22. Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz użytkowych protokołów HTTPS, POP3S, IMAPS.
23. Program ma zapewnić skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zaawansowanych aplikacji takich jak przeglądarki Web lub programy pocztowe.
24. Możliwość zgłoszenia witryny z podejrzeniem złośliwego, z poziomu graficznego interfejsu użytkownika w celu analizy przez laboratorium producenta.
25. Program musi posiadać funkcjonalność która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
26. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania na żądanie oraz przez moduły ochrony w czasie rzeczywistym.
27. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego.
28. 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 heurystyką ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
29. Możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystycznej) do laboratorium 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.
30. Do wysłania próbki zagrożenia do laboratorium producenta aplikacja nie może wykorzystywać klienta pocztowego wykorzystywanego na komputerze użytkownika.
31. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik przy próbie dostępu do konfiguracji był proszony o podanie hasła.
32. Hasło do zabezpieczenia konfiguracji programu oraz deinstalacji musi być takie samo.
33. 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.
34. Po instalacji programu, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której bootuje w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu wirusów.
35. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację bez sygnału wirusów z Internetu lub z bazy zapisanej na dysku.
36. Program ma umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM, urządzeń przenośnych oraz urządzeń dowolnego typu.

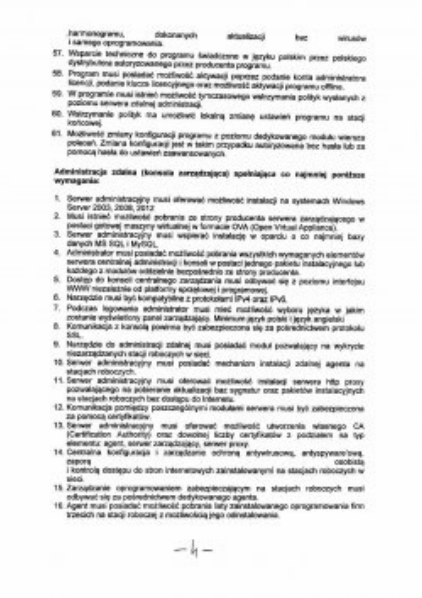
Komputer2 Grzegorz Ląd



37. Funkcja blokowania ścinków wybranych będź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia, model.
38. Program ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, całkowite brak dostępu do podłączanego urządzenia.
39. Program ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
40. W momencie podłączenia zewnętrznego ścinka aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej powierzchni podłączanego ścinka.
41. Użytkownik ma posiadać możliwość takiej konfiguracji programu aby skanowanie całego ścinka odbywało się automatycznie lub za potwierdzeniem przez użytkownika
42. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).
43. Oprogramowanie musi posiadać zaawansowany skaner pamięci.
44. Program musi być wyposażony w mechanizm ochrony przed exploitami w popularnych aplikacjach np. czytnikach PDF, aplikacjach JAVA, itp.
45. 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.
46. Funkcja generująca taki raport ma oferować przynajmniej 9 poziomów filtrowania wyników pod nazwą tego, które z nich są podejrzane dla programu i mogą stanowić dla niego zagrożenie bezpieczeństwa.
47. Program ma oferować funkcję, która uchronia monitoruje i skutecznie blokuje działania wszystkich plików programu, jego procesów, usług i wpisów w rejestrze przed próbą ich modyfikacji przez aplikacje trzecie.
48. Automatyczna, skonfigurowana aktualizacja baz wirusów i innych zagrożeń dostępna z Internetu.
49. Możliwość określenia maksymalnego czasu ważności dla bazy danych sygnatur, po upływie czasu i braku aktualizacji program zgłosi posiadanie nieaktualnej bazy sygnatur.
50. Program musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji.
51. Program musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji za pomocą wbudowanego w program serwera http.
52. Program musi być wyposażony w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji w celu ich późniejszego przywrócenia (rollback).
53. Program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (wirusy, antyspyware, malody heurystyczne).
54. Program ma być w pełni zgodny z technologią CISCO Network Access Control.
55. W momencie wykrycia trybu pełnoekranowego aplikacja ma wstrzymać wyświetlanie wszelkich powiadomień związanych ze swoją pracą oraz wstrzymać swoje zadania zmiany czasu się w harmonogramie zadań aplikacji.
56. Program ma być wyposażony w dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, pracy zapory osobistej, modułu antispamowego, kontroli stron internetowych i kontroli urządzeń, skanowania na żądanie i według

- 3 -

Komputer3 Iwona Wójcik



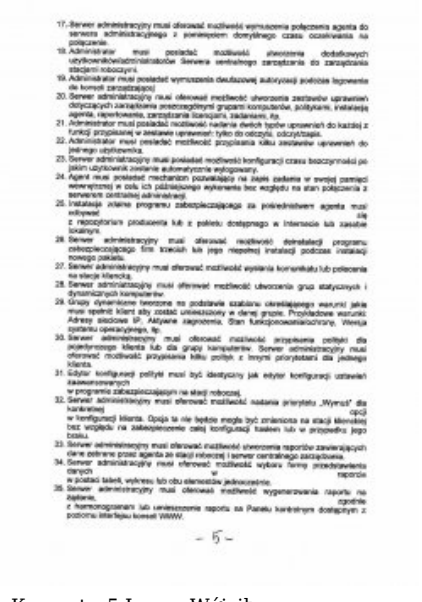
harmonogramu, dokonanych aktualizacji bez wirusów i całego oprogramowania.
57. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.
58. Program musi posiadać możliwość aktywacji poprzez podanie klucza administratora licencji, podanie klucza licencyjnego oraz możliwość aktywacji programu offline.
59. W programie musi istnieć możliwość tymczasowego wstrzymania polityk wysłanych z poziomu serwera zdalnej administracji.
60. Wstrzymanie polityk na urządzeniu lokalną zmianę ustawień programu na stacji końcowej.
61. Możliwość zmiany konfiguracji programu z poziomu dedykowanego modułu wiersza poleceń. Zmiana konfiguracji jest w takim przypadku autoryzowana bez hasła lub za pomocą hasła do ustawień zaawansowanych.

Administracja zdalna (konsola zarządzająca) spełniająca co najmniej poniższe wymagania:

1. Serwer administracyjny musi oferować możliwość instalacji na systemach Windows Server 2003, 2008, 2012
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 wspierać instalację w oparciu o co najmniej bazy danych MS SQL i MySQL.
4. Administrator musi posiadać możliwość pobrania wszystkich wymaganych elementów serwera centralnej administracji z konsoli w postaci jednego pakietu instalacyjnego lub każdego z osobna oddzielnie bezpośrednio ze strony producenta.
5. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW niezależnie od platformy systemowej i oprogramowań.
6. Narzędzie musi być kompatybilne z protokołami IPv4 oraz IPv6.
7. Podczas logowania administrator musi mieć możliwość wyboru języka w jakim zostanie wyświetlony panel zarządzający. Minimum język polski i język angielski
8. Komunikacja z konsolą powinna być zabezpieczona się za pośrednictwem protokołu SSL.
9. Narzędzie do administracji zdalnej musi posiadać moduł pozwalający na wykrycie niezarządzanych stacji roboczych w sieci.
10. Serwer administracyjny musi posiadać mechanizm instalacji zdalnej agenta na stacjach roboczych.
11. Serwer administracyjny musi oferować możliwość instalacji serwera http przy pozwalającego na pobieranie aktualizacji bez sygnatur oraz pakietów instalacyjnych na stacjach roboczych bez dostępu do Internetu.
12. Komunikacja pomiędzy poszczególnymi modułami serwera musi być zabezpieczona za pomocą certyfikatów.
13. Serwer administracyjny musi oferować możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy.
14. Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware'ową, zaporą osobistą i kontrolą dostępu do stron internetowych zainstalowanymi na stacjach roboczych w sieci.
15. Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta.
16. Agent musi posiadać możliwość pobrania listy zainstalowanego oprogramowania firm trzecich na stacji roboczej z możliwością jego odinstalowania.

- 4 -

Komputer4 Iwona Wójcik



17. Serwer administracyjny musi oferować możliwość wymuszenia połączenia agenta do serwera administracyjnego z pominięciem domyślnego czasu oczekiwania na połączenie.
18. Administrator musi posiadać możliwość stworzenia dodatkowych użytkowników/administratorów Serwera centralnego zarządzania do zarządzania stacjami roboczymi.
19. Administrator musi posiadać wymuszenia dwuetapową autoryzację podczas logowania do konsoli zarządzającej
20. Serwer administracyjny musi oferować możliwość stworzenia zestawów uprawnień dotyczących zarządzania poszczególnymi grupami komputerów, politykami, instalacją agenta, raportowania, zarządzania licencjami, zadaniami, itp.
21. Administrator musi posiadać możliwość nadania dwóch typów uprawnień do każdej z funkcji przypisanej w zestawie uprawnień: tylko do odczytu, odczyt/zapis.
22. Administrator musi posiadać możliwość przypisania kilku zestawów uprawnień do jednego użytkownika.
23. Serwer administracyjny musi posiadać możliwość konfiguracji czasu bezczynności po jakim użytkownik zostanie automatycznie wylogowany.
24. Agent musi posiadać mechanizm pozwalający na zapis zadania w swojej pamięci wewnętrznej w celu ich późniejszego wykonania bez względu na stan połączenia z serwerem centralnej administracji.
25. Instalacja zdalna programu zabezpieczającego za pośrednictwem agenta musi odbywać się z repozytorium producenta lub z pakietu dostępnego w Internecie lub zasobie lokalnym.
26. Serwer administracyjny musi oferować możliwość dezinstalacji programu zabezpieczającego firm trzecich lub jego niepełnej instalacji podczas instalacji nowego pakietu.
27. Serwer administracyjny musi oferować możliwość wysłania komunikatu lub polecenia na stacje klienckie.
28. Serwer administracyjny musi oferować możliwość utworzenia grup statycznych i dynamicznych komputerów.
29. Grupy dynamiczne tworzone na podstawie szablonu określającego warunki jakie musi spełnić klient aby został umieszczony w danej grupie. Przykładowe warunki: Adres sieciowe IP, Aktywna zagrożenia, Stan funkcjonowania/ochrony, Wersja systemu operacyjnego, itp.
30. Serwer administracyjny musi oferować możliwość przesłania polityki dla jednorazowego klienta lub dla grupy komputerów. Serwer administracyjny musi oferować możliwość przypisania kilku polityk z innymi priorytetami dla jednego klienta.
31. Edytor konfiguracji polityki musi być identyczny jak edytor konfiguracji ustawień zaawansowanych w programie zabezpieczającym na stacji roboczej.
32. 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.
33. Serwer administracyjny musi oferować możliwość stworzenia raportów zawierających dane pobrane przez agenta ze stacji roboczej i serwer centralnego zarządzania.
34. Serwer administracyjny musi oferować możliwość wyboru formy przedstawienia danych w raporcie w postaci tabeli, wykresu, lub obu elementów jednocześnie.
35. Serwer administracyjny musi oferować możliwość wygenerowania raportu na żądanie, cyklicznie z harmonogramem lub zwielokrotnienie raportu za Panelu konkretnym dostępnym z poziomu interfejsu konsoli WWW.

- 5 -

Komputer5 Iwona Wójcik

36. Raport generowany okresowo może zostać wysłany za pośrednictwem wiadomości email lub zapisany do pliku w formacie PDF, CSV lub Pli.
37. Serwer administracyjny musi oferować możliwość maksymalizacji wybranego elementu monitorującego.
38. Raport na panelu kontrolnym musi być w pełni interaktywny pozwalając przejść do zarządzania stacjami/agentami, której raport dotyczy.
39. Administrator musi posiadać możliwość wysłania powiadomienia za pośrednictwem wiadomości email lub komunikatu SNMP.
40. Serwer administracyjny musi oferować możliwość konfiguracji własnej treści komunikatu
w powiadomieniu.
41. Serwer administracyjny musi oferować możliwość podłączenia serwera administracji zdalnej do portalu zarządzania licencjami dostępnego na serwerze producenta.
42. Serwer administracyjny musi oferować możliwość dodania licencji do serwera bezpośrednio na podstawie klucza licencyjnego lub pliku offline licencji.
43. Serwer administracyjny musi posiadać możliwość dodania dowolnej ilości licencji obejmujących różne produkty.
44. Serwer administracyjny musi być wyposażone w mechanizm autodopasowania kolumn w zależności od rozdzielczości urządzenia na jakim jest wyświetlana.
45. Administrator musi mieć możliwość określenia zakresu czasu, w jakim dane zadanie będzie wykonywane (sekundy, minuty, godziny, dni, tygodnie).
46. Serwer administracji musi umożliwić granularne uprawnienia dla Administratorów w taki sposób, aby każdemu z nich możliwe było przyznanie oddzielnych uprawnień do poszczególnych grup komputerów, polityk lub zadań.

Zamawiający
Grzegorz Lipa

Komputer6 Iwona Wójcik