Zał. Nr 3 do postępowania PO 2/25

OPIS OPROGRAMOWANIA ANTYWIRUSOWEGO

Opis funkcjonalny oprogramowania antywirusowego:

- Oprogramowanie ma być zarządzane przy użyciu konsoli centralnej
- Oprogramowanie ma zapewnić zabezpieczenie:
    - Ochrona systemów serwerowych,
    - Ochrona stacji roboczych
    - Ochrona urządzeń mobilnych,
    - Pełne szyfrowanie dysków,
    - Sandboxing w chmurze,
    - Ochrona aplikacji w chmurze,
    - Zarządzanie podatnościami,
    - Bezpieczeństwo serwerów pocztowych,
    - Uwierzytelnianie wieloskładnikowe,
    - Rozszerzone wykrywanie i reagowanie,

1. Ochrona antywirusowa i antyspyware:

1.1. pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami,

1.2. program musi oferować funkcję samo ochrony,

1.3. wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.,

1.4. skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików,

1.5. możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu,

1.6. 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,

1.7. możliwość skanowania dysków sieciowych i dysków przenośnych,

1.8. skanowanie plików spakowanych i skompresowanych,

1.9. możliwość definiowania listy rozszerzeń plików, które mają być skanowane (w tym z uwzględnieniem plików bez rozszerzeń),

1.10. możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach,

1.11. możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu,

1.12. brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu,

1.13. 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,

1.14. skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Windows Mail,

1.15. możliwość definiowania różnych portów dla POP3 i IMAP, na których ma odbywać się skanowanie,

1.16. możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail,

1.17. skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie,

1.18. możliwość automatycznego wysyłania powiadomienia o wykrytych zagrożeniach do dowolnej stacji roboczej w sieci lokalnej,

1.19. w przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e-mail,

1.20. możliwość definiowania różnych portów dla HTTP, na których ma odbywać się skanowanie,

1.21. program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów

HTTPS, POP3S, IMAPS,

1.22. program ma zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe,

1.23. możliwość uruchomienia zdalnego skanowania wybranych stacji roboczych z opcją wygenerowania raportu ze skanowania i przesłania do konsoli zarządzającej,

1.24. 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),

1.25. 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,

1.26. możliwość centralnej aktualizacji stacji roboczych z serwera w sieci lokalnej lub Internetu,

1.27. możliwość skanowania sieci z centralnego serwera zarządzającego w poszukiwaniu niezabezpieczonych stacji roboczych,

1.28. dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe,

1.29. możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta,

1.30. możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy komputerze przy próbie dostępu do konfiguracji był proszony o podanie hasła,

1.31. 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,

1.32. hasło do zabezpieczenia konfiguracji programu oraz deinstalacji musi być takie samo,

1.33. 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,

1.34. 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,

1.35. 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,

1.36. 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,

1.37. automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń dostępna z Internetu,

1.38. możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami,

1.39. program musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji,

1.40. program musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji za pomocą wbudowanego w program serwera http,

1.41. 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,

1.42. wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.

Zamawiający oczekuje dostawy 280 licencji ESET PROTECT Elite (lub równoważnych). Licencje mają być przedłużone na okres 12 m-cy od daty zakończenia dotychczasowej licencji.