**Opis przedmiotu zamówienia**

**część 4: Zakup oprogramowania antywirusowego dla Urzędu Miejskiego w Nowym Tomyślu**

# Szczegółowe wymagania techniczne dla programu antywirusowego.

Miejsce dostawy: Urząd Miejski w Nowym Tomyślu, ul. Poznańska 33, 64-300 Nowy Tomyśl

Okres obowiązywania licencji na 36 miesięcy.

Wymagana dostawa oprogramowania antywirusowego dla 100 stanowisk wraz z wdrożeniem, instalacją i konfiguracją konsoli administracyjnej z implementacją w środowisku zamawiającego zgodnie z wymaganiami zamawiającego. Sprawdzenie poprawności działania przedmiotu zamówienia w środowisku zamawiającego oraz szkoleniem z obsługi oprogramowania.

|  |  |
| --- | --- |
| **L.p.** | **Wymagania minimalne** |
| **1.** | **Administracja zdalna / konsola** |
| 1.1. | Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego. |
| 1.2. | Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW. |
| 1.3. | Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL. |
| 1.4. | Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji. |
| 1.5. | Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy. |
| 1.6. | Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM. |
| 1.7. | Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej. |
| 1.8. | Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak. |
| 1.9. | Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta. |
| 1.10. | Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów. |
| 1.11. | Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera. |
| 1.12. | Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej. |
| **2.** | **Ochrona stacji roboczych** |
| 2.1. | Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11). |
| 2.2. | Rozwiązanie musi wspierać architekturę ARM64. |
| 2.3. | Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. |
| 2.4. | Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet. |
| 2.5. | Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. |
| 2.6. | Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. |
| 2.7. | Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. |
| 2.8. | Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych. |
| 2.9. | Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku. |
| 2.10. | Rozwiązanie musi integrować się z Intel Threat Detection Technology. |
| 2.11. | Rozwiązanie musi zapewniać skanowanie i oczyszczanie 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). |
| 2.12. | Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. |
| 2.13. | Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. |
| 2.14. | Rozwiązanie musi zapewniać 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 oraz urządzeń przenośnych. |
| 2.15. | Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia. |
| 2.16. | Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów: 1. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika, 2. tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie, 3. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika, 4. tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach, 5. tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach. |
| 2.17. | Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników. |
| 2.18. | Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa. |
| 2.19. | Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji. |
| 2.20. | Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). |
| 2.21. | Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. |
| 2.22. | Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook. |
| 2.23. | Zapora osobista rozwiązania musi pracować w jednym z czterech trybów: 1. tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące, 2. tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie, 3. tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora, 4. tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu. |
| 2.24. | Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki. |
| 2.25. | Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika. |
| 2.26. | Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki. |
| 2.27. | Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych. |
| 2.28. | Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii. |
| 2.29. | Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day. |
| 2.30. | W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum. |
| **3.** | **Ochrona serwera** |
| 3.1. | Rozwiązanie musi wspierać systemy Microsoft Windows Server oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL), Rocky Linux, Ubuntu, Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux oraz Amazon Linux. |
| 3.2. | Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami. |
| 3.3. | Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. |
| 3.4. | Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS. |
| 3.5. | Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. |
| 3.6. | Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji. |
| 3.7. | Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów. |
| 3.8. | Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty. |
| **4.** | **Dodatkowe wymagania dla ochrony serwerów Windows:** |
| 4.1. | Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive. |
| 4.2. | Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS). |
| 4.3. | Rozwiązanie musi wspierać skanowanie magazynu Hyper-V. |
| 4.4. | Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. |
| 4.5. | Rozwiązanie musi zapewniać 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 oraz urządzeń przenośnych. |
| 4.6. | Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki. |
| 4.7. | Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych. |
| 4.8. | Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP. |
| 4.9. | Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu. |
| **5.** | **Dodatkowe wymagania dla ochrony serwerów LINUX:** |
| 5.1. | Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej. |
| 5.2. | Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web. |
| 5.3. | Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon. |
| 5.4. | Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu. |
| **6.** | **Szyfrowanie** |
| 6.1. | System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 10 i Microsoft Windows 11. |
| 6.2. | System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault). |
| 6.3. | Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia. |
| 6.4. | Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI. |
| **7.** | **Ochrona urządzeń mobilnych opartych o system ANDROID** |
| 7.1. | Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie. |
| 7.2. | Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne. |
| 7.3. | Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki). |
| 7.4. | Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM. |
| 7.5. | Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi: 1. usunięcie zawartości urządzenia, 2. przywrócenie urządzenie do ustawień fabrycznych, 3. zablokowania urządzenia, 4. uruchomienie sygnału dźwiękowego, 5. lokalizację GPS. |
| 7.6. | Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji. |
| 7.7. | Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o: 1. nazwę aplikacji, 2. nazwę pakietu, 3. kategorię sklepu Google Play, 4. uprawnienia aplikacji, 5. pochodzenie aplikacji z nieznanego źródła. |
| **8.** | **Sandbox w chmurze** |
| 8.1. | Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day. |
| 8.2. | Rozwiązanie musi wykorzystywać do działania chmurę producenta. |
| 8.3. | Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi. |
| 8.4. | Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta. |
| 8.5. | Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek. |
| 8.6. | Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania. |
| 8.7. | Po zakończonej analizie pliku, rozwiązanie musi przesyłać wynik analizy do wszystkich wspieranych produktów. |
| 8.8. | Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy. |
| 8.9. | Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione. |
| 8.10. | Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych. |
| 8.11. | Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzeć jakie pliki zostały wysłane do analizy oraz przez kogo. |
| 8.12. | Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem: 1. Czysty, 2. Podejrzany, 3. Bardzo podejrzany, 4. Szkodliwy. |
| 8.13. | W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum. |
| 8.14. | W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki. |
| 8.15. | Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia. |
| **9.** | **Moduł XDR** |
| 9.1. | Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW. |
| 9.2. | Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego producenta. |
| 9.3. | Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL. |
| 9.4. | Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa. |
| 9.5. | Wykluczenia muszą dotyczyć procesu lub procesu „rodzica”. |
| 9.6. | Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia. |
| 9.7. | Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika. |
| 9.8. | Serwer musi posiadać ponad 900 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator musi też posiadać możliwość utworzenia własnych reguł i edycji reguł dodanych przez producenta. |
| 9.9. | Serwer administracyjny musi oferować możliwość blokowania plików po sumach kontrolnych. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej. |
| 9.10. | Administrator musi posiadać możliwość weryfikacji uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku. |
| 9.11. | Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania. |
| 9.12. | Administrator musi posiadać możliwość weryfikacji uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny. |
| 9.13. | W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej. |
| 9.14. | W ramach przeglądania wykonanego skryptu lub pliku exe, administrator musi posiadać możliwość weryfikacji powiązanych zdarzeń dotyczących przynajmniej: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych. |
| 9.15. | Serwer administracyjny musi oferować możliwość przekierowania do konsoli zarządzającej produktu antywirusowego tego samego producenta, w celu weryfikacji szczegółów wybranej stacji roboczej. W konsoli zarządzającej produktu antywirusowego, administrator musi mieć możliwość podglądu informacji dotyczących przynajmniej: podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich. |
| 9.15. | Konsola administracyjna musi mieć możliwość tagowania obiektów. |
| 9.16. | Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń powershell. |
| **10.** | **Wsparcie** |
| 10.1. | W okresie gwarancji (okres równy okresowi licencji) wykonawca zobowiązany jest świadczyć usługi wparcia technicznego w wymiarze 24 godzin w ciągu roku kalendarzowego. Usługi wsparcia muszą być świadczone przez osobę posiadającą certyfikat techniczny producenta rozwiązania (Zamawiający zastrzega sobie prawo weryfikacji posiadania ww. certyfikatu). |