Załącznik nr 2

OPIS PRZEDMIOTU ZAMÓWIENIA DLA

Miejski Ośrodek Pomocy Społecznej w Augustowie

Przedmiotem zamówienia jest:

1. Przedmiotem zamówienia jest dostawa oprogramowania antywirusowego, spełniającego wymagania specyfikacji wraz ze szkoleniem administratora tego oprogramowania i usługą weryfikacji jego konfiguracji na okres od dnia podpisania protokołu zdawczo-odbiorczego do dnia 17 kwietnia 2026 r.
2. Kod CPV: 48761000-0 - Pakiety oprogramowania antywirusowego
3. Wymagania:

	Nazwa elementu, parametru lub cechy	Wartość/występowanie
Podstawowe cechy	Zgodność z systemami operacyjnymi fizycznymi i wirtualnymi	Windows : 7 SP 1, 10 wersja 22H2 , 11 - wszystkie edycje, Windows Server 2019 i 2022 z funkcjonalnością Hyper-V Hypervisor
	Rodzaj konsoli zarządzania	chmurowa
Funkcjonalność ochrony przed cyberzagrożeniami	1. Pełna ochrona przed zagrożeniami, wymienionymi na stronie: https://www.gov.pl/web/baza-wiedzy/zagr-techniczne 2. Wbudowana ochrona przed exploitami. Funkcja umożliwia również: a) Możliwość wymuszenia funkcji DEP systemu Windows b) Możliwość wymuszenia relokacji modułów (ASLR) 3. Możliwość wykrywania i blokowania ataków typu ransomware niezależnie od tego czy atak został przeprowadzony lokalnie lub zdalnie na punkcie końcowym oraz utworzenie kopii zapasowej plików a w przypadku ataku odzyskanie i przywrócenie ich do pierwotnej lokalizacji.	Tak, wykrywanie, usuwanie i blokowanie minimum 15 różnych technik wykrywania eksploitów z możliwością włączenia lub wyłączenia każdej z nich oraz dająca możliwość dodania własnych procesów cab, cer, dll, doc, docm, docx, exe, ini, mdf, msg,

	Nazwa elementu, parametru lub cechy	Wartość/występowanie
	4. Możliwość odzyskania plików na żądanie lub automatycznego odzyskiwania. 5. Musi być możliwość odzyskania plików w następujących formatach:	odt, pdf, pem, py, xls, xlsx, xml
Funkcjonalność zarządzania ryzykiem	System zarządzania ryzykiem winien być zintegrowany z konsolą zarządzającą systemem, który pozwala oszacować podatność środowiska na atak na podstawie punktów ryzyka. Punkty ryzyka powinny być przydzielane od 0 do 100 gdzie liczba mniejsza stanowi mniejsze ryzyko a liczba większa większe ryzyko. Ponadto musi posiadać: a) Funkcję, która pozwala wykrywać błędne konfiguracje oraz naprawiać je lub ignorować z podziałem na typ błędnej konfiguracji: - Ochrony przeglądarki internetowej - Sieć i poświadczenia - Błędna konfiguracja systemu operacyjnego b) System ponadto musi określać nasilenie tych błędnych konfiguracji w oparciu o punkty procentowe. c) System zarządzania ryzykiem który powinien wykrywać luki w aplikacjach podając przy tym numer CVE tych luk. d) System, który pozwala na śledzenie i wykrywanie niezwyczajnych działań jakie podejmuje użytkownik na punkcie końcowym wraz z poinformowaniem ilu użytkowników takie działanie dotyczy oraz jakie jest jego nasilenie. e) System pozwala na skanowanie punktów końcowych pod kątem wykrywania ryzyka na podstawie harmonogramu lub pojedynczo utworzonego zadania. f) System pozwala na raportowanie na ilu urządzeniach wykryto błędną konfigurację i luki w aplikacjach oraz jaka jest ilość takich podatności i ich nasilenie wyrażone w procentach. g) System pozwala na raportowanie u ilu użytkowników wykryto podejrzane działania oraz jakie jest ich nasilenie	

	Nazwa elementu, parametru lub cechy	Wartość/występowanie
Funkcjonalność Ochrony przed zagrożeniami od strony plików i folderów	1. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików 2. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" 3. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym 4. Możliwość skanowania dysków sieciowych i dysków przenośnych 5. Skanowanie plików spakowanych i skompresowanych. 6. Możliwość dodawania wykluczeń na podstawie a) Plik b) Folder c) Rozszerzenie d) Proces e) Hash pliku f) Hash certyfikatu g) Nazwa zagrożenia h) Wiersz poleceń i) IP/maska 7. Możliwość definiowania czy pliki z kwarantanny mają być przesyłane do producenta i co jaki czas ma się ta czynność odbywać.	
Funkcjonalność ochrony przed atakami sieciowymi	1. Skanowanie ruchu HTTP na poziomie stacji roboczych; zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie 2. Skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, RDP, FTPS, SCP/SSH 3. Skanowanie ruch HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe 4. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji 5. Blokowanie wysyłanych przez http lub smtp adresów e-mail, PIN-ów, numerów kont bankowych, haseł itp. 6. Mechanizm obronny przed atakującymi próbującymi uzyskać dostęp do systemu	

	Nazwa elementu, parametru lub cechy	Wartość/występowanie
	poprzez wykorzystanie luk w sieci. Funkcja ta musi obejmować ochroną przed technikami takimi jak: - Wczesny dostęp - Dostęp do poświadczeń - Wykrycie - Crimeware 7. Wbudowana zapora, umożliwiająca tworzenie reguł na podstawie aplikacji oraz ruchu sieciowego 8. Wbudowany IDS 9. Możliwość tworzenia list sieci zaufanych 10. Możliwość dezaktywacji funkcji zapory sieciowej.	
Funkcjonalność dodatkowej warstwy ochrony	1. Ochrona proaktywna winna być oparta o maszynowe uczenie, która działa w fazie poprzedzającej wykonanie, ochrona ta musi wy wykrywać zagrożenia takie jak: a) Ukierunkowane ataki b) Podejrzane pliki i ruch w sieci c) Exploity d) Ransomware e) Grayware 2. Moduł ochrony proaktywnej musi posiadać oddzielne działania jakie będzie podejmował dla plików i oddzielne dla ruchu sieciowego 3. Moduł ochrony proaktywnej musi działać w trybach, które administrator może dowolnie zmieniać na: a) Tolerancyjny b) Normalny c) Agresywny	
Funkcjonalność Endpoint Detection and Response	1. Czujnik EDR, który gromadzi i przetwarza dane w celu raportowania danych dotyczących punktu końcowego i zachowania aplikacji. 2. Oddzielny komponent służący do interpretacji metadanych gromadzonych przez czujnik EDR. 3. Możliwość instalacji dodatkowego, lekkiego agenta z czujnikiem EDR dla urządzeń z systemem Windows, aby rozszerzyć już zainstalowaną ochronę. Agent posiada też ochronę urządzenia i ruchu sieciowego oraz filtr stron internetowych. **4. Funkcjonalności:** **4.1. Wykrywanie podejrzanej aktywności**	

	Nazwa elementu, parametru lub cechy	Wartość/występowanie
	Monitorowanie zdarzeń na punktach końcowych w poszukiwaniu oznak ataku i wywoływanie incydentów po wykryciu takiej aktywności. - Bazowanie na systemach bazujących na wskaźnikach ataku MITRE i własnej inteligencji. - Zgłaszanie wszystkich naruszeń jako incydent w funkcjonalności EDR. **4.2. Badanie incydentów i wizualizacja** Zapewnienie wsparcia analizy incydentów poprzez dostarczenie narzędzi, które pomagają filtrować, badać i podejmować działania dotyczące wszystkich zdarzeń bezpieczeństwa wykrytych przez czujnik EDR w określonym przedziale czasu. Integrowanie się z bazą wiedzy ATT & CK firmy MITRE i odpowiednio oznaczanie zdarzeń bezpieczeństwa. Zapewnienie zaawansowanej wizualizacji zdarzeń bezpieczeństwa z określonymi informacjami lub działaniami z następującymi informacjami: a) Możliwość przeglądu wpływu zdarzenia i szczegółowe informacje o każdym węźle zdarzenia b) Możliwość zbierania informacji o rozwoju zdarzenia bezpieczeństwa w kolejności chronologicznej. c) Działania naprawcze muszą gromadzić informacje o działaniach blokujących automatycznie podejmowanych przez produkt w związku z bieżącym zdarzeniem bezpieczeństwa. **4.3 .Incydenty** Informowanie o zagrożeniach wykrytych i zablokowanych w formie grafu i linii zdarzeń oraz możliwość: a) Filtrowania zdarzeń b) Blokowania procesów c) Dodawanie procesów do czarnej listy d) Dodawanie procesów do białej listy e) Izolacji hosta f) Aktualizacja oprogramowania firm trzecich na hoście g) Przesłanie pliku do piaskownicy h) Sprawdzenie informacji o pliku w Google	

	Nazwa elementu, parametru lub cechy	Wartość/występowanie
	i) Sprawdzenie informacji o pliku w VirusTotal	
Funkcjonalność piaskownicy	1. Zintegrowany sandbox działający po stronie producenta, który pozwala na analizę pliku, przy czym: a) Plik może zostać wysłany automatycznie ze stacji roboczej, jeżeli oprogramowanie uzna go za podejrzany lub ręcznie z poziomu konsoli przez administratora b) Możliwość przesłania archiwum zabezpieczonego hasłem c) Możliwość przesłania adresu URL d) W przypadku przesłania wielu plików jednorazowo, możliwość detonacji próbek pojedynczo. 2. Wbudowany sandbox musi działać w trybie monitorowania i blokowania 3. Wbudowany sandbox musi oferować działania naprawcze takie jak dezynfekcja lub przeniesienie do kwarantanny 4. Wbudowany sandbox musi oferować opcję wstępnego filtrowania zawartości, która skanuje pliki, argumenty wiersza poleceń i adresy URL pod kątem podejrzanego zachowania. 5. Wbudowany sandbox musi posiadać opcję, która pozwala na dodanie określonych rozszerzeń do wyjątków, pliki z tym rozszerzeniem nie zostaną przesłane do sandboxa. 6. Minimalny rozmiar pliku jaki może zostać przesłany do sandboxa 7. Maksymalny rozmiar pliku jaki może zostać przesłany do sandboxa.	1 KB 50 MB
Funkcjonalność ochrony poczty	1. Ochrona przed phishingiem i podszywaniem się, antymalware, antyspam, antyspoofing 2. Filtracja wiadomości w oparciu o atrybuty takie jak rozmiar, źródło, miejsce docelowe, słowa kluczowe 3. Filtracja wiadomości dla zawartości wiadomości wychodzących, aby zapobiec wpisaniu ich na czarną listę IP. 4. Modyfikowanie linków w wiadomościach w czasie rzeczywistym, blokowanie złośliwych linów i ostrzeganie przed nimi użytkowników poczty.	

	Nazwa elementu, parametru lub cechy	Wartość/występowanie
	5. Ochrona, polegająca na przekierowaniu przychodzącej wiadomości e-mail przez serwery producenta w chmurze poprzez zmianę rekordu MX na specjalny portal producenta	
Funkcjonalność szyfrowanie dysku	1. Pełne szyfrowanie dysków (FDE- Full disk ecryption) 2. Szyfrowanie dysków korzysta z natywnej funkcji Bitlocker na systemach Windows 3. Możliwość szyfrowania i deszyfrowania punktów końcowych poprzez politykę bezpieczeństwa zastosowaną na komputerach. 4. Generowanie klucza odzyskiwania do funkcji Bitlocker z konsoli administracyjnej. 5. Użytkownik musi ustawić hasło do funkcji szyfrowania zgodnie z wymaganiami. 6. Liczba licencji jest zależna od ilości systemów operacyjnych, nie od ilości dysków na komputerze. 7. Szyfrowanie wymaga podania hasła przed odblokowaniem systemu operacyjnego/ dysku. 8. Moduł Szyfrowania zapewnia zgodność wymogami HIPPA, PCI, DSS, GDPR odnośnie szyfrowania danych. 9. Rozwiązanie nie wymaga dodatkowego klienta, czy serwera zarządzającego do zarządzania modułem szyfrowania. 10. Rozwiązanie pozwala na wykorzystywanie modułu szyfrowania w trybie licencjonowania miesięcznego przez dostawcę usługi. 11. Administrator ma możliwość ustawienia czy system szyfrujący ma pytać o hasło w momencie uruchomienia systemu operacyjnego, jeśli aktywny jest moduł TPM. 12. Możliwość automatycznego zaimportowania klucza odzyskiwania do konsoli szyfrowania, jeżeli maszyna została zaszyfrowana ręcznie przed zainstalowaniem oprogramowania antywirusowego 13. Możliwość dodania wyjątków od szyfrowania dla dysków innych niż systemowe. 14. Break konieczności posiadania funkcji TPM	
Funkcjonalność zarządzanie	1. Możliwość działania w trybie automatycznym, w tym:	

	Nazwa elementu, parametru lub cechy	Wartość/występowanie
aktualizacjami systemu i oprogramowania	a) Możliwość oszacowania brakujących łatek b) Możliwość zaplanowania oddzielnej automatycznej instalacji w oparciu o kategorię poprawek (bezpieczeństwo / niezwiązane z zabezpieczeniami) c) Możliwość opóźnienia ponownego uruchomienia, jeśli instalacja łatki tego wymaga 2. Rozwiązanie musi zezwalać na tryb manualny – wykrywanie i instalacje łatek na żądanie 3. Rozwiązanie musi oferować możliwość podejrzenia wszystkich brakujących łatek ze środowiska. Informacje te zostaną zebrane w module zarządzania aktualizacjami. a) Możliwość sprawdzenia które punkty końcowe posiadają zainstalowane lub niezainstalowane aktualizacje. b) Przesyłanie informacji zwrotnych w przypadku niepowodzenia instalacji łatki c) Danie użytkownikowi możliwości szybkiej instalacji brakujących łatek na urządzeniu d) Użytkownik powinien mieć możliwość dodania do czarnej listy jednej lub wielu łatek 4. Raportowanie brakujących łatek z perspektywy punktu końcowego (zainstalowane/ brakujące na każdym punkcie końcowym) 5. Okresowe wysyłanie powiadomień jeśli punkty końcowe nie posiadają zainstalowanych łatek. 6. Zapewnienie możliwości buforowania, w ten sposób łatki będą pobierane z Internetu tylko przez niektóre przypisane punkty końcowe. 7. Możliwość wyświetlenia pozostałego czasu do automatycznego ponownego uruchomienia w powiadomieniu zarządzania poprawkami. 8. Funkcja wykrywania i informowania o każdej nowej zainstalowanej aplikacji na punkcie końcowym i dostępnych dla niej aktualizacji. 9. Możliwość automatycznego usuwania aktualizacji które nie mają już zastosowania	

	Nazwa elementu, parametru lub cechy	Wartość/występowanie
	ponieważ punkt końcowy nie istnieje lub aplikacja została usunięta. 10. Możliwość usunięcia z listy łatek które nie są już dostępne chociaż są obecne na niektórych punktach końcowych.	
Funkcjonalność ochrony urządzeń z systemem Android	1. silnik antywirusowy automatycznie skanuje każdą aplikację po jej zainstalowaniu i natychmiast informuje, czy stanowi ona jakiekolwiek zagrożenie 2. posiada wbudowany system antyphishingowy 3. możliwość zdalnej lokalizacji, blokady i wyczyszczenia danych w przypadku utraty lub kradzieży urządzenia 4. możliwość wysłania wiadomości do urządzenia 5. Wykrywanie anomalii w zainstalowanych aplikacjach 6. Ochrona całego ruchu internetowego, danych bankowych, haseł i pobieranych plików poprzez prywatną sieć VPN 7. możliwości blokowania aplikacji za pomocą kodu PIN w niezaufanych sieciach 8. Możliwość zarządzania urządzeniami za pomocą konsoli	
Usługa przeprowadzenia audytu cyberbezpieczeństwa	1. Weryfikacja poprawności instalatorów, jeśli instalator nie jest skonfigurowany poprawnie to audytor utworzy nowy pakiet 2. Sprawdzenie poprawności działania wymaganych zapytaniem funkcjonalności. Jeśli występują nieprawidłowości to audytor musi pokazać, jak wykonać zadanie rekonfiguracji w sposób zdalny tak, aby wszystkie dostępne funkcjonalności zostały zainstalowane 3. Sprawdzenie poprawności konfiguracji funkcjonalności EDR wraz ze wskazaniem, na co warto zwrócić uwagę w przypadku wystąpienia incydentu 4. Weryfikacja poprawności konfiguracji polityk bezpieczeństwa wraz ze wskazaniem ustawień, które serwis sugerowałby, aby zostały skonfigurowane inaczej wraz z uzasadnieniem zmiany.	

	Nazwa elementu, parametru lub cechy	Wartość/występowanie
	5. Konfiguracja poprawności wykonywania raportów i powiadomień dla administratorów 6. Jednorazowa analiza ryzyk	
Szkolenie dla administratora lokalnego systemu antywirusowego	1. kurs certyfikowany, uzyskany certyfikat musi być imienny 2. Tworzenie pakietów instalacyjnych i ich wdrożenie ręczne oraz zdalne na systemach Windows 3. Tworzenie paczek .msi 4. Konfiguracja szablonów polityk bezpieczeństwa wraz z omówieniem występujących opcji, zwróceniem uwagi na najważniejsze ustawienia pod kątem stacji roboczych i serwerów 5. Obsługa systemu EDR 6. Obsługa funkcjonalności piaskownicy 7. Wyjaśnienie działania funkcjonalności zarządzania ryzykiem 8. Konfiguracja powiadomień i raportów 9. Rozwiązywanie podstawowych problemów przy administracji	
Wynik w teście AV TEST oprogramowania antywirusowego	Test z lutego 2024 r. https://www.av-test.org/en/antivirus/business-windows-client/windows-10/february-2024/	Co najmniej 17,5 punkta
Inne	Pomoc techniczna, interfejs oraz dokumentacja dostarczona i świadczona w języku polskim.	