Żagań, dnia 16.05.2022 r.

WIO.271.2.2022

ZAPROSZENIE DO ZŁOŻENIA OFERTY
w postępowaniu o zamówienie publiczne o wartości szacunkowej poniżej 130 000 zł

Burmistrz Miasta Żagań
Plac Słowiański 17
68-100 Żagań
tel. (068) 477-10-40
fax. (068) 477-10-17
przetargi.wio@um.zagan.pl

zaprasza do składania ofert na wykonanie zamówienia publicznego pod nazwą:
„Dostawa oprogramowania antywirusowego umożliwiającego szyfrowanie dysków"

Zgodnie z art. 2 ust. 1 pkt. 1 Ustawy z dnia 11.09.2019 r. Prawo Zamówień Publicznych (t.j. Dz.U. z 2021 poz. 1129 ze zm.) do przedmiotowego postępowania nie stosuje się ustawy Prawo zamówień publicznych.

I. Określenie przedmiotu zamówienia publicznego:

Przedmiotem zamówienia jest zakup 120 licencji Oprogramowania antywirusowego umożliwiającego szyfrowanie dysków na okres 36 miesięcy, przy spełnieniu wszystkich poniższych wymagań:

- **Konsola zdalnej administracji**

1. Typy konsoli administracyjnej: Konsola Cloud – serwer administracyjny po stronie producenta lub Konsola On-premise – lokalny serwer administracyjny.
2. Centralna instalacja i zarządzanie programami służącymi do ochrony stacji roboczych i serwerów plikowych Windows.
3. Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware'ową, oraz zaporą osobistą (tworzenie reguł obowiązujących dla wszystkich stacji) zainstalowanymi na stacjach roboczych w sieci korporacyjnej z jednego serwera zarządzającego.
4. Możliwość integracji Domeny Active Directory.
5. Możliwość uruchomienia zdalnego skanowania wybranych stacji roboczych.
6. Możliwość sprawdzenia z centralnej konsoli zarządzającej stanu ochrony stacji roboczej (aktualnych ustawień programu, wersji programu i bazy wirusów, wyników skanowania skanera na żądanie, Zainstalowanych modułów, ostatniej aktualizacji oraz przypisanej polityki).
7. Możliwość utworzenia konta użytkownika z rolą administrator firmy, administrator sieci, analityk bezpieczeństwa lub z ustawieniami niestandardowymi.
8. Możliwość sprawdzenia z centralnej konsoli zarządzającej podstawowych informacji dotyczących stacji roboczej: adresów IP, wersji systemu operacyjnego.
9. Możliwość centralnej aktualizacji stacji roboczych z serwera w sieci lokalnej lub Internet.

10. Możliwość wysłania linku instalacyjnego bezpośrednio z poziomu konsoli administracyjnej.
11. Możliwość zmiany konfiguracji na stacjach i serwerach z poziomu centralnej konsoli zarządzającej lub z poziomu punktu końcowego po włączeniu odpowiedniej opcji w politykach bezpieczeństwa.
12. Możliwość uruchomienia centralnej konsoli jedynie z poziomu przeglądarki internetowej.
13. Możliwość ręcznego (na żądanie) i automatycznego generowanie raportów (według ustalonego harmonogramu) i wyeksportowanie go do formatu: pdf i csv
14. Raport generowany według harmonogramu z możliwością automatycznego wysłania go do osób zdefiniowanych w tym raporcie również zbiorczo w formie archiwum zip.
15. Możliwość generowania raportu co godzinę.
16. Po instalacji oprogramowania antywirusowego nie jest wymagane ponowne uruchomienie komputera do prawidłowego działania programu.
17. Aktywacja modułu kontroli urządzeń nie wymaga restartu stacji docelowej.
18. Możliwość dodania etykiety do stacji roboczej.
19. Możliwość dezinstalacji oprogramowania antywirusowego innych firm w trakcie instalacji zdalnej.
20. Możliwość przechowywania kwarantanny maksymalnie 180 dni
21. Możliwość definiowania czy pliki z kwarantanny mają być przesyłane do producenta i co jaki czas ma się ta czynność odbywać.
22. Po aktualizacji sygnatur baz antywirusowych opcja automatycznego przeskanowania kwarantanny.
23. W całym okresie trwania subskrypcji użytkownik ma prawo do korzystania z bezpłatnej pomocy technicznej świadczonej za pośrednictwem telefonu i poczty elektronicznej.
24. Możliwość aktualizacji serwera administracyjnego bez potrzeby przeinstalowywania.
25. Możliwość przypisywania polityk automatycznie po zalogowaniu do systemu operacyjnego w zależności od tego jaki użytkownik domenowy się zalogował lub do jakiej grupy domenowej on należy.
26. Możliwość automatycznego przypisywania polityk na podstawie reguły lokalizacji, możliwość określenia lokalizacji na podstawie
    -Zakres adresów IP/IP
    -Adres bramy
    -Adres serwera WINS
    -Adres serwera DNS
    -Połączenie DHCP sufiksów DNS
    -Punkt końcowy może rozwiązać hosta
    -Typ sieci
    -Nazwa hosta
27. Uwierzytelnienie dwuskładnikowe realizowane np. przez aplikację Google Authenticator
28. Możliwość integracji z innymi systemami poprzez API takich elementów bądź sekcji jak:
    a) Pakiety
    b) Sieć
    c) Kwarantanna
    d) Licencjonowanie
    e) Integracje
    f) Polityki
    g) Raporty

h) Konta

29. Możliwość utworzenia reguły która będzie usuwała punkty końcowe z konsoli zarządzającej jeżeli punkt końcowy nie połączył się z konsolą przez określoną liczbę dni. Funkcja ta pozwala również na określenie wzoru nazw maszyn które automatycznie będą usuwane oraz pozwala na określenie godziny kiedy te maszyny będą usuwane
30. Możliwość wyświetlania adresu MAC dołączonego do nazwy hosta.
31. Możliwość wyświetlenia czy punkt końcowy jest serwerem czy stacją roboczą.
32. Możliwość wyświetlenia informacji czy zainstalowany na punkcie końcowym system operacyjny to Windows, Linux, MacOS
33. Możliwość wyświetlenia wersji systemu operacyjnego zainstalowanego na punkcie końcowym.
34. Możliwość filtrowania punktów końcowych, które były online w ciągu ostatnich 24 godzin, 7 lub 30 dni.
35. Menu tworzenia paczek instalacyjnych musi określać czy dany moduł jest dostępny dla stacji roboczych Windows, Serwerów Windows, Linux, MacOS

- **Ochrona antywirusowa i antyspyware**

1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
2. Pomoc techniczna, interfejs oraz dokumentacja dostarczona i świadczona w języku polskim.
3. Wykrywanie zagrożeń i analiza procesów technikami heurystycznymi.
4. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
5. Wbudowana technologia do ochrony przed rootkitami.
6. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
7. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie".
8. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
9. Możliwość skanowania dysków sieciowych i dysków przenośnych.
10. Skanowanie plików spakowanych i skompresowanych.
11. 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
12. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express.
13. Skanowanie i oczyszczanie poczty przychodzącej POP3 "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
14. Automatyczna integracja skanera POP3 z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.

15. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.
16. Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. Dodatkowo zdefiniowane są grupy stron przez producenta.
17. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
18. Możliwość definiowania czy pliki z kwarantanny mają być przesyłane do producenta i co jaki czas ma się ta czynność odbywać.
19. Program powinien umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS.
20. Program powinien skanować ruch HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.
21. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program powinien pytać o hasło.
22. Po kliknięciu prawym klawiszem myszy na ikonie programu i wybraniu opcji : „O programie" możliwość wyświetlenia danych do pomocy technicznej jak: adres strony pomocy, adres e-mail do administratora ochrony, numer telefonu do administratora ochrony.
23. W GUI programu na punkcie końcowym możliwość wyświetlenia aktualnej wersji produktu i aktualnej wersji silników.
24. W GUI programu możliwość wyświetlenia kiedy była przeprowadzana ostatnia aktualizacja z dokładnością co do dnia i sekundy jej uruchomienia.
25. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń.
26. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.
27. Praca programu musi być niezauważalna dla użytkownika.
28. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania bezpośrednio na stacji roboczej.
29. Stacje robocze mogą łączyć się do serwera administracyjnego za pośrednictwem sieci Internet.
30. Oprogramowanie klienckie posiada wbudowana funkcje do komunikacji z serwerem administracyjnym, ale nie dopuszcza się osobnego agenta instalowanego na stacji roboczej.
31. Możliwość odblokowania ustawień programu po wpisaniu hasła
32. Oprogramowanie posiada możliwość odblokowania ustawień lokalnych konfiguracji po doinstalowaniu odpowiedniego modułu.
33. Wbudowany moduł kontroli urządzeń (możliwość blokowania całkowitego dostępu do urządzeń, podłączenia tylko do odczytu i w zależności do jakiego interfejsu w komputerze zostanie podłączone urządzenie)
34. Możliwość dodania zaufanych urządzeń bezpośrednio z konsoli administracyjnej, na podstawie wykrytych urządzeń lub wpisanych ręcznie ID urządzenia lub ID produktu.
35. Funkcja Ochrony danych umożliwia blokowanie wysyłanych przez http lub smtp jak: (adresy e-mail, Piny, Konta bankowe, hasła itp.
36. Funkcja Ochrony danych konfigurowana zdalnie przez administratora.
37. Jedna wersja instalacyjna na stacje robocze i serwery plików Windows.
38. Wbudowana zapora osobista, umożliwiająca tworzenie reguł na podstawie aplikacji oraz

ruchu sieciowego.

39. Wbudowany IDS
40. Możliwość zainstalowania silnika pełnego lub lekkiego ze sprawdzaniem reputacji plików w chmurze.
41. Możliwość tworzenia list sieci zaufanych.
42. Możliwość dezaktywacji funkcji zapory sieciowej.
43. Możliwość ustawienie skanowania z niskim priorytetem zmniejszając obciążenie systemu w trakcie wykonywania tego procesu.
44. Dodatkowa funkcja ochrony przeciwko znanym zagrożeniom typu ransomware
45. Mechanizm który wspiera powrót do ostatnich działających wersji produktu oraz sygnatur w przypadku wdrożenia wadliwej aktualizacji
46. Użytkownik na punkcie końcowym ma możliwość opóźnienia restartu potrzebnego do zakończenia jednego lub wielu zadań(konfigurowalne w politykach bezpieczeństwa)
47. Automatyczne zezwolenie na dostęp dla użytkowników Active Directory z grupy security groups
48. Wymuszenie połączenia szyfrowanego dla punktów końcowych Windows oraz Linux do serwera zarządzającego.
49. Wbudowana ochrona przed exploitami wyposażona w minimum 15 różnych technik wykrycia exploitów z możliwością włączenia lub wyłączenia każdej z nich oraz dająca możliwość dodania własnych procesów. Funkcja umożliwia również:
    a) Możliwość wymuszenia funkcji DEP systemu Windows
    b) Możliwość wymuszenia relokacji modułów (ASLR)
50. Ochrona przed atakami sieciowymi – Mechanizm obronny przed atakującymi próbującymi uzyskać dostęp do systemu poprzez wykorzystanie luk w sieci. Funkcja ta musi obejmować ochroną przed technikami takimi jak:
    -Wczesny dostęp
    -Dostęp do poświadczeń
    -Wykrycie
    -Crimeware
51. Pełne Szyfrowanie dysków
52. Możliwość wygenerowania i pobrania logów ze stacji roboczej z poziomu konsoli zarządzającej.
53. Ochrona przed ransomware - 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.

- **Pełne szyfrowanie dysków**

1. Szyfrowanie dysków korzysta z natywnej funkcji Bitlocker na systemach Windows.
2. Szyfrowanie dysków korzysta z natywnej funkcji FileVault na systemach Mac Os.
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. Administrator ma możliwość ustawienia czy system szyfrujący ma pytać o hasło w momencie uruchomienia systemu operacyjnego, jeśli aktywny jest moduł TPM.
11. Możliwość automatycznego zaimportowania klucza odzyskiwania do konsoli zdalnej administracji po instalacji oprogramowania, jeżeli maszyna została zaszyfrowana ręcznie przed zainstalowaniem oprogramowania.
12. Możliwość dodania wyjątków od szyfrowania dla dysków innych niż systemowe.

III. Sposób przygotowania oferty:

1. Wykonawca składa tylko jedną ofertę, na załączonym formularzu oferty określonym w załączniku nr 1 do niniejszego zaproszenia.
2. Wraz z ofertą Wykonawca składa oświadczenia i wymagane dokumenty.
3. Oferta musi być sporządzona w języku polskim.
4. Oferta musi być podpisana przez Wykonawcę lub upełnomocnionego przedstawiciela Wykonawcy.
5. Wykonawca ponosi wszelkie koszty związane z przygotowaniem i złożeniem oferty. Zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu.
6. Cenę oferty należy obliczyć uwzględniając wszelkie koszty niezbędne do wykonania zamówienia.

IV. Miejsce i termin składania ofert:

1. Ofertę wraz z załącznikami należy złożyć w Urzędzie Miasta Żagań, Plac Słowiański 17, Punkt Informacji pok. nr 4, 68-100 Żagań do dnia **19.05.2022 r.** do godziny **10:00,** z dopiskiem: „Oferta na dostawę oprogramowania antywirusowego umożliwiającego szyfrowanie dysków - nie otwierać przed 19.05.2022 r. przed godziną 10:00". Koperta powinna zawierać również nazwę Wykonawcy i jego adres.
2. W przypadku przesłania oferty pocztą lub przesyłką kurierską decydująca jest data wpływu do siedziby Urzędu Miasta w Żaganiu a nie data jej wysłania przesyłką pocztową czy kurierską.
3. Dopuszcza się złożenie oferty drogą elektroniczną na adres email: przetargi.wio@um.zagan.pl z tematem „Oferta na dostawę oprogramowania antywirusowego umożliwiającego szyfrowanie dysków" i treścią zawierającą tekst „Oferta na dostawę oprogramowania antywirusowego umożliwiającego szyfrowanie dysków - nie otwierać załączników przed 19.05.2022 r. przed godziną 10:00" oraz nazwę Wykonawcy i jego adres. W tym przypadku oferta wraz z załącznikami powinna być podpisana kwalifikowanym podpisem elektronicznym.
4. Wykonawca może przed upływem terminu do składania ofert, zmienić lub wycofać ofertę.
5. Oferty niekompletne podlegają uzupełnieniu, w terminie określonym przez Zamawiającego.

VI. Kryteria oceny ofert i ich znaczenie:

1. Zamawiający wybiera ofertę najkorzystniejszą, na podstawie ceny brutto - 100%.
2. Oferty oceniane będą punktowo. Najwyższą ilość punktów, tj. 100 pkt. otrzyma cena brutto najniższa wśród złożonych ofert. Pozostałe ceny będą punktowane proporcjonalnie do oferty z najniższą ceną, według następującego wzoru:

   P = Cn/Co x 100

   gdzie:

   P - punktacja dla danej oferty

   Cn - najniższa cena brutto wśród złożonych ofert nie podlegających wykluczeniu

   Co - cena oferty poddawanej punktacji
3. Cenę oferty należy obliczyć uwzględniając wszelkie koszty niezbędne do wykonania zamówienia.
4. Podana w ofercie cena jednostkowa ma charakter ryczałtowy i nie podlega zmianie w trakcie realizacji zamówienia.
5. W toku badania i oceny ofert Zamawiający może żądać od Wykonawców wyjaśnień dotyczących treści złożonych ofert.
6. W przypadku złożenia ofert o takiej samej cenie, Zamawiający negocjuje ceny z każdym Wykonawcom odrębnie.
7. Zamawiający udziela zamówienia Wykonawcy, który złożył uzyskał największą liczbę punktów (tj. złożył ofertę z najniższą ceną brutto).

VII. Postanowienia końcowe:

1. Istotne elementy, które zostaną zawarte w umowie z Wykonawcą zawarte są we wzorze umowy stanowiącym załącznik nr 2 do Zaproszenia do składania ofert.
2. Zamawiający zastrzega sobie możliwość unieważnienia przedmiotowego zamówienia bez podania przyczyny.
3. Klauzula informacyjna z art. 13 RODO znajduje się w załączniku nr 3 do Zaproszenia.

BURMISTRZ
Andrzej Katarzyniec