Szczegółowy opis przedmiotu zamówienia

I. Przedmiot zamówienia

1. Przedmiotem zamówienia jest świadczenie na rzecz Zamawiającego usługi ochrony antywirusowej stacji roboczych przed szkodliwym oprogramowaniem.

1.1. Usługa ochrony antywirusowej powinna być realizowana za pomocą systemu informatycznego który winien składać się z:

a) Konsoli – serwera lub serwerów zainstalowanych w zasobach Zamawiającego wraz z oprogramowaniem służącym do obsługi systemu oraz zarządzania nim przez administratorów.

b) Oprogramowania na stacjach roboczych – oprogramowanie działające na komputerze klienckim i świadczące usługi ochrony antywirusowej oraz komunikujące się z Konsolą.

c) Elementów pośredniczących – proxy, relay; jeśli System wymaga ich do komunikacji. Zamawiający dopuszcza rozwiązanie chmurowe elementów pośredniczących pod warunkiem pisemnego poświadczenia przez producenta rozwiązania, że zasoby te znajdują się na terenie Unii Europejskiej.

d) Niezbędnych licencji i subskrypcji.

II. Realizacja przedmiotu zamówienia

1. W ramach realizacji przedmiotu zamówienia Wykonawca:

1.1. Przeprowadzi analizę przedwdrożeniową uwzględniającą:

a) Architekturę rozwiązania i mechanizmy komunikacji Konsoli z serwerami pośredniczącymi i stacjami roboczymi.

b) Istniejącą strukturę stacji roboczych objętych wdrożeniem.

c) Scenariusze tworzenia i odzyskiwania kopii zapasowych.

d) Ustalenie adresacji sieciowej wszystkich komponentów i zasady konfiguracji firewalli Zamawiającego.

e) Przygotowanie do akceptacji przez Zamawiającego harmonogramu obejmującego Konsolę Systemu, instalację oprogramowania na stacjach roboczych w liczbie 1000 sztuk oraz wykonanie testów odbiorowych. Zamawiający wskaże do 10 lokalizacji, w których zostanie przeprowadzona instalacja oprogramowania na stacjach roboczych. Harmonogram musi uwzględniać lokalizacje, terminy oraz liczbę stacji roboczych podlegających wdrożeniu.

f) Przedłożona dokumentacja przedwdrożeniowa musi uzyskać akceptację Zamawiającego.

1.2. Udostępni oprogramowanie Centralnej Konsoli (Konsoli) i skonfiguruje je w infrastrukturze zamawiającego.

1.3. Skonfiguruje i uruchomi komponenty niezbędne dla zapewnienia ochrony antywirusowej na 1000 stacji roboczych wskazanych przez Zamawiającego oraz skomunikuje je z Konsolą (pozostałe stacje robocze Zamawiający skonfiguruje samodzielnie).

1.4. Będzie aktywował subskrypcje ochrony antywirusowej zgodnie z harmonogramem aktywacji subskrypcji i zapewniał ciągłość działania ochrony antywirusowej

2. Sumaryczna liczba stacji objętych ochroną wyniesie 9000 sztuk.

Niezbędne zasoby i instruktaże

III. Zasoby Zamawiającego

Na potrzeby realizacji zamówienia Zamawiający dedykuje zasoby do osadzenia Konsoli wraz z niezbędnymi elementami:

- dwa procesory Intel Xeon E5-2680 v3;
- 256GB RAM;
- dwa dyski twarde 300GB skonfigurowane w RAID1;
- karta Fibre Channel HP QMH2672 16Gb;
- karta sieciowa HP FlexFabric 10Gb 2-port 536FLB Adapter;
- przestrzeń dyskową z macierzy dyskowej HP 3PAR StoreServ 7400 zaprezentowaną czterema ścieżkami za pośrednictwem interfejsu Fibre Channel;
- system operacyjny bazujący na posiadanej przez Zamawiającego licencji Microsoft Windows 2012 R2 Data Center;
- system operacyjny Linux w dowolnej dystrybucji wspieranej przez Vmware;
- dostęp do Konsoli Systemu poprzez VPN dla osób wskazanych i upoważnionych przez Wykonawcę;

Zamawiający używa systemów archiwizacji danych Avamar i DataDomain.

IV. Licencje

Wykonawca zagwarantuje:

1. Wszystkie licencje niezbędne do poprawnego funkcjonowania Konsoli Systemu, potwierdzone dokumentem licencyjnym wystawionym przez producenta Systemu uprawniającym Zamawiającego do korzystania z Systemu.
2. Subskrypcje na stacje robocze, potwierdzone dokumentem licencyjnym wystawionym przez producenta Systemu oraz statusem licencji z Konsoli systemu.
3. Dopuszcza się nieograniczone licencjonowanie wieczyste/perpetual/enterprise.
4. W ramach systemu pracować będzie do 200 administratorów.

V. Instruktaże

1. Zamawiający wymaga przeprowadzenia instruktaży dla następujących grup użytkowników:
   1.1. Głównych Administratorów systemu – (w liczbie do 12 osób).
   1.2. Administratorów w jednostkach organizacyjnych.
2. Dla Administratorów w jednostkach organizacyjnych: podstawowy instruktaż stanowiskowy obejmujący przygotowanie dedykowanej paczki instalacyjnej oprogramowania na stację końcową, instalację/deinstalację oprogramowania, analizę potencjalnych błędów (debugging), obsługę centralnej Konsoli systemu w zakresie przyłączania zainstalowanego oprogramowania do odpowiedniej jednostki organizacyjnej, zdalnego dostępu, rekonfiguracji stacji końcowej.
3. Wykonawca zapewni instruktaż w formie elearningowej i po zakończeniu wdrożenia udostępni raport z instruktażu zawierający co najmniej:
   - ilość osób które przystąpiły do instruktażu,
   - ilość osób które ukończyły instruktaż.

   3.2. Całość instruktaży i przygotowane przez Wykonawcę materiały muszą być w języku polskim.
4. Dla Głównych Administratorów systemu: zaawansowany instruktaż stanowiskowy, przeprowadzony w siedzibie Zamawiającego lub w lokalizacji zapewnionej przez Wykonawcę, obejmujący instruktaż podstawowy wyszczególniony w poprzednim punkcie oraz instruktaż z zakresu niezbędnych funkcjonalności zapewniających sprawne zarządzanie środowiskiem skonfigurowanym do obsługi wielu jednostek Gminy Lublin, nadawania/odbierania uprawnień, tworzenia polityk, raportów, procedur bezpieczeństwa i zasad bezpiecznej eksploatacji, sposobów analizy logów, debugowania systemu.

   4.1. Instruktaż będzie przeprowadzony w trzech grupach po cztery osoby w niepokrywających się terminach.

4.2. Instruktaż dla Głównych Administratorów systemu wykonany będzie przez certyfikowanego trenera zakończony wydaniem certyfikatu producenta. Zamawiający nie dopuszcza instruktażu online. Wykonawca ponosi koszty organizacji instruktażu

VI. Testy odbiorowe

1. Wykonawca wykona testy Systemu obejmujące co najmniej:
   - **1.1.** Centralną Konsolę systemu.
   - **1.2.** Poprawność działania oprogramowania na Stacjach roboczych.
   - **1.3.** Przeprowadzenie testów penetracyjnych typu whitebox, obejmujących co najmniej skanowanie portów, badanie podatności systemu operacyjnego oraz aplikacji na znane luki w bezpieczeństwie, weryfikację poprawności działania firewalla, ocenę poprawności reakcji systemu zabezpieczeń na wykonywane ataki DDOS.
   - **1.4.** przeprowadzenie backupu i odtwarzania Konsoli systemu,
   - **1.5.** gromadzenia i odczytywania logów systemu za pomocą oprogramowania Zamawiającego (Splunk).
2. Testy kończą się pełnym raportem z przeprowadzonych czynności.
   - **2.1.** Opracowanie dokumentacji powykonawczej w języku polskim obejmującej co najmniej:
     - **a)** architekturę systemu wraz z opisem,
     - **b)** opis komponentów Systemu,
     - **c)** zasady bezpieczeństwa komunikacji, w szczególności bezpieczną komunikację stacji roboczych i serwerów poprzez wyłącznie szyfrowane połączenia i uwierzytelnienia poprzez architekturę certyfikatów SSL,
     - **d)** dokumentację dla Administratorów Systemu i Użytkowników,
     - **e)** wyniki testów,
     - **f)** raporty z wdrożenia zawierające raporty z przeprowadzonych instruktaży

Opis właściwości systemu informatycznego

VII. Właściwości systemu informatycznego

1. System musi zapewniać poufność, a wymiana danych z oprogramowaniem musi odbywać się w kanale szyfrowanym (SSL).
2. System musi zapewniać komunikację pomiędzy Konsolą a Stacjami Roboczymi również poprzez połączenia NAT, bez potrzeby korzystania z technologii VPN.
3. Dystrybucja oprogramowania musi być realizowana każdą z poniższych metod:
   - **3.1.** poprzez instalację oprogramowania z poziomu Konsoli programu w przypadku integracji systemu z usługą Active Directory;
   - **3.2.** poprzez instalację oprogramowania za pomocą reguł GPO; Zamawiający preferuje pakiet msi generowany wprost z Konsoli;
   - **3.3.** poprzez wysłanie linku do pobrania oprogramowania dedykowanego dla danej grupy stacji roboczych;
   - **3.4.** za pomocą dedykowanej paczki instalacyjnej dla co najmniej jednostki organizacyjnej Gminy reprezentowanej w drzewie architektury.

VIII. Właściwości Konsoli

1. Architektura Konsoli musi być jednoinstancyjna, tzn. zapewniać dostęp do wszystkich zarządzanych przez system stacji roboczych w ramach pojedynczej, zintegrowanej Konsoli administratorskiej (bez wymuszonego podziału na funkcjonalnie podobne podsystemy celem obsługi wszystkich objętych licencjonowaniem stacji roboczych).
2. Zamawiający dopuszcza możliwości korzystania z komercyjnego silnika bazy danych w przypadku, gdy jego instancja będzie dedykowana tylko na potrzeby wdrożenia, bez ponoszenia dodatkowych kosztów przez Zamawiającego. Zapewnienie właściwych licencji bazo-

danowych jest w takim przypadku obowiązkiem Wykonawcy.

3. Interfejs Konsoli musi być w całości dostępny z poziomu przeglądarki internetowej (Internet Explorer w wersji 11 lub nowszej, Mozilla 60 lub nowszej, Chrome 70 lub nowszej, Edge w wersji 40 lub nowszej) bez potrzeby instalacji dedykowanego klienta. Dostęp do Konsoli nie może wymagać korzystania z wtyczek w technologii Flash lub Java. Rekomenduje się wykorzystanie otwartej technologii HTML5.
4. Interfejs Konsoli musi być co najmniej w języku polskim lub angielskim.
5. Obsługa Konsoli musi umożliwiać zmianę kontrastu wyświetlanego obrazu oraz wielkość stosowanych czcionek ekranowych, co najmniej poprzez zmianę ustawień przeglądarki internetowej.
6. Konsola musi eksportować swoje logi w standardzie syslog. Zamawiający preferuje wykorzystanie modułu komunikacji z systemem Splunk.
7. Konsola musi zapewniać równoczesny, nieograniczony dostęp do Konsoli dla co najmniej 100 administratorów.
8. Konsola musi rozpoznawać stacje robocze z systemem Microsoft Windows w ramach Active Directory oraz Grup roboczych będących w posiadaniu Zamawiającego, w tym środowiska wielodomenowego.
9. Konsola musi zapewniać drzewiastą i hierarchiczną architekturę dla jednostek, administratorów i stacji roboczych.
10. Konsola musi zapewniać delegację uprawnień do określonych grup zasobów na podstawie uprzednio zdefiniowanych reguł. Wśród dostępnych reguł i uprawnień muszą znajdować się co najmniej:
    - **10.1.** tworzenie użytkowników Konsoli,
    - **10.2.** usuwanie użytkowników Konsoli,
    - **10.3.** edycja użytkowników Konsoli,
    - **10.4.** nadawanie dostępu do gałęzi drzewa architektury dla użytkowników Konsoli
    - **10.5.** odbieranie dostępu do gałęzi drzewa architektury dla użytkowników Konsoli
    - **10.6.** zarządzanie użytkownikami, ich uprawnieniami i przypisywanie im ról (w tym poziomów uprawnień dla administratorów), a także zarządzanie rolami musi odbywać się poprzez interfejs Konsoli, przypisywanie uprawnień może odbywać się na podstawie przynależności użytkownika do odpowiedniej grupy w Active Directory.
    - **10.7.** tworzenie ról użytkowników,
    - **10.8.** usuwanie ról użytkowników,
    - **10.9.** modyfikowanie ról użytkowników,
    - **10.10.** dodawanie stacji roboczych,
    - **10.11.** usuwanie stacji roboczych,
    - **10.12.** definiowanie zadań,
    - **10.13.** uruchamianie zadań,
    - **10.14.** tworzenie i edycja polityk.
11. Konsola musi zapewniać uwierzytelnianie Administratorów na podstawie członkostwa do wcześniej zdefiniowanej Grupy Zabezpieczeń (Security Group) w Active Directory.
12. Konsola musi umożliwiać tworzenie raportów (zdefiniowanych przez Producenta oprogramowania oraz niestandardowych) na podstawie wbudowanych kryteriów, w tym na podstawie podziału na jednostki.
13. Konsola musi mieć możliwość włączenia opcji testowania i zatwierdzania aktualizacji na wybranej grupie urządzeń przed instalacją poprawek w środowisku produkcyjnym.
14. Administrator Konsoli musi mieć możliwość pobrania dedykowanej paczki instalacyjnej z poziomu Konsoli.
15. Konsola musi mieć możliwość włączenia opcji uwierzytelniania dwuskładnikowego. Zamawiający preferuje otwarte standardy (zgodność z Google Authenticator). Jeśli wymagane

jest dodatkowe oprogramowanie Wykonawca dostarczy licencje na potrzebne oprogramowanie.

16. Konsola musi umożliwiać zarządzanie i rozliczanie licencji oprogramowania.
17. Konsola musi umożliwiać zdalne wykrywanie zainfekowanego oprogramowania i uruchamiać zdefiniowane działania naprawcze.
18. Konsola musi zapewniać poprawną obsługę oprogramowania w przypadku, gdy nazwy stacji roboczych i ich adresacja w różnych sieciach powtarzają się.
19. Konsola musi posiadać wbudowane narzędzia systemowe umożliwiające wymuszenie zdalnej aktualizacji wskazanych stacji roboczych oraz zarządzanie harmonogramami skanowania.
20. Konsola musi umożliwiać wykonywanie zadań w określonym przedziale czasowym oraz wysyłać powiadomienia e-mail o zmianach, które wystąpiły w systemie.
21. Konsola musi umożliwiać tworzenie harmonogramów dla raportów i przesyłanie ich w formie pliku XLSX lub CSV lub ODS na wskazany adres mailowy oraz udostępniać możliwość zapisania raportu lokalnie.
22. Konsola musi zapewniać na tworzenie dedykowanej paczki instalacyjnej, po zainstalowaniu której umożliwi jednoznaczną identyfikację stacji roboczej w drzewie architektury.

IX. Właściwości oprogramowania stacji roboczych

1. Interfejs oprogramowania musi być dostępny w języku polskim
2. Oprogramowanie na stacjach roboczych musi działać nawet w przypadku utraty łączności z Konsolą systemu.
3. Stacje robocze muszą samodzielnie aktualizować sygnatury antywirusowe w przypadku utraty komunikacji z Konsolą systemu.
4. Oprogramowanie stacji roboczych musi obsługiwać systemy operacyjne będące w posiadaniu Zamawiającego lub użytkowane przez jednostki Gminy Lublin w wersjach:
   4.1. Microsoft Windows XP, Vista, 7, 8, 10;
   4.2. Linux CentOS 7.x, Debian 8.x, Ubuntu 14.x, RHEL 7.x;
   4.3. MacOS 10.7.5;
   4.4. i nowszych.
5. W przypadku systemów Windows XP, Vista oraz MacOS w wersji niższej niż 10.11 Zamawiający dopuszcza ostatnią stabilną wersję oprogramowania zgodną z wymienionymi systemami operacyjnymi, Wykonawca musi zapewnić aktualizacje sygnatur dla tych wersji oprogramowania.
6. Oprogramowanie stacji roboczych musi mieć możliwość blokowania uruchamiania plików wykonywalnych EXE poprzez reguły oparte na co najmniej na ścieżce dostępu do aplikacji lub wartości hash pliku.
7. Oprogramowanie stacji roboczych musi zapewniać automatyczne skanowanie pod kątem zagrożeń i ewentualne blokowanie urządzeń i nośników wymiennych (karty pamięci, USB, eSATA) w przypadku wykrycia zagrożenia.
8. Oprogramowanie stacji roboczych musi zapewniać automatyczną deinstalację innego oprogramowania antywirusowego podczas instalacji.
9. Oprogramowanie stacji roboczych musi mieć wbudowane narzędzie informujące o brakujących aktualizacjach systemowych.
10. Oprogramowanie stacji roboczych musi gwarantować minimalne wyniki testów oferowanego oprogramowania potwierdzone przez jeden z niezależnych ośrodków (https://www.av-test.org/ https://www.av-comparatives.org/) dla sektora Enterprise w kategorii ochrony dla komputerów stacjonarnych z systemem Windows na poziomie:
    10.1. oceny 6 w kategorii Protection w aktualnym teście https://www.av-test.org/en/antivirus/business-windows-client/ ,
    10.2. oceny 98,5% w kategorii Protection Rate w aktualnym teście https://www.av-compa-

ratives.org/enterprise/latest-tests/ ,

10.3. testy muszą być opublikowane nie wcześniej niż rok przed dniem realizacji zamówienia.

ZASTĘPCA DYREKTORA
Wydziału Informatyki i Telekomunikacji
Jarosław Buczek