Opis przedmiotu zamówienia

Zakup sprzętu komputerowego i oprogramowania w ramach grantu Cyfrowa Gmina

Część III Zakup licencji oprogramowania specjalistycznego – zarządzanie siecią i zasobami IT

W ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1. Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotycząca realizacji projektu grantowego „Cyfrowa Gmina" o numerze POPC.05.01.00-00-0001/21-00.

Minimalna funkcjonalność oprogramowania do monitoringu sieci komputerowej wraz z podłączonymi do niej zasobami sprzętowymi oraz oprogramowaniem zainstalowanym na serwerach oraz stacjach roboczych działających w obrębie sieci.

Oprogramowanie musi posiadać budowę modułową, składać się z serwera zarządzającego, zdalnych konsoli oraz Agentów. Komunikacja pomiędzy Serwerem a Agentami i Konsolami nawiązywana jest przy użyciu szyfrowanego protokołu TLS 1.2. Moduły umożliwiają kompleksowy monitoring sieci, monitoring sprzętu komputerowego na stanowiskach użytkowników pod kątem zmian sprzętowych i programowych oraz pomocy w formie interaktywnego połączenia sieciowego z obsługiwanym użytkownikiem.

Program musi wykorzystywać bazę danych opartą na silniku SQL (np.: PostgreSQL) dzięki czemu nie będzie objęty limitem ilości danych, baza danych jest rozwiązaniem darmowym niewymagającym dodatkowego licencjonowania.

Dane, które dotyczą działań pracownika na komputerze, a więc: historia aktywności, polityka korzystania z Internetu oraz aplikacji, dostęp do zewnętrznych nośników danych itp., muszą być odseparowane od danych stricte technicznych tj. informacji o stacji roboczej. Muszą być one również grupowane w osobnym, dedykowanym oknie. Pozwala to na, zgodne z RODO, usuwanie danych wybranego użytkownika bez konieczności usunięcia informacji o stacji roboczej. Dostęp do danych osobowych oraz danych z monitoringu, zgodnie z RODO, objęty jest kontrolą na poziomie wybranych Administratorów – w programie można nadawać kontom administracyjnym różne poziomy dostępu oraz uprawnień zarówno do funkcji Programu, grup urządzeń, jak i użytkowników.

Główny Administrator ma możliwość zarządzania uprawnieniami konfiguracyjnymi programu dla innych kont z rolą administracyjną np. może wyłączyć możliwość zdalnej deinstalacji Agenta.

Funkcje podstawowe obsługujące infrastrukturę sieciową i jej zasoby.

Monitorowanie infrastruktury musi obejmować serwery windows, linux, routery, przełączniki, urządzenia voip i firewalle w zakresie:

- wykrywania urządzeń w sieci poprzez skanowanie ping (oraz arp-ping),
- wizualizacji stanu urządzeń w postaci ikon urządzeń na graficznych mapach sieci,
- wizualizacji połączeń pomiędzy urządzeniami a przełącznikami i informacji, do którego portu przełącznika podłączone jest dane urządzenie,
- serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych serwisów. Program monitoruje czas ich odpowiedzi i procent utraconych pakietów,
- serwerów pocztowych:
  - program monitoruje zarówno serwis odbierający, jak i wysyłający pocztę,
  - program ma możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS i inne), w razie gdyby przestały one odpowiadać lub funkcjonowały wadliwie (np. gdy ważne parametry znajdą się poza zakresem),
  - program ma możliwość wykonywania operacji testowych,
  - program ma możliwość wysłania powiadomienia jeśli serwer pocztowy nie działa.
- monitorowania serwerów WWW i adresów URL,
- obsługi szyfrowania SSL/TLS w powiadomieniach e-mail,
- obsługi urządzeń SNMP wspierających SNMP v1/2/3 z szyfrowaniem oraz autoryzacją, (np. przełączniki, routery, drukarki sieciowe, urządzenia VoIP itp.) – monitorowanie wartości za pomocą nazw zmiennych oraz OID,
- obsługi komunikatów syslog i pułapek SNMP,
- monitoringu routerów i przełączników wg:
  - zmian stanu interfejsów sieciowych,
  - ruchu sieciowego,
  - podłączonych stacji roboczych – graficzna prezentacja panelu switcha,
  - ruchu generowanego przez podłączone do portów stacje robocze.
- serwisów Windows: monitor serwisów Windows alarmuje gdy serwis przestanie działać oraz pozwala na jego uruchomienie/zatrzymanie/zrestartowanie,
- wydajności systemów Windows:
  - obciążenie CPU,
  - pamięci,

◦ zajętość dysków,

◦ transfer sieciowy.

Program musi posiadać Inteligentne Mapy i Oddziały, które służą do lepszego zarządzania logiczną strukturą urządzeń w przedsiębiorstwie (Oddziały) oraz tworzą dynamiczne mapy wg własnych filtrów (Mapy Inteligentne).

Funkcje przetwarzające informacje o sprzęcie i/oraz oprogramowaniu na nim zainstalowanym.

W ramach tej części funkcjonalności oprogramowanie musi:

• prezentować szczegóły dotyczące sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart itp.;

• obejmować m.in.: zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade;

• informować o zainstalowanych aplikacjach oraz aktualizacjach Windows co bezpośrednio umożliwia audytowanie i weryfikację użytkowania licencji w organizacji;

• zbierać informacje w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP itd.;

• posiadać możliwość wysyłania powiadomienia np. e-mailem w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera;

• umożliwiać odczytanie numeru seryjnego (klucze licencyjne);

• umożliwiać automatyczne zarządzanie instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych;

• umożliwić przegląd informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp.;

• umożliwić utworzenie listy plików użytkowników z określonym rozszerzeniem (np. filmy .AVI) znalezionych na stacjach roboczych oraz ich zdalne usuwanie;

• umożliwić wymianę plików do i ze stacją roboczą poprzez funkcję Menedżera plików - działania administratorów wykonywane w tej funkcji są logowane.

Oprogramowanie musi zapewnić gromadzenie danych o zasobach oraz umożliwiać prowadzenie bazy ewidencji majątku IT w zakresie sprzętu i programowania:

• przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji;

• tworzenia powiązań między zasobami a urządzeniami;

• tworzenia powiązań między zasobami a kontami użytkowników (zarówno lokalnymi, jak i zsynchronizowanymi z Active Directory), wskazywanie osób odpowiedzialnych;

• wskazania osób uprawnionych do użycia zasobów;

• definiowania własnych typów zasobów (elementów wyposażenia), ich atrybutów oraz wartości - dla danego urządzenia lub oprogramowania istnieje możliwość dodawania dodatkowych informacji, np. numer inwentarzowy, osoba odpowiedzialna, numer dokumentu zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu gwarancji, termin kolejnego przeglądu (można podać datę, po której administrator otrzyma powiadomienie e-mail o zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, lub własny komentarz;

• importu danych z zewnętrznego źródła (.CSV);

• przechowywania dowolnych dokumentów (np. pliki .DOCX, .XLSX, .PDF), np.: skan faktury zakupu, gwarancji, dowolnego dokumentu itp.;

• tworzenia powiązań między zasobami a dokumentami w relacji 1:N;

• oznaczania statusów zasobów, np. w użyciu, w naprawie, zutylizowany itp.;

• ewidencji czynności wykonywanych na zasobach, np.: aktualizacja, naprawa w serwisie, konserwacja itp. wraz z możliwością określenia kosztu oraz czasu przeznaczonego na wykonanie czynności;

• generowania zestawienia wszystkich zasobów, w tym urządzeń i zainstalowanego na nich oprogramowania;

• generowania protokołów przekazania zasobów wraz z konfigurowalną sekcją zawierającą dane i logo organizacji;

• archiwizacji i porównywania audytów zasobów;

• tworzenia kodów kreskowych dla zasobów;

• drukowania kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla zasobów, które posiadają numer inwentarzowy;

• inwentaryzacji zasobów posiadających kody kreskowe za pomocą aplikacji mobilnej na system Android;

• inwentaryzacji stacji roboczych niepodłączonych do sieci (bez instalacji Agenta poprzez manualne wykonanie skanów inwentaryzacji offline);

• definiowania alarmów z powiadomieniami e-mail dla dowolnych pól czasowych typu „data” z atrybutów zasobów lub licencji (np. „za 2 tygodnie wygaśnie licencja/gwarancja”).

<u>Inwentaryzacja oprogramowania musi zapewniać funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez:</u>

• skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie archiwów ZIP;

• informacje o aplikacjach używanych w organizacji;

• tworzenie własnych wzorców aplikacji;

• tworzenie dowolnych kategorii aplikacji, np. nowe, zabronione, projektowe itp.;

• informacje o komputerach, na których aplikacja została wykryta;

• zarządzanie posiadanymi licencjami;

• wskazywanie osób odpowiedzialnych za licencję;

• wskazanie użytkowników licencji;

• tworzenia powiązań między licencjami a dokumentami w relacji 1:N;

• rozbudowane zarządzanie licencjami poprzez: przypisywanie do użytkownika, przypisywanie do wielu komputerów tego samego użytkownika, przypisywanie wg numerów seryjnych, przypisywanie wg różnych wersji aplikacji na jednym urządzeniu;

• łatwy audyt legalności oprogramowania oraz powiadamianie tylko w razie przekroczenia liczby posiadanych licencji - w każdej chwili istnieje możliwość wykonania aktualnych raportów audytowych;

• zarządzanie posiadanymi licencjami: raport zgodności licencji;

• możliwość przypisania do programów numerów seryjnych, wartości itp.;

• okna audytowe musi posiadać możliwość filtrowania elementów per oddział.

Funkcje przetwarzające informacje o użytkownikach.

Oprogramowanie musi umożliwiać monitorowanie aktywności użytkowników pracujących na komputerach z systemem Windows poprzez monitorowanie:

• faktycznego czasu aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy);

• procesów (każdy proces ma całkowity czas działania oraz czas aktywności użytkownika) wraz informacją o uruchomieniu na podwyższonych uprawnieniach;

• rzeczywistego użytkowania programów (m.in. procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona) wraz z informacją, na którym komputerze wykonano daną aktywność;

• informacji o edytowanych przez użytkownika dokumentach;

• historii pracy (cykliczne zrzuty ekranowe);

• listy odwiedzanych stron WWW (liczba odwiedzin stron z nagłówkami, liczbą i czasem wizyt);

• transferu sieciowego użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika);

• wydruków m.in. informacje o dacie wydruku, informacje o wykorzystaniu drukarek, raporty dla każdego użytkownika (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument był drukowany), zestawienia pod względem stacji roboczej (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument drukowano z danej stacji roboczej), możliwość "grupowania" drukarek poprzez identyfikację drukarek. Program ma możliwość monitorowania kosztów wydruków;

• nagłówków przesyłanej poczty e-mail;

• blokowania stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla danej stacji roboczej z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających korzystania z danych domen oraz wybranych lub dowolnych sub-domen (np. *.domena.pl);

• blokowania ruchu na wskazanych portach TCP/IP;

• blokowania pobierania poprzez przeglądarki internetowe plików z określonym rozszerzeniem;

• wysyłania powiadomień gdy użytkownik: odwiedzi stronę z określonej grupy domeny; pobierze lub wyśle określoną ilość danych w ciągu dnia w sieci lokalnej lub Internet; wydrukuje określoną ilość stron w ciągu dnia,

• przygotowania zestawienia (metryki) ustawień monitorowania użytkownika w postaci raportu (który można dołączyć np. do akt pracownika);

• możliwość generowania raportów dla użytkowników Active Directory niezależnie od tego, na jakich komputerach pracowali w danym czasie;

• mechanizm blokowania uruchamiania aplikacji;

• program posiada Grupy użytkowników oraz Grupy Inteligentne, które służą do lepszego zarządzania użytkownikami, polityką monitorowania oraz blokowania aplikacji i stron internetowych.

Funkcje realizacji pomocy zdalnej.

W ramach kontroli stacji użytkownika musi być dostępny podgląd pulpitu użytkownika i możliwość przejęcia nad nim kontroli. Podczas dostępu zdalnego, zarówno użytkownik jak i administrator widzą ten sam ekran. Administrator w trakcie zdalnego dostępu ma możliwość zablokowania działania myszy oraz klawiatury dla użytkownika. W niniejszym module znajduje się baza zgłoszeń umożliwiająca użytkownikom zgłaszanie problemów technicznych, które z kolei są przetwarzane i przyporządkowywane

odpowiednim administratorom, otrzymującym automatycznie powiadomienie o przypisanym im problemie. Kolejną ważną funkcjonalnością musi być umożliwienie użytkownikom monitorowania procesu rozwiązywania zgłoszonych przez nich problemów i ich aktualnych statusów, jak również możliwość wymiany informacji z administratorem poprzez komentarze, które są wpisywane i widoczne dla obu stron. Moduł ten musi zawierć również komunikator (czat), który umożliwia przesyłanie wiadomości pomiędzy zalogowanymi użytkownikami i administratorami (wraz z wyszukiwarką wiadomości oraz automatycznym oczyszczaniem historii rozmów) oraz bazę wiedzy pomagającą użytkownikom samodzielnie rozwiązywać najprostsze, powtarzające się problemy.

Moduł pomocy zdalnej umożliwia również:

• pobieranie listy użytkowników z Active Directory,

• zarządzanie dostępem do czatu w 3 poziomach uprawnień: pełny dostęp, brak dostępu lub dostęp ograniczony wyłącznie do pomocy technicznej,

• tworzenie własnego drzewa kategorii zgłoszeń wraz z możliwością grupowania kategorii w folderach (do 4 poziomów kategorii),

• przypisywanie pracowników helpdesk do kategorii zgłoszeń,

• procesowanie zgłoszeń użytkowników z wiadomości e-mail,

• tworzenie formularzy z niestandardowymi polami opisowymi, dedykowanymi do wybranych kategorii zgłoszeń,

• wykonywanie operacji na wielu zgłoszeniach równocześnie,

• dołączanie załączników do zgłoszeń,

• zrzuty ekranowe (podgląd pulpitu),

• dystrybucję oprogramowania przez Agenty,

• dystrybucję oraz uruchamianie plików za pomocą Agentów (w tym plików MSI),

• zadania dystrybucji plików, jeśli komputer jest wyłączony w trakcie zlecania operacji następuje kolejkowanie zadania dystrybucji pliku,

• możliwość skonfigurowania automatyzacji procesowania zgłoszeń,

• planowanie nieobecności pracowników helpdesk,

• obsługę umów o gwarantowanym poziomie świadczenia usług (SLA),

• generowanie raportów obsługi helpdesk,

• zdalne wykonywanie poleceń poprzez Agenty (np. utworzenie / edycja konta lokalnego użytkownika systemu),

• zarządzania procesami systemu Windows (w zakresie: zakończ proces, zakończ drzewo procesu, uruchom nowy proces w sesji użytkownika wraz z parametrami),

• wymiany plików do i ze stacji roboczej poprzez funkcję Menedżera plików.

Funkcje ochrony danych.

Ochrona danych poprzez:

• blokowanie urządzeń i nośników danych per user, nie per host;

• możliwość autoryzacji nośników zewnętrznych - np. szyfrowanych pendrive, dysków itp..

• możliwość blokowania dostępu do napędów zewnętrznych;

• możliwość określania praw dostępu w zależności od typu urządzenia, np. CD, PENDRIVE;

• możliwość blokowania urządzeń i interfejsów fizycznych: USB, Gniazda kart pamięci, SATA, dyski przenośne, CD;

• możliwość blokowania interfejsów bezprzewodowych: WIFI, BT, IRDA;

• blokada dotyczy tylko urządzeń do przenoszenia danych - inne urządzenia peryferyjne mogą być podłączone;

• informowanie o podłączeniu/odłączeniu urządzenia przenośnego.

Zarządzanie prawami dostępu do urządzeń:

• definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików;

• autoryzowanie urządzeń firmowych (przykładowo szyfrowanych): pendrive'ów, dysków itp. - urządzenia prywatne są blokowane;

• całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników lub stacji roboczych;

• centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci lub wybranych stacji roboczych.

Audyt operacji na urządzeniach przenośnych:

• zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych.

• podłączenie/odłączenie urządzenia przenośnego.

Integracja z Active Directory - zarządzanie prawami dostępu przypisanymi do użytkowników oraz grup domenowych.

Zamawiający oczekuje, że po stronie Wykonawcy spoczywa obowiązek instalacji i konfiguracji proponowanego rozwiązania na infrastrukturze Zamawiającego. Wdrożenie zakończy się przeszkoleniem 2 lokalnych administratorów z konfiguracji i obsługi proponowanego rozwiązania.

W ramach oferty Wykonawca gwarantuje:

• wieczystą licencję na oprogramowanie;

• monitorowanie infrastruktury dla nielimitowanej liczby monitorowanych urządzeń;

• 12 miesięcy Umowy Serwisowej w ramach której Zamawiającemu przysługuje pomoc techniczna i prawo do bezpłatnych aktualizacji oprogramowania.

• Możliwość przedłużenia umowy serwisowej na kolejne 12 miesięcy w cenie 20% wartości licencji (przy zachowaniu ciągłości).

• Minimalna liczba zarządzanych stacji poprzez, które zbierane są informacje w ramach jednej licencji to 80 szt.

• Możliwość rozszerzenia funkcjonalności oraz zwiększenia liczby zarządzanych stacji w ramach jednej licencji w dowolnym czasie.

Na Wykonawcy spoczywa obowiązek udokumentowania nie gorszych parametrów zaproponowanego rozwiązania. Dokumentację należy przedłożyć razem z ofertą.