Fundusze Europejskie Polska Cyfrowa | Rzeczpospolita Polska | Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Projekt jest współfinansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego Unii Europejskiej w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 na podstawie Umowy o powierzenie grantu o numerze 3063/1/2021 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

Numer referencyjny postępowania:
TG.271.20.2022.RK

Załącznik nr 2.5 do SWZ

Opis przedmiotu zamówienia
Część nr 5 – Oprogramowanie do zarządzania

Oprogramowanie do zarządzania użytkownikami systemów informatycznych oraz infrastrukturą teleinformatyczną.

W ramach postępowania wymagane jest dostarczenie rozwiązania do zarządzania stacjami roboczymi, użytkownikami systemów informatycznych oraz infrastrukturą teleinformatyczną, z licencją wieczystą na co najmniej 30 użytkowników, z co najmniej 12 miesięczną aktualizacją i pomocą techniczną, spełniające wszystkie wymienione poniżej funkcje i mechanizmy:

— architektura systemu

- budowa modułowa, składającą się z serwera zarządzającego, zdalnych konsoli oraz agentów. Komunikacja pomiędzy serwerem a agentami i konsolami powinna być nawiązywana jest przy użyciu szyfrowanego protokołu co najmniej TLS 1.2. Moduły powinny umożliwiać 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 powinien wykorzystywać darmowy silnik bazy danych z kodem źródłowym dostępnym na licencji open-source, nieobjętym limitem ilości danych, baza danych powinna być 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., powinny być odseparowane od danych technicznych.
- dostęp do danych osobowych oraz danych z monitoringu, zgodnie z RODO, objęty jest kontrolą na poziomie wybranych administratorów
- możliwość zarządzania przez głównego administratora uprawnieniami konfiguracyjnymi programu dla innych kont z rolą administracyjną,

— monitorowanie infrastruktury - obejmujące serwery Windows, Linux, Unix, Mac, routery, przełączniki, urządzenia VoIP i firewalle w zakresie:

- wykrywania urządzeń w sieci poprzez skanowanie ping oraz arp-ping,
- wykrywania urządzeń na podstawie informacji odczytanych z Active Directory,
- wizualizacji stanu urządzeń w postaci ikon urządzeń na graficznych mapach sieci,
- wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map,
- wizualizacji połączeń pomiędzy urządzeniami a przełącznikami za pomocą linii i informacji, do którego portu przełącznika podłączone jest dane urządzenie w sposób manualny oraz automatyczny,
- serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych serwisów z monitorowaniem czasu ich odpowiedzi i procentu utraconych pakietów,

- serwerów pocztowych, program monitoruje czas logowania do serwisu odbierającego oraz czas wysyłania poczty, program ma możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS i inne), w razie gdyby przestały one odpowiadać lub funkcjonowały wadliwie.
- monitorowania serwerów WWW i adresów URL,
- cyklicznego monitorowania czasu ładowania strony internetowej, zmiany treści na stronie internetowej i statusu protokołu HTTPS,
- obsługi szyfrowania SSL/TLS w powiadomieniach e-mail,
- obsługi urządzeń SNMP wspierających SNMP v1/2/3 z szyfrowaniem oraz autoryzacją,
- obsługi komunikatów syslog i pułapek SNMP i ewidencjonowanie odebranych z nich danych.
- 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.

— w zakresie inwentaryzacji program powinien automatycznie gromadzić informacje o sprzęcie i oprogramowaniu na stacjach roboczych oraz:
1. Prezentować szczegóły dotyczące sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart itp.
2. Obejmuje m.in.: zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade.
3. Informuje o zainstalowanych aplikacjach oraz aktualizacjach Windows co bezpośrednio umożliwia audytowanie i weryfikację użytkowania licencji w organizacji.
4. Zbierać informacje w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP, itp.
5. Posiadać możliwość wysyłania powiadomienia np. e-mailem w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera.
6. Umożliwiać odczytanie numeru seryjnego (klucze licencyjne).
7. Umożliwiać automatyczne zarządzanie instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych.
8. Umożliwiać przegląd informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp.
9. Umożliwiać utworzenie listy plików użytkowników z określonym rozszerzeniem.
znalezionych na stacjach roboczych oraz ich zdalne usuwanie wraz z wykrywaniem metadanych plików użytkownika.
10. Umożliwiać wymianę plików do i ze stacją roboczą poprzez funkcję Menedżera plików. Działania administratorów wykonywane w tej funkcji powinny być logowane.
Moduł inwentaryzacji zasobów umożliwia 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,

- określenia atrybutów wymaganych, które są obowiązkowe dla wszystkich zasobów,
- określenia atrybutów dodatkowych tylko dla wybranych typów zasobów,
- definiowanie własnych list jednokrotnego wyboru jako dodatkowe informacje o zasobie,
- importu danych z zewnętrznego źródła (.CSV),
- przechowywania dowolnych dokumentów,
- 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,
- 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.

Dodatkowo powinien być dostępny agent inwentaryzacji na system Android.
Inwentaryzacja oprogramowania powinna zapewniać funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez:
1. Skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie archiwów ZIP.
2. Informacje o aplikacjach używanych w organizacji.
3. Tworzenie własnych wzorców aplikacji.
4. Tworzenie dowolnych kategorii aplikacji, np. nowe, zabronione, projektowe itp.
5. Informacje o komputerach, na których aplikacja została wykryta.
6. Zarządzanie posiadanymi licencjami.
7. Wskazywanie osób odpowiedzialnych za licencję.
8. Wskazanie użytkowników licencji.
9. Tworzenia powiązań między licencjami a dokumentami w relacji 1:N.
10. 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.
11. Łatwy audyt legalności oprogramowania oraz powiadamianie tylko w razie przekroczenia liczby posiadanych licencji.
12. Zarządzanie posiadanymi licencjami: raport zgodności licencji.
13. Możliwość przypisania do programów numerów seryjnych, wartości itp.

— w zakresie obsługi użytkowników program powinien 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,
- 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 z możliwością monitorowania kosztów wydruków

Program powinien posiadać możliwość:
- blokowania stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla stacji roboczej, na której zalogowany jest użytkownik, z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających korzystania z danych domen oraz wybranych lub dowolnych subdomen. Reguły w postaci listy domen tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane pomiędzy grupami lub kontami.
- 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 (ustawień monitorowania użytkownika w postaci raportu,
- definiowania godzin lub dni tygodnia, w których monitorowanie użytkowników jest wyłączone.
- możliwość generowania raportów dla użytkowników Active Directory niezależnie od tego, na jakich komputerach pracowali w danym czasie.
- mechanizm blokowania uruchamiania aplikacji wg maski nazwy oraz lokalizacji pliku. Reguły w postaci

listy blokowanych plików lub lokalizacji tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane pomiędzy grupami lub kontami.
- realizację pomocy zdalnej użytkownikom poprzez mechanizmy wbudowane w system,

— w zakresie ochrony danych przed wyciekiem:
1. Blokowanie urządzeń i nośników danych, z możliwością zarządzania prawami dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera firmowego lub uruchomić z nich program zewnętrzny.
2. Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskietek.
3. Blokowanie interfejsów bezprzewodowych: Wi-Fi, Bluetooth, IrDA.
4. Blokownie dotyczy tylko urządzeń służących do przenoszenia danych - inne urządzenia (drukarka, klawiatura, mysz itp.) mogą być podłączane.
5. Alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych wraz z możliwością ograniczenia alarmów tylko do nośników niezaufanych.
6. Funkcje wspierające bezpieczeństwo systemu: integracja i zarządzanie ustawieniami Windows Defender.
7. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu szyfrowania dysków BitLocker.
8. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu modułu TPM.

Zarządzanie prawami dostępu do urządzeń:
1. Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików.
2. Autoryzowanie urządzeń firmowych (przykładowo szyfrowanych): pendrive, dysków itp. - urządzenia prywatne są blokowane.
3. Całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników.
4. Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci.
5. Możliwość usuwania z listy znanych urządzeń tych nośników, które np. zostały zutylizowane.

Audyt operacji na plikach na urządzeniach przenośnych:
1. Zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych.
2. Podłączenie/odłączenie urządzenia przenośnego.

- monitorowanie operacji na plikach w lokalnych folderach komputera użytkownika.
- możliwość integracji z Active Directory - zarządzanie prawami dostępu przypisanymi do użytkowników oraz grup domenowych. Przydzielanie uprawnień do kont użytkowników lokalnych.

System powinien umożliwiać płatne rozszerzenia funkcjonalności oraz zwiększenie liczby zarządzanych stacji roboczych w ramach posiadanej licencji, w dowolnym czasie.

Wykonawca może zostać wezwany, przed podpisaniem umowy, do dostarczenia wersji czasowej systemu, celem przetestowania i potwierdzenia przez Zamawiającego spełnienia funkcjonalności określonych zgodnie z powyższymi wymaganiami.