Gmina Lelkowo

Załącznik Nr 1 do postępowania znak: I.271.2.2023

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.05.01.00-000001/21-00.

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

Dotyczy: zakupu i dostarczenia oprogramowania do zarządzania zasobami IT wspomagającego zarządzanie bezpieczeństwem informacji zgodnym z RODO.
Licencja na oferowane oprogramowanie powinna być licencją wieczystą, na co najmniej 20 stacji roboczych, nielimitowaną liczbę użytkowników i urządzeń sieciowych, z co najmniej 12 miesięczną umową serwisową i aktualizacyjną dla nowych wersji oprogramowania w trakcie trwania gwarancji serwisowej.

Miejsce wykonania usługi: Gmina Lelkowo, 14-521 Lelkowo, Lelkowo 21

Termin wykonania usługi: do 30 dni kalendarzowych od daty zawarcia umowy.

Oprogramowanie powinno posiadać budowę modułową z możliwością rozdzielania ilości licencji oraz posiadać interfejs w języku polskim. Komunikacja w systemie pomiędzy Agentem, Konsolą i Serwerem musi być szyfrowana. Moduły powinny umożliwiać kompleksowy monitoring sieci, sprzętu komputerowego na stanowiskach użytkowników pod kątem zmian sprzętowych i programowych oraz pomocy w formie interaktywnego połączenia sieciowego z obsługiwanym użytkownikiem. System musi posiadać konsolę administracyjna oraz agenta na stacje komputerowe z systemem Windows. System musi umożliwiać integrację konta użytkowników systemu z kontami użytkowników Active Directory.

W zakresie obsługi sieci program powinien wykrywać konfigurację sieci i pozwalać na jej prezentację na interaktywnych mapach. Monitorowanie powinno obejmować serwery Windows, Linux, Unix; routery, przełączniki, VoIP i firewall'e w zakresie:

1. Urządzeń SNMP wspierających SNMP v1/2/3 np. switch'e, routery, drukarki sieciowe, urządzenia VoIP itp.
2. Serwisów TCP/IP, SMB, HTTP, POP3, SNMP, IMAP, SQL i inne. Możliwość monitorowania czasu odpowiedzi oraz ilości odebranych/utraconych pakietów.
3. Wydajności systemów Windows – minimum: obciążenie procesora, zajętość dysków, obciążenie pamięci, transfer sieciowy.
4. Monitorowania działania systemu Windows: zmiana stanu usług (zatrzymanie, uruchomienie, restart), wpisy dziennika zdarzeń.

5. System powinien umożliwić generowanie raportów dla: urządzenia, wybranej mapy, całej sieci.
6. Powiadomień: pulpitowe, e-mail, SMS.
7. Możliwości nakładania na urządzenie liczników wydajności według szablonu.
8. Możliwości współpracy z urządzeniem oraz czujnikami, które będą monitorować warunki środowiska w pomieszczeniach IT (minimum temperatura, wilgotność)
9. Mapowania portów: routery i switche.

W zakresie inwentaryzacji sprzętu i audytu program powinien automatycznie gromadzić informacje o sprzęcie i oprogramowaniu urządzeń w sieci oraz:

1. Prezentować szczegółowe informacje i ewidencję czynności wykonywanych na zasobach, umożliwiać definiowanie statusów i pól oraz generowanie protokołu przekazania sprzętu.
2. Przedstawiać widok zasobów, aplikacji, dokumentów, licencji dla poszczególnego użytkownika lub osobny widok według zasobów przypisanych do urządzeń.
3. Posiadać generator dokumentów na podstawie szablonów.
4. Posiadać system zarządzania aplikacjami i licencjami umożliwiający identyfikację realnego zużycia licencji (rozliczanie licencji według użytkownika, urządzenia, numeru seryjnego lub na podstawie wersji zainstalowanej aplikacji).
5. Umożliwiać audyt inwentaryzacji sprzętu i oprogramowania.
6. Przedstawiać informacje o wpisach rejestrowych, plikach i archiwach .zip na stacji roboczej oraz szczegółowe informacje o konfiguracji sprzętowej konkretnej stacji roboczej.
7. Umożliwiać zarządzanie instalacjami/dezinstalacjami oprogramowania w oparciu o menedżera pakietów MSI oraz zdalny dostęp do managera plików z możliwością usuwania plików użytkownika.
8. Umożliwiać ewidencjonowanie zasobów takich jak: komputery, laptopy, serwery, urządzenia sieciowe, pracownicy oraz licencje wraz z możliwością dodawania, edycji oraz usuwania zasobów.
9. Umożliwiać dowolne opisywanie zasobów włącznie z ich cechami szczególnymi oraz posiadać dodatkowe konfigurowalne pola dla zasobów.
10. Pozwalać na identyfikację graficzną urządzeń, do których można przypisać zasoby.
11. Automatycznie zbierać informacje o konfiguracji sprzętu, w szczególności o:
    - parametrach płyty głównej tj. producent, nr seryjny, ilość gniazd pamięci wraz z informacją o ich zajętości;
    - pamięci RAM z podaniem specyfikacji tj. typu (DDR/DDR2/DDR3 itp.), numeru seryjnego oraz model a także informację o taktowaniu;
    - procesorach;
    - dyskach twardych z podaniem numerów seryjnych.
12. Automatycznie zbierać informacje o kontach lokalnych użytkowników systemów operacyjnych Windows wraz z informacją o ich aktywności (włączone/wyłączone), a także uprawnieniach np. administrator komputera, gość.
13. Zbierać pełne informacje o wersji zainstalowanego systemu operacyjnego Windows.
14. Odczytywać klucze instalacyjne do oprogramowania minimum dla takich programów jak: Microsoft Windows, Microsoft Office.
15. Automatycznie identyfikować oprogramowanie zainstalowane na komputerze, w tym także rozpoznawać oprogramowanie typu „portable".

16. Automatycznie rozpoznawać sposoby licencjonowania oprogramowania dzieląc je na kategorie: darmowe i płatne.
17. Pozwalać na zbieranie dowolnych innych informacji o zgromadzonych na dyskach twardych plikach np. pliki muzyczne, filmy, zdjęcia itp.
18. Umożliwiać przeglądanie zgromadzonych danych w formie tabelarycznych zestawień.

W zakresie Helpdesk (pomocy technicznej) program powinien:

1. Umożliwiać zdalny dostęp do komputera użytkownika oraz przejęcie jego konsoli, a także dwukierunkową wymianę plików.
2. Posiadać bazę zgłoszeń (możliwość zarządzania zgłoszeniami), która umożliwi użytkownikom zgłaszać problemy techniczne wraz z możliwością dodawania komentarzy, zrzutów ekranowych oraz załączników.
3. W czasie rzeczywistym przekazywać powiadomienia i zgłoszenia.
4. Posiadać bazę wiedzy z kategoryzacją artykułów z możliwością wstawiania grafik oraz filmów.
5. Posiadać komunikator (czat) z możliwością przydzielania uprawnień oraz przesyłania plików i tworzenia rozmów grupowych.
6. Umożliwiać wysyłanie komunikatów do użytkowników z możliwym/obowiązkowym potwierdzeniem odczytu.
7. Posiadać możliwość zarządzania procesami Windows z poziomu okna informacji o urządzeniu, a także zdalnej dystrybucji oraz uruchamiania plików (zdalna instalacja oprogramowania).
8. Umożliwiać integrację bazy użytkowników z Active Directory oraz zarządzanie kontami lokalnych użytkowników Windows (min. tworzenie, usuwanie, edycja, reset hasła, włączenie/wyłączenie kont).

W zakresie zarządzania użytkownikami oraz bezpieczeństwa danych program powinien:

1. Umożliwiać pełne zarządzanie użytkownikami, bazujące na grupach i politykach bezpieczeństwa,
2. Gromadzić dane przyporządkowywane do konkretnego użytkownika (wszystkie dostępy, uprawnienia, polityki aplikacji i stron oraz polityki monitorowania), które są niezależne od stacji roboczej, na której pracuje.
3. Mieć możliwość blokowania niebezpiecznych domen WWW przed przypadkowym wejściem i pobraniem złośliwego oprogramowania, blokowania uruchamianych aplikacji, monitorowania wiadomości e-mail (nagłówki) – antyphishing oraz zarządzania regułami blokowania aplikacji i stron WWW.
4. Umożliwiać rozróżnienie, na którym urządzeniu dana czynność została wykonana.
5. Umożliwiać monitorowanie ruchu sieciowego generowanego przez użytkowników – użycie łącza.
6. Umożliwiać wykonanie audytu wydruków (drukarka, użytkownik, komputer).
7. Mieć możliwość podglądu pulpitu użytkownika bez dostępu – statyczny zdalny pulpit.
8. Umożliwiać blokowanie uruchamiania procesów na podstawie lokalizacji pliku .EXE.

W zakresie kontroli dostępu do danych program powinien:

1. Przekazywać informacje o urządzeniach podłączonych do danego komputera oraz wszystkich urządzeń podłączonych do komputerów w sieci. Powiadamiać o każdej próbie podłączenia „obcego" nośnika, blokada obcego nośnika.
2. Jednoznaczne rozpoznawać urządzenia pamięci masowej m.in. pendrive, dyski USB, czytniki kart pamięci, smartphone, aparaty cyfrowe, kamery oraz inne urządzenia podłączone do komputera za pomocą portów USB działających jako pamięć masowa lub wykorzystujące protokoły MTP i PTP oraz napędów optycznych.
3. Umożliwiać włączenie blokowania wszystkich w/w urządzeń dla wybranych komputerów.
4. Umożliwiać stosowanie wyjątków pozwalających na dostęp do w/w urządzeń dla wskazanych użytkowników.
5. Zarządzanie prawami dostępu dla użytkowników (zapis, uruchomienie, odczyt).
6. Umożliwiać centralną konfigurację reguł dla całej sieci, dla wybranych map sieci oraz dla grup i użytkowników Active Directory
7. Umożliwiać monitorowanie operacji wykonywanych na w/w urządzeniach tj. informacja o zapisie pliku na urządzeniu, usunięciu pliku z urządzenia, zmianie (edycji) pliku na urządzeniu. Zawarcie dla każdej akcji daty operacji, informacji o nazwie pliku, rozmiaru oraz pełnej ścieżki dostępu do pliku.
8. Monitorowanie katalogów na dyskach komputerów.
9. Konfiguracja zakresu monitorowania i blokowania dla pojedynczych użytkowników.
10. Możliwość definiowania własnych nazw dla monitorowanych urządzeń.
11. Umożliwiać integrację z Windows Bitlocker: odczyt stanu modułu TPM oraz zaszyfrowania woluminów.

Z up. WÓJTA

mgr Agnieszka Stech

Sekretarz Gminy