SPECYFIKACJA TECHNICZNA
oprogramowania do monitorowania sieci i zarządzania zasobami IT

Oprogramowanie powinno posiadać budowę modułową z możliwością rozdzielenia ilości licencji. Moduły powinny umożliwić 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.

W zakresie obsługi sieci program powinien wykrywać konfigurację sieci automatycznie i pozwalać na jej prezentację na interaktywnych mapach. Monitorowanie infrastruktury powinno obejmować Serwery Windows, Linux, Unix, Mac; 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, HTTP, POP3, SMTP, FTP i inne. Możliwość monitorować ich czasu odpowiedzi i procentu utraconych pakietów.
3. Serwerów pocztowych
   1) program powinien monitorować zarówno serwis odbierający, jak i wysyłający pocztę.
   2) program powinien mieć możliwość monitorowania stanu systemów i wysyłania powiadomienia, w razie, gdyby przestały one odpowiadać lub wadliwie funkcjonowały (np. gdy ważne parametry znajdą się poza zakresem)
   3) program powinien mieć możliwość wykonywania operacji testowych.
   4) program musi posiadać możliwość wysłania powiadomienia, jeśli serwer pocztowy nie działa.
4. Monitorowania serwerów WWW i adresów URL
5. Monitoringu routerów i przełączników wg:
   1) zmian statusu interfejsów sieciowych,
   2) ruchu sieciowego,
   3) podłączonych komputerów,
   4) generowanego ruchu przez podłączone komputery.
6. Serwisów Windows
   Monitor serwisów Windows powinien alarmować w razie gdy serwis przestanie działać oraz pozwalać na jego uruchomienie/zatrzymanie/zrestartowanie.
7. Wydajności systemów Windows
   Obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy.

Program powinien mieć możliwość współpracowania z urządzeniem oraz czujnikami które będą monitorować warunków środowiska w pomieszczeniach IT (Temperatura, wilgotność, zalanie, otwarcie drzwi).

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

1. prezentować szczegóły dotyczące sprzętu: model, CPU, pamięci, płyty głównej, napędów, kart, etc.,
2. audyt sprzętowy powinien obejmować m.in.: zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dysku, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade,
3. informować o zainstalowanych aplikacjach oraz aktualizacjach Windows, co bezpośrednio umożliwia audytowanie i weryfikację użytkowania licencji w firmie,
4. zbierać informacje w zakresie wszystkich zmian przeprowadzonych na wybranym komputerze: instalacji/deinstalacji aplikacji, zmian adresu IP itd.,
5. posiadać możliwość wysyłania powiadomienia np. emailem w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera,
6. umożliwić odczytywania numeru seryjnego (klucze licencyjne),

Z modułem inwentaryzacji sprzętu program powinien umożliwiać prowadzenie bazy ewidencji majątku IT w zakresie:

1. przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji,
2. definiowania własnych typów (elementów wyposażenia), ich atrybutów oraz wartości - dla danego urządzenia lub oprogramowania powinna istnieć możliwość podawania dodatkowych informacji, np. numer inwentarzowy, osoba odpowiedzialna, numer i skan faktury zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu i skan gwarancji, termin przeglądu (można podać datę, po której administrator otrzyma powiadomienie o zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, inny dowolny plik .DOC, .XLS, skan dokumentu czy też własny komentarz; możliwość importu danych z zewnętrznego źródła (CSV),
3. możliwości wygenerowania zestawienia wszystkie środków trwałych, w tym urządzeń i zainstalowanego na nich oprogramowania.

Inwentaryzacja oprogramowania powinna zapewnić funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez:

1. skanowanie plików wykonywalnych i multimedialnych na dyskach komputerów oraz skanowanie archiwów,
2. zarządzanie posiadanymi licencjami; pakietami oprogramowania, licencjami dostępowymi (tzw. CAL'e) itd.,
3. łatwy audyt legalności oprogramowania oraz powiadamianie tylko w razie przekroczenia liczby posiadanych licencji - w każdej chwili powinna istnieć możliwość wykonania aktualnych raportów audytowych,
4. zarządzanie posiadanymi licencjami: raport zgodności licencji,
5. 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 analizę:

1. faktycznego czasu aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy),
2. monitorowanie procesów (każdy proces ma całkowity czas działania oraz czas wykorzystania przez użytkownika),
3. rzeczywistego użytkowania programów (m.in. procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona),
4. informacji o edytowanych przez pracownika dokumentach,
5. historii pracy (cykliczne zrzuty ekranowe),
6. listy odwiedzanych stron www (liczba odwiedzin stron z nagłówkami, liczbą i czasem wizyt),
7. transferu sieciowego użytkowników (ruch sieciowy lokalny i transfer internetowy wygenerowany przez pracowników),
8. wydruków m.in. informacje o dacie wydruku, informacje o wykorzystaniu drukarek, zestawienia pod względem użytkownika (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument drukował), 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 będzie miał możliwość monitorowania kosztów wydruków.

Program ponadto powinien posiadać możliwość blokowanie stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla danego użytkownika z możliwością definiowania wyjątków - zarówno zezwalających, jak i zabraniających korzystania z danej strony.

Kolejny moduł powinien umożliwiać realizację zdalnej pomocy użytkownikom sieci lokalnej. W ramach kontroli stacji użytkownika wymagany jest podgląd pulpitu użytkownika i możliwość przejęcia jego konsoli. Ważne aby podczas przejęcia kontroli nad komputerem pracownika zarówno pracownik jak i administrator widzieli ten sam ekran. W powyższym module powinna znajdować się baza zgłoszeń umożliwiająca użytkownikom zgłaszać problemy techniczne, które z kolei byłyby przetwarzane i przyporządkowywane odpowiednim administratorom (wg kategorii problemów) otrzymującym automatycznie powiadomienie o przypisanym im problemie do rozwiązania. Atutem będzie funkcjonalność pozwalająca użytkownikom na monitorowanie procesu rozwiązywania zgłoszonego przez niego problemu i jego aktualnego statusu, jak również wymiany informacji z administratorem za pomocą komentarzy, które mogą być wpisywane i śledzone przez obydwie strony. Moduł ten powinien zawierać również komunikator **(czat),** który umożliwiać będzie przesyłanie wiadomości pomiędzy zalogowanymi użytkownikami i administratorami.
W module tym powinna być możliwość pobrania użytkowników z Active Directory

Kolejny moduł programu powinien posiadać w sobie możliwość ochrony danych przed wyciekiem przez blokowanie portów.

Blokowanie portów i nośników danych
Program, ma możliwość zarządza prawami dostępu do wszystkich portów wejścia i wyjścia (przewodowych i bezprzewodowych) oraz urządzeń fizycznych, przez które użytkownik może skopiować pliki z komputera firmowego lub uruchomić na nim program zewnętrzny.

1. Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda SD itp., SATA, dyski przenośne, napędy CD/DVD, stacje dyskietek.
2. Blokowanie interfejsów bezprzewodowych: WiFi, Bluetooth, IrDA.
3. Blokada dotyczy tylko urządzeń do przenoszenia danych - inne urządzenia (drukarka, klawiatura itp.) można podłączyć.

Zarządzanie prawami dostępu do portów

1. Definiowanie praw użytkowników/grup do odczytu i kopiowania plików.
2. Autoryzowanie urządzeń firmowych: pendrive'ów, dysków itp. - urządzenia prywatne są blokowane.
3. Całkowite zablokowanie określonych typów portów dla wybranych lub komputerów.
4. Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci lub wybranych grup komputerów.

Audyt operacji na urządzeniach przenośnych
Zapisywanie informacji o wszystkich operacjach na urządzeniach przenośnych dla każdego użytkownika:
1. podłączenie/odłączenie pendrive'a,
2. odczyt i kopiowanie plików na/z pendrive'a.

Ochrona przed usunięciem
Program jest zabezpieczony hasłem przed ingerencją użytkownika w jego działanie i próbą usunięcia, nawet jeśli użytkownik ma prawa administratora.

Program powinien zawierać minimum 12 miesięcy pomocy technicznej oraz aktualizacji.
Program powinien być w języku polskim.

Szkolenie dwóch administratorów w trybie on-line z wystawionym certyfikatem ukończenia szkolenia.

Biała Podlaska, dnia 29 czerwca 2018 r.

Rafał Jarzębski
Informatyk