Nr pisma: DIN.0421.5.2019.4.AST
Wrocławskie Centrum Zdrowia SP ZOZ ul. Podróżnicza 26/28 53-208 Wrocław

Opis przedmiotu zamówienia (OPZ)

Na ZAMÓWIENIE PN.:
„Dostawa i wdrożenie systemu ochrony przed wyciekiem informacji DLP” ***48730000-4 - Pakiety oprogramowania zabezpieczającego***

Specyfikacja niniejsza zawiera:

Opis przedmiotu zamówienia (OPZ)

Znak postępowania DIN.0421.5.2019

I. Nazwa (firma) oraz adres Zamawiającego

Wrocławskie Centrum Zdrowia SP ZOZ
ul. Podróżnicza 26/28
53-208 Wrocław
NIP: 894 24 60 800; REGON: 000313331
tel: 71 39 11 748 Faks: **71 39 11 759,**
adres strony internetowej: http://www.spzoz.wroc.pl/bip

1. Ochrona danych przed wyciekiem (DLP)

1. Rozwiązanie musi składać się z centralnego serwera zarządzającego, konsoli zarządzania opartej na przeglądarce web oraz modułu DLP (agenta) instalowanego na komputerach użytkowników.
2. System musi umożliwić bezproblemową obsługę co najmniej 250 agentów jednocześnie.
3. System musi posiadać mechanizm automatycznej aktualizacji wszystkich swoich komponentów.
4. System musi mieć możliwość współpracy komponentów (agent/serwer) w taki sposób aby serwer mógł współpracować ze wszystkimi poprzednimi wersjami agentów przy zachowaniu jednoczesnej pracy wielu serwerów.
5. System musi znakować czasowo wszystkie zdarzenia napływające do serwera.
6. Serwer administracyjny musi oferować możliwość instalacji min. na systemach Windows Server 2008 R2 i nowszych lub serwerach opartych na systemie linux.
7. Serwer administracyjny musi umożliwiać wykonanie instalacji/dezinstalacji zdalnej agenta na stacjach roboczych.
8. Lokalny agent musi mieć możliwość egzekwowania reguł DLP niezależnie od stanu połączenia sieciowego.
9. Serwer administracyjny musi mieć możliwość dla konkretnej stacji wymuszenia komunikacji w czasie rzeczywistym w celu sprawdzania konfiguracji.
10. System powinien umożliwiać klasyfikację istotnych danych podlegających ochronie w oparciu o minimum:
    a. zawartość pliku z danymi (słowa, wyrażenia, słowniki ze słowami i wyrażeniami, wyrażenia regularne), przy czym musi być możliwe określenie minimalnej ilości wystąpień słowa/wyrażenia/wyrażenia regularnego w pliku, która powoduje wykonanie klasyfikacji dokumentu jako chronionego
    b. aplikację, która wytworzyła dane i typ pliku zawierający dane
    c. indeksy utworzone z wybranych dokumentów podlegających ochronie (tzw. fingerprint)
11. Musi istnieć możliwość zawężenia definicji chronionych danych w oparciu o:
    a. Rodzaj pliku
    b. Rozszerzenie nazwy pliku
    c. Meta dane dokumentu – co najmniej: autor, nazwa pliku, data utworzenia, data modyfikacji, szablon użyty do utworzenia dokumentu
12. Minimalny wymagany zakres działań ochronnych modułu DLP
    a. Reagować (monitorowanie, blokowanie – zależnie od konfiguracji), gdy:

i. dane chronione są kopiowane przez połączenie sieciowe
ii. dane chronione znajdują się w wychodzącym emailu z dokładnością do odbiorcy maila, domeny mailowej
iii. następuje próba wysłania danych przez przeglądarkę internetową
iv. nastąpiła próba przeniesienia danych chronionych przez schowek systemowy (clipboard)
v. nastąpiła próba przeniesienia danych chronionych na urządzenia zewnętrzne (tzw. Removable storage)

b. Dostępność różnych rodzajów reakcji modułu DLP na wykryte naruszenie polityki ochrony:
i. Blokowanie akcji (np. zablokowanie wysłania email oraz wysłanie alertu i logu do serwera zarządzającego)
ii. Monitorowania akcji (wysłanie alertu i logu do serwera zarządzającego)
iii. Powiadomienie użytkownika (wyświetlenie użytkownikowi informacji, że podjęta akcja została zablokowana / jest monitorowana przez moduł DLP oraz wysłanie alertu i logu do serwera zarządzającego)
iv. Automatyczne szyfrowanie chronionych plików podczas ich przesyłania na dysk zewnętrzny USB

c. Wykrywanie czy dane wysyłane przez email poza organizację są zaszyfrowane lub spakowane z hasłem i możliwość blokowania i rejestrowania takiej akcji przez moduł DLP

13. Wymagania dla podsystemu modułu DLP dotyczącego zarządzania urządzeniami i portami na stacjach użytkowników:
a. System musi wykrywać i blokować urządzenia podłączane przez wszystkie porty zewnętrzne komputera wliczając w to: USB, Serial, Fire-Wire, takie jak PDA, kamera cyfrowa, odtwarzacze MP3, drukarki i inne typy urządzeń oraz umożliwiać zmianę parametrów urządzeń posiadających system plików na „tylko do odczytu”
b. Musi wykrywać i blokować urządzenia Floppy Disks, USB, nagrywarki CD/DVD oraz umożliwiać zmianę parametrów urządzenia na „tylko do odczytu”
c. Rozwiązanie musi przechowywać informacje o nazwie urządzenia, czasie przyłączenia, typie urządzania, kodzie producenta i urządzenia, nr seryjnym i typie systemu plików (zależnie od typu urządzenia i jego zestawu parametrów).

2. Wymagania ogólne dla oprogramowania modułów DLP:

14. To samo oprogramowanie modułu (agenta) musi wspierać instalacje min. na systemach Windows Vista, Windows 7, Windows 8.x, Windows 10 (wersje 32/64 bit)
    a. Musi istnieć możliwość skonfigurowania modułu tak, aby jego praca była niewidoczna dla użytkownika (tryb ukryty).
    b. Musi istnieć możliwość podania w języku polskim treści informacji o powodzie podjęcia akcji przez moduł, która jest wyświetlana użytkownikowi.
    c. Moduł musi mieć możliwość: logowania zdarzenia, powiadomienia użytkownika, zablokowania zdarzenia z logowaniem oraz kopiowania przedmiotu akcji w celach dowodowych
    d. Moduł nie może wpływać na właściwą pracę użytkownika,
    e. Moduł musi w sposób minimalny wpływać na obciążenie hosta
15. Wymagania dla systemu zarządzania i raportowania DLP:
    a. System zarządzania powinien umożliwić operacje na obiektach typu: użytkownik, grupa użytkowników zsynchronizowanych z MS Active Directory
        i. Konsola zarządzania musi umożliwiać ustawienie polityk dla użytkowników, grup użytkowników lub całej domeny,
        ii. Powinna istnieć możliwość przydzielenia określonych zasad działania modułu DLP zależnie od kombinacji grup i pojedynczych użytkowników, z możliwością wyłączenia wybranych użytkowników z zasad obowiązujących dla grupy AD, do której należą
        iii. Powinna istnieć możliwość uzależnienia działania systemu DLP od stanu stacji roboczej – czy jest ona podłączona do sieci firmowej (tryb on-line) czy pracuje poza nią (tryb off-line)
    b. Proces tworzenia polityk dla systemu powinien być uproszczony przez predefiniowane szablony np.: urządzenia USB, CD/DVD-ROM itp.
    c. Rozwiązanie powinno generować log zarówno z incydentów bezpieczeństwa określonych w politykach jak i działań administratorów systemu (cele audytowe)
    d. Log musi zawierać user ID, czas zdarzenia, nazwę hosta oraz informacje o zdarzeniu takie jak: nazwa procesu, nazwa reguły, podjęte akcje, itp.
    e. System powinien umożliwiać przeglądanie na bieżąco zdarzeń napływających z komputerów objętych ochroną i wspierać generowanie własnych raportów z zebranych danych oraz umożliwiać eksport danych do postaci plików CSV i/lub formatu XML
    f. System powinien umożliwić podgląd statusu wszystkich agentów

g. Konsola zarządzania powinna mieć możliwość ograniczenia dostępu administracyjnego z podziałem co najmniej na: tylko do odczytu, przeglądanie zdarzeń, pełna administracja.

16. Administrator musi mieć możliwość ustawienia godzin w których nie będą obowiązywały użytkowników reguły kontroli aplikacji oraz stron internetowych. Godziny pracy muszą być ustalane dla poszczególnych dni tygodnia.
17. System musi posiadać możliwości audytu stacji roboczych/użytkowników w oparciu o uruchomione aplikacje, podłączane urządzenia, odwiedzane strony internetowe, dokumenty drukowane, ruch sieciowy, wysyłane oraz odbierane wiadomości e-mail oraz wykonywane czynności na plikach.

3. Szyfrowanie

18. Szyfrowanie wybranych katalogów na dysku komputera, określonych typów plików oraz urządzeń przenośnych (USB, CD/DVD):
    a. Rozwiązanie musi zapewnić:
        i. szyfrowanie plików i katalogów w ramach systemu operacyjnego i udziałów sieciowych udostępnianych przez serwery sieciowe
        ii. szyfrowanie danych kopiowanych na urządzenia zewnętrzne USB oraz CD/DVD
        iii. zabezpieczenie danych przenoszonych na USB między komputerami poprzez utworzony na USB szyfrowany kontener
        iv. integrację z podsystemem ochrony przed wyciekiem danych – DLP opisanym powyżej – co najmniej poprzez umożliwienie sterowania szyfrowaniem plików kopiowanych na nośniki USB z poziomu polityki DLP
19. System szyfrowania plików i folderów musi być możliwy do wdrożenia niezależnie od rozwiązania do szyfrowania dysków opisanego powyżej
    a. W centralnym systemie zarządzania mają być generowane i przetrzymywane klucze używane do szyfrowania oraz definiowane szczegółowe polityki działania szyfrowania plików i folderów
    b. Oprogramowanie szyfrujące na stacjach użytkowników musi komunikować się z serwerem zarządzającym w bezpieczny (transmisja szyfrowana z obustronną autentykacją) sposób z wykorzystaniem protokołów opartych na TCP/IP
    c. Rozwiązanie musi wykorzystywać algorytm min.: AES 256 do szyfrowania danych
    d. Rozwiązanie musi umożliwiać centralnie, z serwera zarządzającego:
        i. Określenie typów plików, jakie mają być szyfrowane przez wskazanie procesu jakie je tworzy i rozszerzeń plików

ii. Określenie czy i jakim kluczem mają być szyfrowane dane kopiowane na nośniki USB i CD/DVD
iii. Określenie czy pliki jakie znajdują się już wcześniej na nośniku USB mają być także zaszyfrowane po zastosowaniu polityki szyfrowania czy też pozostawione bez zmian

e. Rozwiązanie musi umożliwiać centralne zdefiniowanie katalogów na dyskach lokalnych komputerów użytkowników, które mają być zaszyfrowane
i. Musi być możliwe określenie, jaki klucz ma być użyty do szyfrowania
ii. Musi być możliwe używanie zmiennych systemowych Windows do określenia jaki folder ma być zaszyfrowany – w szczególności dla określenia folderów typu „Moje Dokumenty"
iii. Musi być możliwa zmiana widoku ikony folderu i zaszyfrowanych plików w sposób identyfikujący, że są one zaszyfrowane

20. Szyfrowanie plików i katalogów musi wykorzystywać centralnie generowane i przechowywane klucze z opcją generacji kluczy lokalnie dla wskazanych użytkowników
21. System musi posiadać możliwość zaszyfrowania całej powierzchni dysku w oparciu o funkcjonalność BitLocker z użyciem hasła lub modułu TPM.
22. System musi posiadać możliwość szyfrowania dysków zewnętrznych w oparciu o funkcjonalność BitLocker. Szyfrowanie oraz autoryzowanie do zaszyfrowanych nośników wymiennych musi być w pełni niezauważalne dla użytkownika.
23. System musi posiadać możliwość tworzenia kluczy szyfrujących które będą kompatybilne z funkcjonalnością BitLocker dla zapewnienia transparentności współdzielenia zaszyfrowanych nośników wymiennych.
24. System musi umożliwiać dostęp do danych zaszyfrowanych przez wielu użytkowników zarówno w przypadku szyfrowania plików i katalogów jak również plików szyfrowanych przy kopiowaniu na USB/CD/DVD
25. System musi zapewnić centralne przechowywanie kluczy użytych do szyfrowania danych i możliwość odzyskania zaszyfrowanych danych z ich wykorzystaniem w sytuacji awarii
26. System musi zapewniać centralne przydzielenie tych samych kluczy używanych szyfrowania do wielu użytkowników i grup użytkowników z Active Directory (AD)
27. Niezależnie od centralnie przydzielonych wspólnych kluczy dla grupy użytkowników, każdy użytkownik musi posiadać także unikalny klucz, przypisany do niego automatycznie, wykorzystywany do szyfrowania plików i katalogów
28. Musi istnieć możliwość użycia kluczy wykorzystywanych do szyfrowania plików i katalogów także w trybie off-line (kiedy stacja nie jest podłączona do sieci Zamawiającego i jeśli nie ma połączenia z centralnym serwerem zarządzającym)

29. Instalacja oprogramowania na stacji powinna się odbywać bez interwencji użytkownika
30. System szyfrowania powinien zapewnić obsługę następujących systemów operacyjnych: Windows 7, Windows 8.x, Windows 10 (wersje 32/64 bit)
31. System szyfrowania plików i katalogów powinien zapewnić obsługę następujących systemów plików:
    a) dla systemów lokalnych: NTFS, FAT32, FAT16, CDFS, UDFS
    b) dla sieciowych udziałów dyskowych: NTFS, FAT32, FAT16
32. System do szyfrowania plików i folderów musi umożliwiać także utworzenie na dowolnym nośniku USB zaszyfrowanego kontenera (folderu), do którego dostęp musi być chroniony hasłem. Dane kopiowane do tego katalogu podlegają automatycznemu szyfrowaniu.

4. Zarządzanie i inne wymagania

33. System musi monitorować i zapobiegać wyciekom danych (DLP) poprzez monitorowanie w trybie online działań użytkowników wg ściśle zdefiniowanych polityk bezpieczeństwa oraz reguł ich opisujących.
34. System musi gromadzić szczegółowe informacje o zarządzanych komputerach, automatycznie je inwentaryzując.
35. System musi pozwalać definiować polityki ochrony danych oraz reguły ochrony.
36. System musi być wyposażony w mechanizm tworzenia reguł ochrony (DLP) w oparciu o zdefiniowane polityki, nazwy użytkowników, datę ważności polityki itp.
37. System musi umożliwić monitorowanie działania danej polityki, blokowanie (dezaktywacja/aktywacja działania bez usuwania) polityki (tj. wykonywania zdefiniowanych akcji), powiadamianie o incydencie oraz pełnego logowania zdarzeń dotyczących polityki.
38. Konsola zarządzania dla aplikacji zarządzającej działającej na serwerze musi działać w oparciu o przeglądarkę WWW i połączenie HTTPS.
39. Konsola zarządzająca powinna być obsługiwana co najmniej przez przeglądarki: Opera, Firefox, Edge w najnowszych dostępnych wersjach (zgodnej z HTML5).
40. Dostęp do systemu zarządzania powinien być autentykowany w oparciu o lokalnie utworzone konta administratorów i konta z domeny Microsoft AD
41. System zarządzania ma umożliwić:
    a. centralne definiowanie i zachowanie polityk i konfiguracji dla podsystemów
    b. centralne gromadzenie i przetwarzanie logów generowanych przez podsystemy
    c. centralne opracowanie raportów na podstawie zgromadzonych danych i prezentację ich w różnych formatach

d. raporty powinny być generowane na żądanie, ale powinna istnieć możliwość określenia zakresu raportu i częstotliwości jego automatycznego generowania

42. System zarządzania musi umożliwiać automatyczne wygenerowanie alertu poprzez co najmniej wysłanie email, wykonanie wcześniej zdefiniowanego skryptu w razie wystąpienia określonego zdarzenia (np. wykryty wyciek danych poprzez email)
43. Komunikacja między zarządzanymi stacjami a serwerem zarządzania musi być inicjowana ze strony stacji i musi być autentykowana na podstawie certyfikatów serwera.
44. System musi mieć wbudowane mechanizmy automatycznej konserwacji/utrzymania zgodnie ze zdefiniowanym harmonogramem realizujące co najmniej: usuwanie zbędnych danych z systemu (dane z monitoringu uruchamianych aplikacji, uruchamianych procesów, odwiedzonych stron www, wydrukowanych dokumentów, indeksowanie bazy danych, kopie bezpieczeństwa przyrostowe i nie przyrostowe, zmniejszanie bazy danych. Harmonogram musi mieć możliwość ustalenia częstotliwości wykonywania zadania (godzina, dzień, tydzień, miesiąc), możliwość zmiany wartość parametrów wejściowych do wykonania danej konserwacji, a także zatrzymania/uruchomienia wybranych pozycji harmonogramu w dowolnym momencie. System musi prezentować historię przeprowadzonych konserwacji/utrzymania.
45. System musi umożliwiać wielokrotny (harmonogram), na życzenie, import użytkowników, struktury organizacyjnej z usługi MS Active Directory, przy czym import struktury organizacyjnej musi następować we wskazane miejsce struktury organizacyjnej systemu.
46. Administrator musi mieć możliwość tworzenia nowych kont administratorów w konsoli programu jak i ich klonowania oraz usuwania.
47. Serwer administracyjny musi posiadać funkcjonalność globalnego zablokowania oraz zezwolenia na korzystanie z określonych folderów lokalnych, sieciowych, dysków o określonych literach oraz folderów synchronizacji z usługami chmury.
48. w sytuacji jeżeli użytkownik zapomni hasła, Serwis administracyjny musi posiadać możliwość wygenerowania hasła ratunkowego do odblokowania dostępu do zaszyfrowanych dysków oraz dysków wymiennych.
49. System musi umożliwiać generowanie raportów z danymi na temat bezpieczeństwa danych, produktywności pracowników oraz utylizacji sprzętu. Raporty muszą być generowane dla wybranych grup komputerów/użytkowników w interwałach tygodniowych lub miesięcznych. Raporty powinny być przesyłane drogą e-mailową.