Wrocław 27-05-2019r.

Nr pisma: DIN.0421.5.2019.6.AST

WSZYSCY OFERENCI

Odpowiedzi na pytania Dotyczące zapytania ofertowego: „**Dostawa i wdrożenie systemu ochrony przed wyciekiem informacji DLP**" Znak sprawy: DIN.0421.5.2019

1. Rozwiązanie musi składać się z centralnego serwera zarządzającego, konsoli zarządzania opartej **na przeglądarce web** oraz modułu DLP (agenta) instalowanego na komputerach użytkowników.
Czy konsola zarządzająca może być oparta o aplikację?

Odp: *TAK, Zamawiający dopuści rozwiązanie gdzie konsola zarządzająca może być oparta o aplikację.*

3. System musi posiadać mechanizm automatycznej aktualizacji **wszystkich** swoich komponentów.
Czy automatyczna aktualizacja może dotyczyć części komponentów?

ODP. TAK, jeżeli oferowany system zachowa spójność po automatycznej aktualizacji części komponentów.

7. Serwer administracyjny musi umożliwiać wykonanie instalacji/dezinstalacji zdalnej **agenta** na stacjach roboczych.
Czy punkt może odnosić się do klienta a nie agenta?

Odp: *TAK, Zamawiający dopuści takie rozwiązanie o ile klient realizuje takie same zadania jak agent.*

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
Czy zamiast meta danych dokumentu może odnosić się do atrybutów (pochodzenie, źródło) ?

Odp: *TAK, Zamawiający dopuści takie rozwiązanie.*

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
Czy dopuszczą Państwo rozwiązanie bez tego szyfrowania?

Odp: *TAK, Szyfrowanie można realizować za pomocą innych aplikacji. Zamawiający dopuści takie rozwiązanie.*

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
Czy dopuszczą Państwo rozwiązanie bez tej funkcjonalności?

Odp: *TAK, Zamawiający dopuści takie rozwiązanie.*

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)
Czy dopuszczą Państwo wsparcie dla wymienionych systemów, ale bez systemu Vista?

Odp: *TAK, Zamawiający dopuści takie rozwiązanie.*

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)

Czy dopuszczą Państwo rozwiązanie bez tej funkcjonalności – jednak poza siecią (offline) ochrona nadal obowiązuje (bez względu na sieć do której stacja jest podpięta)?

Odp: *TAK, Zamawiający dopuści takie rozwiązanie.*

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.

Czy dopuszczą Państwo rozwiązanie bez user ID?

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.

Odp: *TAK, Zamawiający dopuści takie rozwiązanie o ile będzie możliwość identyfikacji użytkownika.*

3. Szyfrowanie

Czy rozwiązanie może być bez modułu związanego z szyfrowaniem – rozwiązanie jest klasy DLP a nie szyfrującym.

Odp: *TAK, Zamawiający dopuści takie rozwiązanie.*

4. Zarządzanie i inne wymagania

36. System musi być wyposażony w mechanizm tworzenia reguł ochrony (DLP) w oparciu o zdefiniowane polityki, nazwy użytkowników, **datę ważności polityki** itp.

Czy dopuszczą Państwo rozwiązanie bez reguł w oparciu o daty ważności?

Odp: *TAK, Zamawiający dopuści takie rozwiązanie o ile będzie możliwość aktywowania lub dezaktywacji danej polityki.*

38. Konsola zarządzania dla aplikacji zarządzającej działającej na serwerze **musi działać w oparciu o przeglądarkę WWW** i połączenie HTTPS.

Czy dopuszczą Państwo rozwiązanie działające w oparciu o aplikację?

Odp: *TAK, Zamawiający dopuści takie rozwiązanie.*

39. **Konsola zarządzająca powinna być obsługiwana co najmniej przez przeglądarki**: Opera, Firefox, Edge w najnowszych dostępnych wersjach (zgodnej z HTML5).

Czy dopuszczą Państwo rozwiązanie działające w oparciu o aplikację?

Odp: *TAK, Zamawiający dopuści takie rozwiązanie.*

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.

Czy dopuszczą Państwo rozwiązanie bez tej funkcjonalności?

Odp: *Tak, zamawiający dopuści takie rozwiązanie, pod warunkiem, że system umożliwi w jakikolwiek sposób identyfikację użytkowników.*

48. w sytuacji jeżeli użytkownik zapomni hasła, Serwis administracyjny musi posiadać możliwość wygenerowania hasła ratunkowego do odblokowania dostępu do zaszyfrowanych dysków oraz dysków wymiennych.

Czy dopuszczą Państwo rozwiązanie bez tej funkcjonalności?

Odp: *TAK, Zamawiający dopuści takie rozwiązanie.*

Kierownik Działu Informatyki
Arkadiusz Strzałkowski