SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest dostawa systemu ochrony przed wyciekiem informacji DLP (Data Loss Prevention) – Safetica ONE lub rozwiązania równoważnego (dalej jako: System DLP) wraz z kompletem niezbędnych licencji oraz zapewnieniem wsparcia technicznego i serwisu dla zaoferowanego systemu. Obecnie używana licencja wygasa dnia 19.05.2023 r.

I. Słownik pojęć i skrótów

Tag - oznaczenie stosowane na plikach i dokumentach elektronicznych, wiadomościach mailowych umożliwiające identyfikację. Tag może istnieć: w treści dodanej w metadanych, w postaci nagłówka, stopki lub dodatkowego elementu np. pliku JPEG dodanego do pliku.

Klasyfikacja dokumentów / plików – nadawanie odpowiedniej kategorii. Kategorie są możliwe do zdefiniowania i edycji np. poufne, tajne. Możliwość nadawania poprzez odpowiedni system lub funkcję np. menu kontekstowe w systemie Windows.

Polityka – inaczej zasada DLP. Pakiet stanowiący zbiór reguł, które zawierają określone warunki, akcje i wyjątki, które mogą np. monitorować pliki na podstawie ich zawartości i generować incydenty.

Agent – program / usługa instalowana na stacji końcowej, służący do nawiązania połączenia z serwerem.

Klient – program / usługa instalowany na stacji końcowej, odpowiedzialny za funkcjonowanie polityk bezpieczeństwa systemu DLP.

LTS – Long Term Support.

SCCM – System Center Configuration Manager.

MECM – Microsoft Endpoint Configuration Manager.

SIEM – Security Information and Event Management.

II. Przedmiot zamówienia obejmuje:

1) dostawę niezbędnych licencji i oprogramowania Systemu DLP dla 900 stanowisk w ramach zamówienia podstawowego na okres 12 lub 24 miesięcy, licząc od dnia 20.05.2023 r.;
2) możliwość zakupu w ramach prawa opcji 15% dodatkowych licencji, ujętych w zamówieniu podstawowym, w razie zaistnienia potrzeby (Prawo Opcji może zostać zrealizowane przez Zamawiającego w ramach jednego bądź większej liczby zamówień).
3) świadczenie serwisu i wsparcia technicznego Wykonawcy przez okres obowiązywania umowy:
   a) dostęp do wsparcia i pomocy technicznej Wykonawcy w dni robocze w godzinach 8.00-16.00, przez okres trwania umowy,
   b) usuwanie usterek i błędów (zwanych Wadami) z zachowaniem poniższych zasad:
      – potwierdzenie przyjęcia zgłoszenia dot. błędu krytycznego nastąpi niezwłocznie od wpłynięcia zgłoszenia od Zamawiającego do systemu zgłoszeniowego Wykonawcy lub Producenta. Zgłoszenie zostanie podjęte przez inżyniera Wykonawcy lub Producenta

ul. Chmielna 69, 00-801Warszawa
tel. +48 22 39 07 401
gov.pl/NCBR

najszybciej jak to będzie możliwe. Jeżeli bezpośrednią przyczyną powstania błędu krytycznego Systemu DLP jest wada w oprogramowaniu, usunięcie błędu krytycznego nastąpi poprzez współpracę Wykonawcy z producentem Rozwiązania w terminie możliwie najszybszym z punktu widzenia producenta. Przez błąd krytyczny należy rozumieć wadę w oprogramowaniu przez, którą niemożliwe jest wykonanie kluczowych funkcji w oprogramowaniu,

- rozpoczęcie prac nad usunięciem usterki musi nastąpić w terminie mnie dłuższym niż 72 godziny z wyłączeniem dni wolnych od pracy i dni świątecznych od czasu zgłoszenia usterki. Przez usterkę należy rozumieć błąd wynikający z wady systemu, który nie wpływa znacząco na pracę,
- w przypadku braku możliwości usunięcia Wad w podanych wyżej terminach, Wykonawca dostarczy i wdroży równoważne rozwiązanie zastępcze (workaround), każdorazowo w terminie usunięcia danej Wady. Rozwiązanie zastępcze musi zostać każdorazowo uzgodnione i zaakceptowane przez Zamawiającego, Rozwiązanie zastępcze może funkcjonować do momentu, aż producent oprogramowania wyda, a Wykonawca wdroży stosowną łatkę do oprogramowania usuwającą błąd krytyczny.

c) dostęp do poprawek i nowych wersji Systemu DLP,

d) dostęp do dokumentacji technicznej Systemu DLP, dostępnej co najmniej w języku angielskim,

e) usługę konsultacji w trybie 5x8 z czasem reakcji następnego dnia roboczego w zakresie konfiguracji, optymalizacji i innych czynności dotyczących Systemu DLP w wymiarze nieprzekraczającym 80 roboczogodzin (ang. man-day), zgodnie z zapotrzebowaniem Zamawiającego, możliwych do wykorzystania w terminie obowiązywania umowy. Zamawiający zastrzega sobie możliwość korzystania z usługi wsparcia technicznego i serwisu w miarę identyfikowanych potrzeb, przez co możliwe jest niewykorzystanie pełnej puli roboczogodzin.

4) zapewnienie dostępu do konta wsparcia Systemu DLP, zawierającego dostęp do bazy wiedzy oraz systemu zgłoszeń producenta;

5) świadczenie serwisu i wsparcia technicznego wykonawcy lub producenta elementów Systemu DLP przez okres 12 lub 24 miesięcy, licząc od daty podpisania bez uwag protokołu odbioru.

III. Zamawiający dopuszcza zaoferowanie rozwiązania równoważnego spełniającego następujące wymagania:

1. Zarządzanie serwerem administracyjnym

Serwer administracyjny musi:

1) umożliwiać instalację na systemach Windows Server 2019 lub nowszych. Zamawiający dopuszcza pracę na systemach z rodziny GNU/Linux pod warunkiem, że oferowana dystrybucja posiada wsparcie producenta i będzie to dystrybucja LTS;

ul. Chmielna 69, 00-801Warszawa
tel. +48 22 39 07 401
gov.pl/NCBR

2) w przypadku jeśli System DLP wymaga do pracy zewnętrznego silnika bazodanowego Wykonawca musi dostarczyć kompletne rozwiązanie tj. oprogramowanie Systemu DLP oraz silnik bazodanowy wraz z ewentualnymi licencjami wymaganymi do rekomendowanej przez producenta oprogramowania pracy (900 stacji roboczych w ramach zamówienia podstawowego lub do 1035 stacji roboczych w przypadku skorzystania przez Zamawiającego z prawa opcji). Zamawiający dopuszcza wykorzystanie zewnętrznych silników bazodanowych pod warunkiem, że posiadają one wsparcie producenta co najmniej do końca roku 2025. Zamawiający nie dopuszcza rozwiązań bazodanowych nie posiadających komercyjnego wsparcia technicznego producenta silnika bazodanowego (np. Microsoft SQL Server Express Edition);
3) działać w architekturze serwer-klient, gdzie komunikacja serwera administracyjnego z klientem odbywa się przy pomocy agenta instalowanego na stacji końcowej;
4) umożliwiać zarządzanie za pośrednictwem konsoli;
5) umożliwiać zarządzanie przez administratora bazą danych poprzez określone zadania np.: wykonanie kopii bazy danych, usunięcie kopii bazy danych, wyczyszczenie bazy danych, wykonanie kopii ustawień serwera. Administrator musi posiadać możliwość określenia wykonywania czasu związanego z wykonywaniem zadań na bazie danych (określenie interwału czasowego między wykonywanymi zadaniami);
6) posiadać funkcję automatycznej kopii bazy danych w określonym przez administratora harmonogramie;
7) umożliwiać wykonanie instalacji/deinstalacji zdalnej klienta Systemu DLP na stacjach roboczych;
8) mieć możliwość automatycznego pobierania aktualizacji definicji kategoryzowania stron internetowych, aplikacji oraz rozszerzeń plików. Musi mieć możliwość wyłączenia automatycznego pobierania;
9) komunikować się ze stacjami roboczymi za pomocą instalowanego na nich agenta i/lub klienta. W przypadku braku połączenia agenta/klienta z serwerem administracyjnym, agent/klient musi mieć możliwość lokalnego przechowywania informacji oraz zebranych danych do czasu ponownego połączenia z serwerem administracyjnym;
10) umożliwiać przygotowanie pliku instalacyjnego agenta za pośrednictwem konsoli zarządzającej. Zamawiający dopuszcza sytuację gdy producent oprogramowania Systemu DLP będzie oferować pliki instalacyjne do dystrybucji poprzez SCCM i/lub MECM;
11) posiadać konsolę dostępną z poziomu przeglądarki internetowej, służącą do raportowania i zarządzania stacjami roboczymi;
12) posiadać funkcjonalność synchronizacji użytkowników oraz stacji roboczych z usługą Microsoft Active Directory;

ul. Chmielna 69, 00-801 Warszawa
tel. +48 22 39 07 401
gov.pl/NCBR

13) zapewniać administratorowi możliwość, wymuszenia synchronizacji ustawień oraz logów, pomiędzy stacją roboczą, a serwerem, w czasie rzeczywistym;
14) umożliwiać ustawianie powiadomień dla użytkownika końcowego, w przypadku złamania reguł ustawionych w modułach związanymi z ochroną DLP. W powiadomieniu administrator musi posiadać możliwość określenia własnej grafiki, kontaktowego adresu e-mail oraz odnośnika do polityki bezpieczeństwa organizacji;
15) umożliwiać wykonanie zadania oznaczania (tagowania) plików, które już znajdują się na stacjach roboczych i zasobach sieciowych oraz nowych plików, które powstaną na bazie istniejących plików z tagami;
16) umożliwiać oznaczanie (tagowanie) plików na poziomie systemu plików lub na poziomie metadanych pliku;
17) umożliwiać klasyfikację pliku użytkownikowi na stacji końcowej. Klasyfikacja musi odbywać się poprzez integrację z menu kontekstowym. Klasyfikacja użytkownika musi posiadać opcję, która uniemożliwi użytkownikowi zmianę klasyfikacji na niższą;
18) posiadać możliwość wyznaczenia progu ilości wystąpień danych wrażliwych od jakich zostanie uruchomione zadanie tagowania;
19) Serwer administracyjny musi umożliwiać eksport identyfikatorów oznaczonych (otagowanych) plików do rozwiązania FortiMail (Zamawiający posiada Fortimail Cloud), które będzie w stanie kontrolować przesyłanie tak oznaczonych plików;
20) Serwer administracyjny musi umożliwiać integrację w stopniu umożliwiającym przesyłanie logów i incydentów DLP z Systemu DLP do oprogramowania klasy SIEM (Zamawiający posiada Splunk ES);
21) umożliwiać integrację z Office365. Integracja musi pozwalać na:
    a) audyt i logowanie wiadomości e-mail,
    b) audyt i logowanie operacji na plikach,
    c) wprowadzanie polityk zabezpieczeń do wiadomości e-mail.
22) mieć możliwość tagowania plików wrażliwych w oparciu o:
    a) aplikację, z której zostały utworzone,
    b) lokalizację lokalną lub sieciową,
    c) adres URL, z którego został pobrany plik,
    d) format pliku,
    e) zawartość pliku,
    f) autora pliku - opcjonalnie,
    g) datę utworzenia pliku – opcjonalnie.
23) posiadać możliwość wyszukiwania i ochrony plików w oparciu o ich zawartość, co najmniej o:
    a) numery kart kredytowych,

ul. Chmielna 69, 00-801Warszawa
tel. +48 22 39 07 401
gov.pl/NCBR

b) numer PESEL,
c) numer polskiego dowodu osobistego,
d) polski numer paszportu,
e) wyrażenia regularne (możliwość definiowania swoich własnych wzorców opartych na wyrażeniach regularnych),
f) określone ciągi znaków,
g) numer IBAN.

Weryfikacja zawartości pliku powinna odbywać się w czasie rzeczywistym;

24) posiadać wbudowany serwer SMTP udostępniony przez producenta oprogramowania;
25) posiadać funkcjonalność skonfigurowania reguł dostępu dla urządzeń podłączanych do portu USB, urządzeń przenośnych, nośników optycznych CD/DVD, urządzeń Firewire, urządzeń podczerwieni, urządzeń Bluetooth, portów COM oraz LPT;
26) umożliwiać określenie tzw. białych i czarnych list zawierających urządzenia pamięci masowej, drukarek fizycznych i sieciowych, lokalizacji sieciowych, adresów email, domen, urządzeń przenośnych, firewire oraz bluetooth, które mogą być wykorzystywane do określenia reguł dostępu;
27) posiadać funkcjonalność globalnego zablokowania lub zezwolenia na korzystanie z określonych folderów lokalnych, sieciowych, dysków o określonych literach oraz folderów synchronizacji z usługami chmury;
28) posiadać możliwość konfiguracji raportów w oparciu o uruchomione aplikacje, podłączane urządzenia, odwiedzane strony internetowe, drukowane dokumenty, ruch sieciowy, wysyłane wiadomości e-mail oraz wykonywane czynności na plikach;
29) posiadać możliwość wysłania alertów co najmniej za pośrednictwem wiadomości email.

2. Zarządzanie konsolą

Konsola administracyjna musi:

1) wyświetlać informacje na temat bezpieczeństwa danych, produktywności pracowników oraz utylizacji sprzętu, które są podzielone na kategorie:
   a) bezpieczeństwo danych:
      – przegląd informacji o incydentach bezpieczeństwa,
      – przegląd danych przychodzących,
      – przegląd danych wychodzących,
      – przegląd informacji z Office365 które dotyczą m.in. pobierania, współdzielenia oraz lokalnego dostępu do plików,
      – podłączane/odłączane urządzenia przenośne.
   b) produktywność:
      – przegląd informacji na temat produktywności użytkowników,

ul. Chmielna 69, 00-801Warszawa
tel. +48 22 39 07 401
gov.pl/NCBR

- aktywność użytkowników podczas przeglądania stron WWW oraz korzystania z aplikacji,
- trendy.

c) eksploatacja sprzętu:

- przegląd informacji na temat eksploatacji sprzętu komputerowego,
- eksploatacja sprzętu komputerowego, najbardziej nieaktywne komputery,
- eksploatacja drukarek,
- eksploatacji sieci.

2) umożliwiać tworzenie nowych kont administratorów w konsoli programu, jak i ich usuwanie oraz klonowanie;
3) umożliwiać pobranie pliku instalacyjnego agenta i/lub klienta;
4) posiadać możliwość wysyłania alarmów dotyczących incydentów bezpieczeństwa;
5) posiadać możliwość wysyłania powiadomień, jeśli dany użytkownik przekroczy określoną dopuszczalną ilość wysyłanych maili oraz w przypadku przekroczenia dopuszczalnej ilości wysyłanych danych do sieci w danym dniu lub tygodniu;
6) konsola webowa musi posiadać możliwość konfiguracji/zmiany domyślnego serwera SMTP;
7) konsola webowa musi umożliwiać weryfikację wersji zainstalowanego oprogramowania klienta wraz z możliwością aktualizacji do nowej wersji lub dezaktywacji tego oprogramowania;
8) konsola webowa musi umożliwiać wygenerowanie raportu w postaci pliku DOCX lub CSV, który zawiera informacje:
   a) plików przenoszonych na nośniki USB i inne urządzenia przenośne,
   b) plików przesłanych za pomocą wiadomości e-mail,
   c) plików przesłanych za pomocą poczty webowej,
   d) plików przesłanych do Internetu,
   e) plików wysłanych za pomocą komunikatorów,
   f) plików przesłanych na dyski chmurowe,
   g) analiza sposobu korzystania z aplikacji,
   h) analiza korzystania z Internetu,
   i) analiza wykorzystania portali do poszukiwania pracy.

3. Ochrona danych i bezpieczeństwo

Zamawiane oprogramowanie musi:

1) Posiadać możliwość logowania zdarzeń aktywności stacji roboczej, w oparciu o co najmniej:
   a) logowanie oraz wylogowanie użytkownika,
   b) włączenie oraz wyłączenie stacji roboczej,
   c) blokada oraz odblokowanie stacji roboczej,
   d) przejście w stan bezczynności stacji roboczej.

ul. Chmielna 69, 00-801 Warszawa
tel. +48 22 39 07 401
gov.pl/NCBR

2) Umożliwiać zablokowanie uruchomienia trybu awaryjnego na stacji końcowej;
3) Posiadać możliwości audytu stacji roboczych/użytkowników w oparciu o uruchomione aplikacje, podłączane urządzenia, odwiedzane strony internetowe, wydrukowane dokumenty, ruch sieciowy, wysyłane oraz odebrane wiadomości e-mail oraz wykonane czynności na plikach;
4) Posiadać możliwość importu własnych słowników do wyszukiwania danych;
5) Wykonać duplikat pliku lub wiadomości email, w którym znajdują się dane wrażliwe (tzw. funkcjonalność „Shadow-copy") w przypadku zaistnienia incydentu bezpieczeństwa;
   a) przypisywanie i odbieranie uprawnień do wybranych modułów programu przez administratora Systemu DLP. Zamawiający rekomenduje, aby uprawnienia były podzielone na moduły:
      – Monitorowania: wykorzystywanych aplikacji, odwiedzanych stron internetowych, wykorzystywanych plików, podłączonych urządzeń zewnętrznych oraz przesłanych i odebranych wiadomości e-mail,
      – DLP: służące do oznaczania plików, tworzenia reguł dla plików wrażliwych, tworzenia białych i czarnych list urządzeń,
      – Nadzorcy: Kontroli dostępu do stron internetowych oraz kontroli dostępu do aplikacji;
   b) tworzenie własnych kategorii dla stron internetowych, aplikacji oraz typów plików przez administratora Systemu DLP;
   c) filtrowanie oraz sortowanie zebranych danych przez administratora Systemu DLP. Tak odfiltrowane dane, administrator może zapisać w postaci plików PDF lub XLS lub CSV;
   d) wyszukiwanie danych osobowych na zasobach zarówno lokalnych jak i sieciowych przez administratora Systemu DLP.

4. Agent stacji końcowych

System DLP musi umożliwiać:

1) instalację klienta na następujących systemach operacyjnych:
   a) Microsoft Windows 10 (wersja x64),
   b) Microsoft Windows 11 (wersja x64),
   c) Mac OS X 11.x i wyżej.
2) egzekwowanie reguł DLP również w przypadku braku połączenia między klientem, a serwerem administracyjnym;
3) instalację na stacjach końcowych za pośrednictwem systemu SCCM lub MECM;
4) zabezpieczenie klienta DLP przed wyłączeniem/zawieszeniem lub dezinstalacją przez nieuprawnionego użytkownika;
5) lokalne przechowywanie informacji w przypadku zerwania połączenia z serwerem administracyjnym, do czasu ponownego połączenia;

ul. Chmielna 69, 00-801Warszawa
tel. +48 22 39 07 401
gov.pl/NCBR

6) wyświetlanie powiadomień (np. okno pop-up) dla użytkowników w języku polskim;
7) Zamawiający dopuszcza możliwość nie rozdzielania oprogramowania na klienta i agenta, a zastosowanie jednego programu/usługi pełniącej taką rolę.

5. Ochrona danych

1) dla plików otagowanych, musi być możliwe utworzenie następujących reguł:
   a) blokowanie oraz zezwalanie na zapisywanie, przenoszenie plików, do lokalizacji na określonych dyskach lokalnych,
   b) blokowanie oraz zezwalanie na zapisywanie, przenoszenie do lokalizacji na dyskach zewnętrznych z możliwością określenia białej oraz czarnej listy tych urządzeń,
   c) blokowanie oraz zezwalanie na drukowanie na określonych drukarkach,
   d) blokowanie oraz zezwalanie na zapisywanie i przenoszenie do lokalizacji sieciowej,
   e) blokowanie oraz zezwalanie na wysyłanie za pośrednictwem klientów pocztowych z możliwością określenia białej i czarnej listy adresów i domen,
   f) blokowanie oraz zezwalanie na wysyłanie do poczty webowej,
   g) blokowanie oraz zezwalanie na zapisywanie, przenoszenie plików do chmury, zarówno za pomocą przeglądarki internetowej jak i aplikacji, w oparciu o co najmniej poniższe usługi:
      – Dropbox,
      – Google Drive,
      – SharePoint,
      – OneDrive Business,
      – OneDrive Personal.
   h) blokowanie oraz zezwalanie na przesyłanie danych za pomocą komunikatorów (w szczególności MS Teams, Skype, Slack),
   i) blokowanie oraz zezwalanie na zapisywanie i przenoszenie danych poprzez usługę pulpitu zdalnego,
   j) blokowanie oraz zezwalanie na wykonywanie zrzutów ekranowych, skopiowania zawartości, nagrywania na płyty oraz wirtualnego drukowania,
   k) uruchomienie wybranego formatu pliku przez wskazaną przez administratora aplikacje,
   l) blokowanie oraz zezwalanie na przesyłanie za pomocą protokołów sieciowych takich jak http, ftp, smtp, pop3, imap, p2p oraz ich szyfrowanych odpowiedników,
   m) blokowanie oraz zezwalanie na zapisywanie poprzez Bluetooth oraz Firewire;
2) każda z polityk musi posiadać możliwość ustawienia jej w trybie powiadomienia widocznego dla użytkownika;
3) Serwer administracyjny musi posiadać możliwość zaszyfrowania całej powierzchni dysku w oparciu o funkcjonalność BitLocker (lub równoważną) z użyciem hasła lub modułu TPMv2;

ul. Chmielna 69, 00-801Warszawa
tel. +48 22 39 07 401
gov.pl/NCBR

4) Serwer administracyjny musi posiadać możliwość szyfrowania dysków zewnętrznych w oparciu o funkcjonalność BitLocker (lub równoważną). Szyfrowanie oraz autoryzacja dla zaszyfrowanych nośników wymiennych musi być w pełni niezauważalna dla użytkownika;
5) Serwer administracyjny musi posiadać możliwość wyświetlenia i eksportu klucza odzyskiwania do zaszyfrowanych dysków oraz dysków wymiennych.

6. Raportowanie i analityka

System DLP musi zapewniać generowane raportów w oparciu o wskazane stacje robocze, użytkowników bądź grupy w określonym przedziale czasu. Raporty muszą być generowane do pliku PDF i/lub XLS, CSV po podaniu lokalizacji zapisywanego pliku lub na wskazany adres(y) e-mail.

W przypadku zaoferowania oprogramowania równoważnego Wykonawca zobowiązany jest do:

1) **przeprowadzenia szkolenia z zakresu administrowania Systemem DLP, dla min. 2 osób, w terminie do 90 dni kalendarzowych od dnia podpisania bez uwag protokołu odbioru. Zamawiający wyraża zgodę na przeprowadzenie szkolenia w siedzibie Zamawiające lub online, bądź poprzez przekazanie voucherów.**
2) **przeprowadzenie przy udziale Zamawiającego wstępnej konfiguracji tj. instalacji serwera Systemu DLP oraz konsoli administracyjnej i konfigurację dwóch reguł DLP dla danych pochodzących z lokalizacji lokalnej oraz zdalnej (będącej w sieci LAN Centrum), w terminie do 10 dni roboczych od dnia zawarcia umowy. Konfiguracja wstępna nie obejmuje instalacji agentów na stacjach roboczych (klientach).**

IV. Wymagania dotyczące dostawy Systemu DLP:

1. Dostawa musi zostać zrealizowana zgodnie z terminem wskazanym w ofercie Wykonawcy, ale nie później niż 10 dni roboczych od dnia podpisania umowy;
2. Wykonawca zobowiązuje się dostarczyć wymagane oprogramowanie oraz licencje pochodzące z legalnego źródła, zakupione w autoryzowanym kanale sprzedaży producenta i objęte standardowym pakietem usług gwarancyjnych świadczonych przez sieć serwisową producenta na terenie Polski;
3. Dostawa oprogramowania, aplikacji, modułów, wymaganych do prawidłowego funkcjonowania zaoferowanego systemu DLP, zgodnie z wymaganymi funkcjonalnościami oraz specyfikacją Zamawiającego;
4. Dostawa licencji wymaganych do poprawnej pracy systemu DLP, zgodnie z wymaganymi funkcjonalnościami opisanymi w specyfikacji;
5. Dostarczone do Zamawiającego licencje muszą być w postaci wygenerowanych na stronie producenta plików licencyjnych lub w formie wygenerowanych i przesłanych emailem przez Wykonawcę plików.

ul. Chmielna 69, 00-801Warszawa
tel. +48 22 39 07 401
gov.pl/NCBR