Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

Załącznik nr 2

Szczegółowy opis przedmiotu zamówienia do zapytania ofertowego nr S.042.5.2024

I. UWIERZYTELNIANIE DWUSKŁADNIKOWE

Niniejsza specyfikacja określa wymagania dotyczące wdrożenia rozwiązania uwierzytelniania dwuskładnikowego (MFA). Rozwiązanie ma na celu ochronę poufnych danych firmowych przed nieautoryzowanym dostępem i wzmocnienie uwierzytelniania użytkowników podczas korzystania z zasobów firmowych.

Ilość licencji 17

Minimalny zakres jaki musi spełniać dostarczony sprzęt/oprogramowanie:

Ochrona:

1. Wsparcie dla systemów z rodziny Microsoft Windows Server: 2008 / 2008 R2 / 2012 / 2012 R2 / SBS 2008 / SBS 2011 / 2012 Essentials / 2012 R2 Essentials / Windows Server 2016 / Windows Server 2016 Essentials / Windows Server 2019 / Windows Server 2019 Essentials.
2. Rozwiązanie musi posiadać wbudowany serwer RADIUS umożliwiający uwierzytelnianie użytkowników dla rozwiązań VPN, które wspierają technologię RADIUS.

Aplikacja mobilna:

1. Aplikacja mobilna musi wspierać telefony działające pod kontrolą systemów mobilnych: Android (w wersji 4.4 lub wyższej), iOS (12 lub wyższej).
2. Aplikacja mobilna do generowania OTP (jednorazowego hasła) musi być dostarczona przez producenta rozwiązania w ramach zakupionej licencji.
3. Użytkownik musi mieć możliwość dodatkowego zabezpieczenia aplikacji w postaci kodu PIN.
4. Aplikacja do działania nie może wymagać od użytkownika aktywnego połączenia z Internetem – generowanie OTP (jednorazowego hasła) musi odbywać się w trybie offline.
5. Dwuskładnikowe uwierzytelnienie musi być możliwe również przy użyciu jednorazowych haseł SMS.
6. Aplikacja zainstalowana na urządzeniach mobilnych musi umożliwiać generowanie OTP dla więcej niż jednego serwera uwierzytelniającego
7. Wsparcie techniczne do programu świadczone w języku polskim, przez polskiego dystrybutora autoryzowanego przez producenta programu.

II. SYSTEM OCHRONY PRZED WYCIEKAMI

Niniejsza specyfikacja określa wymagania dotyczące zakupu i wdrożenia systemu Data Loss Prevention (DLP) dla Zleceniodawcy. Celem jest zapewnienie kompleksowej ochrony przed wyciekiem danych wrażliwych, poufnych informacji oraz danych osobowych, zarówno w formie strukturalnej, jak i niestrukturalnej. System DLP ma na celu monitorowanie, wykrywanie, zapobieganie oraz raportowanie wszelkich nieautoryzowanych prób przesyłania, kopiowania lub udostępniania danych poza organizację, zarówno poprzez kanały elektroniczne, jak i fizyczne. Dodatkowo, system DLP ma umożliwić kontrolę nad przepływem informacji w ramach organizacji, zapewniając zgodność z obowiązującymi przepisami prawa oraz wewnętrznymi politykami bezpieczeństwa.

Ilość licencji: 17

Minimalny zakres jaki musi spełniać dostarczony sprzęt/oprogramowanie:

1. System operacyjny:
a) Windows 10 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi
b) Windows 11 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi
2. Serwer administracyjny musi obsługiwać instalację na systemach: a. Windows Server 2016 (64-bit) i nowszych.
3. Serwer administracyjny musi obsługiwać bazy danych: a. MS SQL Server 2016 lub nowsze, b. MS SQL Express
4. Pomoc i dokumentacja programu dostępne w języku angielskim.
5. Konsola administracyjna i komunikaty klienta muszą być w języku polskim.
6. Konsola zarządzająca musi umożliwiać pobranie pliku instalacyjnego agenta.
7. Serwer administracyjny musi umożliwiać instalację/dezinstalację zdalnego klienta na stacjach roboczych.
8. Reguły DLP muszą być egzekwowane nawet przy braku połączenia między klientem a serwerem zarządzającym.
9. Brak połączenia klienta z serwerem zarządzającym musi umożliwiać lokalne przechowywanie informacji i zebranych danych do czasu ponownego połączenia.
10. Serwer administracyjny musi umożliwiać zarządzanie za pośrednictwem konsoli.
11. Administrator musi mieć możliwość konfiguracji automatycznej konserwacji dla bazy danych, usuwając najstarsze informacje, gdy rozmiar bazy osiągnie skonfigurowany limit.
12. Serwer administracyjny musi automatycznie pobierać aktualizacje definicji kategoryzowania stron internetowych, aplikacji i rozszerzeń plików, z opcją wyłączenia automatycznego pobierania.
13. Administrator musi mieć możliwość aby tworzyć, usuwać i konta administratorów w konsoli programu.
14. Administrator musi mieć możliwość przypisywania i odbierania uprawnień do wybranych modułów programu, podzielonych na ustawienia (konfiguracja modułu) i logi (wyświetlanie logów modułu).

15. Serwer musi synchronizować użytkowników i stacje robocze z domeną Active Directory.
16. System musi rejestrować zdarzenia aktywności stacji roboczej, takie jak logowanie, wylogowanie, włączenie, wyłączenie, blokada, odblokowanie i przejście w stan bezczynności.
17. Administrator musi móc wymusić synchronizację ustawień i logów między stacją roboczą a serwerem w czasie rzeczywistym.
18. Serwer administracyjny musi umożliwiać ustawienie powiadomień dla użytkownika końcowego w przypadku złamania reguł związanych z ochroną DLP, z możliwością dostosowania grafiki, adresu e-mail i odnośnika do polityki bezpieczeństwa.
19. Administrator musi mieć możliwość wykonać audyt stacji roboczych/użytkowników w oparciu o różne czynności, takie jak uruchomione aplikacje, podłączone urządzenia, odwiedzane strony internetowe, wydrukowane dokumenty, wysyłane i odebrane wiadomości e-mail oraz czynności na plikach.
20. Administrator musi mieć możliwość tworzenia własnych kategorii dla stron internetowych, aplikacji i typów plików.
21. Administrator musi mieć możliwość filtrowania i sortowania zebranych danych.
22. Serwer musi posiadać możliwość wysyłania alertów, przynajmniej za pośrednictwem wiadomości email.
23. Dashboardy muszą być generowane na podstawie wskazanych stacji roboczych, użytkowników lub grup w określonym przedziale czasu.
24. Serwer administracyjny musi posiadać wbudowany serwer SMTP dostarczony przez producenta oprogramowania.
25. Serwer administracyjny musi umożliwiać wykonywanie zadań kategoryzacji plików, zarówno istniejących na stacjach roboczych i zasobach sieciowych, jak i nowo powstałych na bazie już skategoryzowanych plików.
26. Serwer administracyjny musi mieć możliwość kategoryzacji plików wrażliwych na podstawie aplikacji, lokalizacji, adresu URL, formatu pliku i zawartości pliku.
27. Administrator musi mieć możliwość wyszukiwania danych osobowych na zasobach zarówno lokalnych, jak i sieciowych.
28. Dla plików skategoryzowanych, wymagana jest możliwość tworzenia reguł dotyczących blokowania i zezwalania na różne operacje, takie jak zapisywanie, przenoszenie, drukowanie, wysyłanie pocztą, wysyłanie do chmury, przesyłanie komunikatorami itp.
29. Serwer administracyjny musi umożliwiać wyszukiwanie i ochronę plików w oparciu o różne kryteria, takie jak numery kart kredytowych, numer PESEL, numer dowodu osobistego, numer paszportu, wyrażenia regularne, określone ciągi znaków i numer IBAN.
30. Weryfikacja zawartości pliku musi odbywać się w czasie rzeczywistym.
31. Serwer administracyjny musi pozwalać na eksport logów do rozwiązania SIEM.
32. Konsola musi umożliwiać konfigurację/zmianę domyślnego serwera SMTP.
33. Konsola webowa musi pozwalać na weryfikację wersji zainstalowanego oprogramowania klienta, a także umożliwia aktualizację do nowej wersji lub dezaktywację tego oprogramowania.
34. System musi ochraniać pocztę e-mail Microsoft 365, sprawdzając każdą wiadomość e-mail wysyłaną przez użytkowników Microsoft 365.
35. System musi ochraniać pliki w Microsoft 365, kontrolując aktywność plików w Microsoft SharePoint, Microsoft OneDrive dla Firm i Microsoft Teams.

36. System musi wykorzystywać mechanizm OCR (optical character recognition), aby wykrywać poufne treści w obrazach, zdjęciach i zeskanowanych dokumentach

III. OPROGRAMOWANIE SZYFRUJĄCE

Niniejsza specyfikacja określa wymagania dotyczące zakupu i wdrożenia oprogramowania szyfrującego dla Zleceniodawcy. Celem jest zapewnienie kompleksowej ochrony poufnych danych oraz informacji wrażliwych przed nieautoryzowanym dostępem, zarówno w spoczynku, jak i podczas transmisji. Oprogramowanie szyfrujące ma na celu umożliwienie bezpiecznego przechowywania danych na różnych nośnikach, takich jak dyski twarde, pamięci przenośne czy chmura obliczeniowa, a także ochronę danych przesyłanych przez sieci komputerowe, w tym Internet. Dodatkowo, oprogramowanie szyfrujące ma zapewnić zgodność z obowiązującymi przepisami prawa oraz wewnętrznymi politykami bezpieczeństwa, a także umożliwić łatwe zarządzanie kluczami szyfrującymi oraz kontrolę dostępu do zaszyfrowanych danych.

Ilość licencji: 17

Minimalny zakres jaki musi spełniać dostarczony sprzęt/oprogramowanie:

Ochrona danych - szyfrowanie

1. Konsola centralnego zarządzania musi wspierać systemy operacyjne Microsoft Windows Server 2016, 2019, 2022 oraz Microsoft Windows 10 i 11.
2. Serwer centralnego zarządzania musi współpracować co najmniej z silnikami baz danych takimi jak Microsoft SQL Server 2012, 2014, 2016, 2017, 2019 w wersji przynajmniej Express.
3. Konsola centralnego zarządzania musi pozwalać na generowanie pakietów instalacyjnych dla stacji końcowych w formacie MSI.
4. Komunikacja pomiędzy serwerem centralnego zarządzania, a serwerem proxy musi odbywać się na bezpiecznym porcie 443.
5. Administrator musi mieć możliwość tworzenia i zarządzania wieloma kluczami szyfrującymi, opartymi o kilka algorytmów szyfrujących, co najmniej AES, 3DES, Blowfish.
6. Administrator musi mieć możliwość tworzenia różnych użytkowników, mających dostęp do konsoli centralnego zarządzania wraz z możliwością przypisywania im różnych ról.
7. Administrator musi mieć możliwość tworzenia dodatkowych ról, na podstawie opcji dostępnych w konsoli centralnego zarządzania.
8. Logowanie do konsoli centralnego zarządzania powinno być objęte warunkami złożoności hasła.
9. Musi istnieć możliwość konfiguracji złożoności hasła do konsoli centralnego zarządzania, w oparciu o przynajmniej:

a) ilość znaków,
b) czy hasło ma zawierać wielkie litery,

c) czy hasło ma zawierać małe litery,
d) czy hasło ma zawierać cyfry,
e) czy hasło ma zawierać znaki specjalne,
f) okres ważności,
g) ilość nieudanych logowań.
10. Administrator musi mieć możliwość konfiguracji złożoności haseł dla użytkowników na stacjach roboczych.
11. Musi istnieć możliwość konfiguracji złożoności hasła dla użytkowników na stacjach roboczych, w oparciu o przynajmniej:
a) ilość znaków,
b) czy hasło ma zawierać wielkie litery,
c) czy hasło ma zawierać małe litery,
d) czy hasło ma zawierać cyfry,
e) czy hasło ma zawierać znaki specjalne,
f) okres ważności,
g) ilość nieudanych logowań,
h) możliwość zmiany hasła.
12. Konsola centralnego zarządzania musi gromadzić informacje o: a) nazwach stacji roboczych, na których jest zainstalowany klient systemu szyfrowania danych,
b) dacie ostatniej modyfikacji ustawień klienta systemu szyfrowania danych,
c) dacie aktywacji klienta systemu szyfrowania danych,
d) statusu szyfrowania,
e) typie urządzenia na którym jest zainstalowany klient systemu szyfrowania danych,
f) stanie polityki,
g) wersji klienta systemu szyfrowania danych,
h) wersji systemu operacyjnego stacji roboczej,
i) użytkownikach uprawnionych do logowania do oprogramowania na stacji roboczej.
13. Konsola centralnego zarządzania musi pozwalać na wygenerowanie dla każdej zaszyfrowanej stacji płyty ratunkowej.
14. Konsola musi być dostępna z poziomu interfejsu WWW.
15. Administrator musi mieć możliwość zarządzania stacjami klienckimi, które mają dostęp do sieci Internet.
16. Administrator musi mieć możliwość konfiguracji automatycznego szyfrowania pełnej powierzchni dysku po wykonanej instalacji oprogramowania.
17. Konsola centralnego zarządzania musi posiadać możliwość automatycznej aktywacji licencji w ramach kont domenowych.
18. Administrator musi mieć możliwość wykonania poniższych czynności w sposób zdalny:
a) instalacji klienta na stacji,
b) zaszyfrowania/odszyfrowania stacji,
c) wygenerowania klucza aktywacyjnego dla użytkownika,

d) administrowania kluczami szyfrującymi,
e) administrowania użytkownikami, którzy mają dostęp do stacji,
f) administrowania profilem ustawień dla użytkowników,
g) administrowania profilem ustawień dla stacji roboczych,
h) wymuszenia zmiany hasła,
i) zarządzania wieloma organizacjami z poziomu jednej konsoli.

Wymagania systemowe aplikacji klienckiej

19. System szyfrowania danych musi wspierać instalacje aplikacji klienckiej w środowisku Microsoft Windows 10 i 11 oraz w środowiskach Microsoft Windows Server 2012, 2012 R2, 2016, 2019, 2022.

Wymagania dotyczące uwierzytelniania

20. Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny.
21. Aplikacja musi umożliwiać określenie, co najmniej 127 unikalnych użytkowników, którzy będą mieć dostęp do chronionej stacji roboczej na poziomie Pre-Boot.
22. Aplikacja musi umożliwiać przetrzymywanie, co najmniej 64 kluczy szyfrujących w jednym pęku kluczy (key file).
23. Dostęp do pliku klucza musi być chroniony przy pomocy hasła. Domyślnie wykorzystywane hasło musi być hasłem systemu Windows.
24. Administrator musi posiadać możliwość modyfikacji ekranu logowania (Pre-boot).

Wymagania dotyczące ustawień aplikacji klienckiej

25. Aplikacja musi być dostępna, przynajmniej w języku polskim i angielskim.
26. Defragmentacja dysku nie może mieć negatywnego wpływu na system szyfrowania.
27. Aplikacja musi umożliwiać szyfrowanie nośników wymiennych w następujący sposób:
a) sektor po sektorze,
b) kontener.
28. Zaszyfrowany nośnik wymienny oraz nośnik CD/DVD może być odczytany na dowolnej stacji, na której nie ma zainstalowanego klienta systemu szyfrowania. Dostęp do takiego nośnika musi być możliwy po podaniu hasła.
29. Aplikacja musi pozwalać na szyfrowanie wiadomości e-mail wraz z załącznikami.
30. Aplikacja musi umożliwiać automatyczną deszyfrację otrzymywanych wiadomości e-mail.
31. Aplikacja musi pozwalać na szyfrowanie całego tekstu dokumentu, jego części, a także zawartości schowka systemowego.
32. Zaszyfrowany tekst może być odczytany, za pomocą narzędzia, dostarczanego przez producenta, na stacji bez zainstalowanego klienta systemu szyfrowania.
33. Aplikacja musi umożliwiać wybór klucza szyfrującego (w przypadku posiadania wielu kluczy w pęku), który ma być używany w procesie szyfrowania.
34. Aplikacja musi umożliwiać wybór domyślnego klucza szyfrowania.
35. Aplikacja musi umożliwiać zaszyfrowanie pliku lub folderu z poziomu menu kontekstowego.

36. Możliwe jest utworzenie skrótów klawiszowych umożliwiających zaszyfrowanie/odszyfrowanie całego tekstu dokumentu, jego części, a także zawartości schowka systemowego.
37. Aplikacja musi umożliwiać tworzenie wirtualnych partycji. Dostęp do takich partycji ma być możliwy przy użyciu klucza szyfrującego lub hasła.
38. Aplikacja musi umożliwiać zdefiniowanie wielkości wirtualnej partycji, z dokładnością do 1MB.
39. Aplikacja musi umożliwiać tworzenie zaszyfrowanego archiwum. Dostęp do takiego archiwum ma być możliwy, przy użyciu klucza szyfrującego lub hasła.
40. Aplikacja musi umożliwiać trwałe usuwanie danych za pomocą poniższych algorytmów:
a) Guttman.
b) US Department of Defence 5220.22-M (8-306. /E).
c) US Department of Defence 5220.22-M (8-306. /E, CiE).
d) Kryptograficzne losowe dane liczbowe.
41. Aplikacja musi posiadać dedykowaną wtyczkę co najmniej dla klientów pocztowych MS Outlook 2003 lub nowszych, również dostępnych z poziomu Office 365.
42. Aplikacja musi umożliwiać automatyczne zalogowanie użytkownika do pęku klucza (key file) systemu szyfrowania danych po uruchomieniu systemu operacyjnego.
43. Aplikacja musi umożliwiać automatyczne wylogowanie z aplikacji w przypadku bezczynności użytkownika w systemie.
44. Aplikacja musi posiadać opcję automatycznego odpytywania serwerów producenta o dostępność nowszych wersji.
45. Użytkownik musi posiadać możliwość ręcznego sprawdzania czy dostępna jest nowsza wersja programu, z poziomu GUI.

Wymagania dotyczące szyfrowania

46. Aplikacja musi dawać możliwość szyfrowania powierzchni dysku sektor po sektorze.
47. Szyfrowanie pełnej powierzchni dysku musi umożliwiać wykorzystanie modułu TPM.
48. Aplikacja musi umożliwiać wstrzymanie procesu szyfrowania powierzchni dysku i jego wznowienie. Proces szyfrowania danych powinien rozpocząć się od momentu, w którym został przerwany.
49. Aplikacja musi umożliwiać wstrzymanie procesu szyfrowania, w sytuacji gdy laptop nie jest podłączony do zasilania. Proces szyfrowania musi zostać wznowiony automatycznie, po podłączeniu zasilacza.
50. Wymagane jest wykorzystanie kluczy szyfrujących, utworzonych przy użyciu jednego z poniższych algorytmów szyfrowania:
a) AES (Rijndael).
b) Blowfish.
c) Triple DES (3DES).
51. Aplikacja musi umożliwiać współpracę z dyskami SSD.

52. Aplikacja musi umożliwiać współpracę z dyskami sprzętowo szyfrowanymi, działającymi w technologii TCG OPAL.
53. Aplikacja musi umożliwiać szyfrowanie danych na komputerach z UEFI.
54. Administrator musi mieć możliwość sprawdzenia, przed zaszyfrowaniem całej powierzchni dysku, czy nie pojawią się problemy po ponownym uruchomieniu komputera.
55. Administrator musi mieć możliwość opcjonalnego szyfrowania niesystemowych partycji dysku.

Wymagania dotyczące sytuacji krytycznych

56. W przypadku utraty hasła, aplikacja musi umożliwiać Administratorowi odzyskanie dostępu do zaszyfrowanego dysku poprzez użycie zdefiniowanego wcześniej hasła administratora.
57. W przypadku utraty hasła, aplikacja musi umożliwiać użytkownikowi odzyskanie dostępu do zaszyfrowanego dysku, poprzez użycie otrzymanego od administratora jednorazowego hasła, wygenerowanego z poziomu konsoli centralnego zarządzania.

Piotr Sinkiewicz

Elektronicznie podpisany przez Piotr Sinkiewicz
Data: 2024.08.23 10:29:05 +02'00'