DOSTAWA OPROGRAMOWANIA ANTYWIRUSOWEGO ORAZ OPROGRAMOWANIA DO SZYFROWANIA DYSKÓW I WIADOMOŚCI E-MAIL

ZAPYTANIE O INFORMACJĘ (RFI)

Luty 2020 r.

SPIS TREŚCI

1. INFORMACJE PODSTAWOWE

1.1. WŁASNOŚĆ DOKUMENTU

Niniejszy dokument stanowi własność Energa Informatyka i Technologie Sp. z o.o. (dalej: EITE). Kopiowanie lub rozpowszechnianie tego dokumentu, w całości lub częściowo, w jakiejkolwiek formie, jest niedozwolone bez uprzedniej zgody.

Energa Informatyka i Technologie Sp. z o.o. ma prawo zażądać w dowolnym momencie zwrotu wszystkich kopii tego dokumentu.

1.2. INFORMACJE NA TEMAT GRUPY ENERGA

Grupa ENERGA jest jedną z czterech grup elektroenergetycznych w Polsce. Siedziba spółki zarządzającej – Energa SA znajduje się w Gdańsku. Podstawowa działalność spółek Grupy obejmuje dystrybucję, wytwarzanie oraz obrót energią elektryczną, cieplną i gazem. Jesteśmy jednym z trzech największych dostawców energii elektrycznej w Polsce. Zasilamy w energię elektryczną ponad 2,9 mln klientów indywidualnych i biznesowych. Eksploatujemy ponad 184 tys. km linii energetycznych.

Wizja Grupy ENERGA zakłada stworzenie zwartej, efektywnej i innowacyjnej Grupy Kapitałowej, która dzięki współdziałaniu i wzajemnemu wspieraniu się wszystkich podmiotów Grupy jest liderem w zakresie jakości usług i obsługi na polskim rynku mediów użytkowych, stale podnoszącym swoją efektywność.

2. OPIS PRZEDMIOTU ZAPYTANIA

W związku z prowadzoną analizą rynku wykonawców, mogących zrealizować dostawę licencji i wsparcia dla oprogramowania antywirusowego oraz oprogramowania do szyfrowania dysków i wiadomości e-mail, zapraszamy Państwa do przedstawienia informacji obejmujących warunki cenowe dla realizacji powyższego, wg wskazanych informacji ogólnych oraz specyfikacji technicznej.

2.1. INFORMACJE OGÓLNE

1. Przedmiotem zapytania RFI jest zakup oprogramowania wraz z licencjami oraz wsparcie (nie przewidujemy wariantu subskrypcji), w następujących wariantach:
    a. Zakup licencji i wsparcie na okres 12 miesięcy
    b. Zakup licencji i wsparcie na okres 24 miesięcy
    c. Zakup licencji i wsparcie na okres 36 miesięcy
2. Wykaz ilości zamawianego oprogramowania
    a. Ochrona antywirusowa – 8400
    b. Szyfrowanie dysków – 3500
    c. Szyfrowanie wiadomości – 500

3. Wycena powinna uwzględniać koszty wdrożenia oprogramowania oraz przeszkolenia min. 4 osób.

2.2. SPECYFIKACJA TECHNICZNA - WYMAGANIA

CZĘŚĆ I – OCHRONA ENDEPOINT

1. Ochrona antywirusowa

1.1. Usuwanie wirusów, makro–wirusów, robaków internetowych oraz koni trojańskich (oraz wirusów i robaków z plików skompresowanych oraz samorozpakowujących się) lub kasowanie zainfekowanych plików. Ochrona przed oprogramowaniem typu „spyware" i „adware", włącznie z usuwaniem zmian wprowadzonych do systemu przez to oprogramowanie tego typu.

1.2. Wykrywanie wirusów, makro-wirusów, robaków internetowych, koni trojańskich, spyware, adware i dialerów ma być realizowane w pojedynczym systemie skanującym.

1.3. Określanie obciążenia CPU dla zadań skanowania zaplanowanego oraz skanowania na żądanie,

1.4. Skanowanie zaplanowane musi umożliwiać automatyczne pomijanie plików uznanych przez producenta za zaufane

1.5. Skanowanie plików pobranych z Internetu wraz ze skryptami umieszczonymi w sieci Internet oraz plików skompresowanych,

1.6. Zapewnienie stałej ochrony wszystkich zapisywanych, odczytywanych, a także uruchamianych plików przez mechanizm skanujący pracujący w tle wraz z metodą heurystyczną wyszukiwania wirusów (na życzenie); pliki te mogą być skanowane:

1.6.1. na dyskach twardych

1.6.2. w boot sektorach

1.6.3. na dyskietkach

1.6.4. na płytach CD/DVD

1.6.5. na zewnętrznych dyskach twardych (np. podłączonych przez port USB)

1.7. Możliwość samodzielnego pobierania aktualizacji z Internetu do stacji roboczej

1.8. Możliwość zablokowania funkcji zmiany konfiguracji klienta lub ukrycie interfejsu użytkownika klienta.

1.9. Scentralizowaną obsługę wirusów polegającą na przekazywaniu nieodwracalnie zainfekowanych plików do bezpiecznego miejsca w postaci centralnej kwarantanny na centralnym serwerze, w celu przeprowadzenia dalszych badań

1.10. Wbudowana w oprogramowanie funkcja do wysyłania podejrzanych lub zainfekowanych nowymi wirusami plików do producenta w celu uzyskania szczepionek

1.11. Wyszukiwanie i usuwanie wirusów w plikach skompresowanych (także zagnieżdżonych wewnątrz innych plików skompresowanych) w szczególności z plikach typu ZIP, GNU, LZH/LHA, BinHex, ARJ, RAR, MIME/UU, TAR, kontenery CAB,UUE, Rich Text Format,

1.12. Aktualizacja definicji wirusów nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie – serwerze czy stacji roboczej

1.13. Mikrodefinicje wirusów - przyrostowe, scentralizowane aktualizowanie klientów jedynie o nowe definicje wirusów i mechanizmy skanujące

1.14. Możliwość cofnięcia procesu aktualizacji definicji wirusów i mechanizmów skanujących – powrót do poprzedniego zastawu definicji wirusów bez konieczności deinstalacji oprogramowania czy też restartu komputerów

1.15. Możliwość natychmiastowego wymuszenia aktualizacji definicji wirusów na stacjach klienckich i serwerach.

1.16. Aktualizacja bazy definicji wirusów oraz mechanizmów skanujących, co najmniej 3 razy dziennie

1.17. Aktualizacja baz definicji musi być aplikowana tylko w czasie nieaktywności użytkownika na komputerze – jeżeli użytkownik komputera na nim pracuje, aplikacja automatycznie zostaje opóźniona

1.18. Możliwość aktualizacji bazy definicji wirusów średnio, co 1 godzinę

1.19. Heurystyczna technologia do wykrywania nowych, nieznanych wirusów

1.20. Dedykowany moduł analizy w czasie rzeczywistym zachowań aplikacji do wykrywania nowych, nieznanych zagrożeń typu robak internetowy, koń trojański, keylogger – analiza zachowania opiera się na wykonywanych przez aplikację czynnościach (tworzenie nowych plików, komunikacja z Internetem, podmiana strony w przeglądarce, itp.). Schematy szkodliwego działania powinny być generowane w procesie uczenia maszynowego (Machine Learning) zaimplementowanego na sieci składającej się z co najmniej 150milionów sond.

1.21. Dedykowany moduł analizy w czasie rzeczywistym musi być aktualizowany niezależnie od ochrony antywirusowej poprzez konsolę zarządzającą oraz niezależnie, w postaci pliku exe, który można bezpośrednio uruchomić na kliencie

1.22. Automatyczna rejestracja w dzienniku zdarzeń wszelkich nieautoryzowanych prób zmian rejestru dokonywanych przez użytkownika.

1.23. Automatyczne ponowne uruchomianie skanowania w czasie rzeczywistym, jeśli zostało wyłączone przez użytkownika mającego odpowiednie uprawnienia na z góry określony czas.

1.24. Automatyczne wymuszanie na kliencie programu pobrania zaktualizowanych definicji wirusów, jeśli aktualnie przechowywane pliki są przestarzałe

1.25. Aktualizacje definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione

1.26. Skanowanie poczty klienckiej (na komputerze klienckim)

1.27. Opóźnienie skanowania zaplanowanego w wypadku działania komputera (laptopa) na bateriach

1.28. Ściągnięcie dowolnego pliku na komputer musi spowodować sprawdzenie reputacji takiego pliku – jako reputacja rozumie się odpowiedź, co do ilość użytkowników w Internecie korzystających z danej aplikacji/pliku, czasu, kiedy aplikacja/plik pojawiła się w Internecie po raz pierwszy, oraz czy aplikacja/plik jest „dobra" czy też nie

1.29. Produkt musi umożliwić utworzenie grup, które będą miały prawo uruchamiać ściągniętą aplikacje, jeżeli będzie z niej korzystać w Internecie zdefiniowana ilość użytkowników (przynajmniej: 5, 50, 100, setki użytkowników) oraz dana aplikacja będzie widziana w Internecie od określonej ilości dni

1.30. W Windows 8 i Windows 10 wsparcie dla funkcji ELAM (Early Launch Anti-Malware) poprzez dostarczenie odpowiedniego sterownika ELAM.

1.31. Dedykowany moduł wywoływany lokalnie lub zdalnie na żądanie z serwera zarządzającego wykonujący agresywne czynności naprawcze w przypadku infekcji na komputerze.

1.32. Dla systemów typu Windows Embedded wsparcie dla Windows Embedded write filters w tym dla File-Based Write Filter (FBWF)

1.33. Możliwość wyboru wielkości definicji antywirusowych, z której będzie korzystał zainstalowany agent – system musi posiadać pełna wersję sygnatur oraz ich wersję uproszczoną znacząco mniejszą od pełnej do instalacji na systemach z niewielką ilością miejsca na dyskach oraz w systemach VDI. Najmniejsze sygnatury nie powinny być większe niż

1.34. System musi posiadać możliwość emulacji w celu analizy polimorficznego złośliwego oprogramowania.

1.35. System musi być wyposażony w dynamiczny klasyfikator próbek wykorzystujący mechanizmy uczenia maszynowego (Machine Learning) w celu wykrywania nowych wersji znanych rodzin złośliwego oprogramowania. Zbiór danych wykorzystywany w algorytmach uczących musi pochodzić z sieci składającej się z co najmniej 150mln sond. Musi istnieć możliwość konfiguracji agresywności (czułości) mechanizmu Machine Learning zarówno w

zakresie poziomu, powyżej którego zostanie zgłoszony alarm jak również w zakresie poziomu, powyżej którego system podejmie akcje remediacyjne.

2. Zapora ogniowa – system Firewall

2.1. Pełne zabezpieczenie stacji klienckich przed: atakami hakerów oraz nieautoryzowanymi próbami dostępu do komputerów i skanowaniem jego portów.

2.2. Moduł firewall ma mieć możliwość monitorowania i kontroli, jakie aplikacje łączą się poprzez interfejsy sieciowe,

2.3. Administrator może definiować połączenia, które stacja robocza może inicjować i odbierać,

2.4. Administrator może konfigurować dostęp stacji do protokołów rozszerzonych innych niż ICMP,UDP czy TCP np.: IGMP, GRE, VISA, OSPFIGP, L2TP, Lite-UDP,

2.5. Program ma pozwalać na zdefiniowanie indywidualnych komputerów lub całych zakresów adresów IP, które są traktowane, jako: całkowicie bezpieczne lub niebezpieczne

2.6. Program musi wykrywać próby wyszukiwania przez hakerów luk w zabezpieczeniach systemu w celu przejęcia nad nim kontroli

2.7. Konfiguracja zezwalanego i zabronionego ruchu ma się odbywać w oparciu o takie informacje jak: interfejs sieciowy, protokół, stacja docelowa, aplikacja, godzina komunikacji

2.8. Konfiguracja stacji ma się odbywać poprzez określenie: Adresu MAC, numeru IP, zakresu numerów IP, wskazanie podsieci, nazwy stacji DNS (FQDN) lub domeny DNS

2.9. Firewall powinien umożliwiać nagrywanie komunikacji spełniającej wskazane wymagania.

2.10. Firewall ma mieć konfigurowalną funkcjonalność powiadamiania użytkownika o zablokowanych aplikacjach. Ma istnieć możliwość dodania własnego komunikatu.

2.11. W przypadku wykrycia zdefiniowanego ruchu, firewall ma wysłać wiadomość do administratora

2.12. Uniemożliwianie określenia systemu operacyjnego i rodzaju przeglądarki internetowej przez serwery www

2.13. Uniemożliwienie określenia systemu operacyjnego poprzez analizę pakietów sieciowych wysyłanych przez stację

2.14. Uniemożliwienie przejęcia sesji poprzez losowo generowane numery sekwencji TCP

2.15. Domyślne reguły zezwalające na ruch DHCP, DNS, WINS.

3. Ochrona przed włamaniami – system IPS

3.1. Producent ma dostarczyć bibliotekę ataków i podatności (sygnatur) stosowanych przez produkt. Administrator ma mieć możliwość uaktualniania tej biblioteki poprzez konsolę zarządzającą oraz niezależnie, w postaci pliku exe, który można bezpośrednio uruchomić na kliencie.

3.2. Biblioteka ataków i podatności musi zawierać przynajmniej 4500 sygnatur.

3.3. Biblioteka sygnatur musi zawierać również sygnatury dotyczące działalności programów P2P.

3.4. Produkt ma mieć możliwość tworzenia własnych wzorców włamań (sygnatur), korzystając z semantyki Snort'a. Sygnatury te mogą działać w trybie blokuj lub rejestruj.

3.5. Wykrywanie skanowania portów

3.6. Ochrona przed atakami typu odmowa usług (Denial of Service)

3.7. Blokowanie komunikacji ze stacjami z podmienionymi MAC adresami (spoofed MAC)

3.8. Wykrywanie trojanów i generowanego przez nie ruchu

3.9. Wykrywanie prób nawiązania komunikacji za pośrednictwem zaufanych aplikacji, przez inne oprogramowanie.

3.10. Blokowanie komunikacji ze stacjami uznanymi za wrogie na zdefiniowany przez administratora czas. Ma istnieć możliwość definiowania wyjątków

3.11. System ochrony przed włamaniami musi automatycznie integrować się z przeglądarką internetową (przynajmniej z Internet Explorer oraz Firefox) – uniemożliwiając wykonanie w nich (nawet, jeżeli są podatne) szkodliwego dla nich kodu

3.12. System musi posiadać mechanizm blokowania wykorzystywania nieznanych podatności w określonym oprogramowaniu (Exploit Prevention) co najmniej dla aplikacji pakietu Office, Firefox, Internet Explorer oraz aplikacji napisanych w języku Java a także VLC. System musi implementować co najmniej 10 technik ochrony w tym następujące metody prewencji:

3.12.1. Java Exploit Protection

3.12.2. Structured Exception Handling Overwrite Protection (SEHOP)

3.12.3. Heap Spray Memory Attack

3.12.4. Forced DEP

3.12.5. Forced ASLR

3.12.6. Anti-ROP

4. Ochrona systemu operacyjnego

4.1. Produkt ma umożliwiać uruchamianie i blokowanie wskazanych aplikacji

4.2. Produkt ma umożliwiać ładownie modułów lub bibliotek DLL

4.3. Produkt ma umożliwiać kontrolę odczytywania i zapisywania na systemie plików przez wskazane aplikacje

4.4. Aplikacje powinny być rozróżniane poprzez nazwę i sygnaturę cyfrową

4.5. Produkt ma umożliwiać blokowanie wskazanego typu urządzeń przed dostępem użytkownika – urządzenia muszą być identyfikowane po ich numerze seryjnym

4.6. Produkt ma kontrolować dostęp do rejestru systemowego

4.7. Produkt ma umożliwiać logowanie plików wgrywanych na urządzenia zewnętrzne

4.8. Produkt musi automatycznie umożliwić zablokowanie pliku autorun.inf na urządzeniach zewnętrznych i na udziałach sieciowych

4.9. Polityki ochrony mają mieć możliwość pracy w dwóch trybach, testowym i produkcyjnym. W trybie testowym aplikacje i urządzenia nie są blokowane, ale jest tworzony wpis w logu

4.10. Możliwość wykluczenia dowolnej aplikacji z trybu ochrony systemu operacyjnego

4.11. Możliwość utworzenie listy zaufanych aplikacji (tzw. białej listy) i konfiguracji produktu w taki sposób, by żadna inna aplikacja/biblioteka z poza listy nie mogła uruchomić się na komputerze

4.12. Kolekcja aktualnie znajdujących się aplikacji na systemie końcowym musi być możliwa do wywołania bezpośrednio z konsoli zarządzającej – bez konieczności wykonania jakichkolwiek czynności na systemie końcowym

4.13. Możliwość utworzenia listy blokowanych aplikacji (tzw. czarnej listy) i konfiguracji produktu w taki sposób, by tylko aplikacja znajdujące się na liście nie mogły uruchomić się na komputerze

4.14. Możliwość automatycznego importu list zarówno białej, jaki i czarnej, co zdefiniowany interwał czasu

5. Mechanizm pułapek:

5.1. System musi posiadać wbudowany mechanizm pułapek pozwalający na detekcję zaawansowanych ataków poprzez obserwowanie sztucznie wytworzonych zasobów - przynęt.

5.2. System powinien umożliwiać zdefiniowanie następujących przynęt:

5.2.1. Użytkownika – przynętą są sztucznie spreparowane informacje uwierzytelniające dla użytkownika. Każda próba użycia tych informacji uwierzytelniających powinna generować alarm.

5.2.2. Proces – przynęta imituje działanie procesu innego systemu ochrony. Każda próba zatrzymania sztucznego procesu powinna generować alarm.

5.2.3. Udział sieciowy – powinna wykrywać próby połączenia z nieistniejącym, ale specjalnie spreparowanym udziałem sieciowym. Każda próba dostępu do udziału powinna generować alarm.

5.2.4. IP – przynęta polegająca na sztucznym wstrzyknięciu do systemu operacyjnego informacji o nieistniejącym adresie IP. System powinien wygenerować alarm w przypadku próby połączenia z adresem-przynętą.

5.2.5. DNS – przynęta polegająca na wstrzyknięciu w system operacyjny sztucznej domeny. Każda próba dostępu do tej domeny powinna generować alarm.

5.3. System powinien samodzielnie ustawiać i usuwać przynęty w zależności od konfiguracji polityki. Konfiguracja powinna być dostępna z interfejsu administracyjnego rozwiązania.

5.4. Mechanizm pułapek powinien mieć wspólny panel raportowania z pozostałymi elementami systemu.

6. Integralności komputera:

6.1. Oprogramowanie musi umożliwiać wykonywanie szerokiego zakresu testów integralności komputera pod kątem zgodności z polityką bezpieczeństwa urządzeń końcowych, w tym: programów antywirusowych, poprawki firmy Microsoft, dodatki Service Pack firmy Microsoft, osobistych zapór ogniowych

6.2. Testy integralności ma być przeprowadzany cyklicznie, co zdefiniowany okres czasu.

6.3. Powyższe szablony muszą być automatycznie aktualizowane ze strony producenta

6.4. Oprogramowanie musi umożliwiać wykonanie niestandardowego (dowolnie zdefiniowanego) testu integralności komputera, posiadać zaawansowaną składnie If…Then…Else.

6.5. W przypadku niestandardowego testu integralności musi istnieć dostępność następujących testów:

6.5.1. Wpisy rejestru systemu operacyjnego - istnienie, określona wartość, inne

6.5.2. Pliki - istnienie, data, rozmiar, suma kontrolna

6.5.3. Wiek, data, rozmiar pliku sygnatury oprogramowania antywirusowego

6.5.4. Zainstalowane poprawki

6.5.5. Uruchomiony proces, wersja systemu operacyjnego

6.5.6. Własny skrypt VisualBasic, wsh, itp.

6.5.7. Własna aplikacja

6.6. W przypadku niezgodności stacji z testem integralności, musi być możliwość ustawienia akcji naprawczej na poziomie pojedynczego testu. Jako możliwe operacje do wykonania, musi istnieć możliwość:

6.6.1. Uruchamianie dowolnego/własnego skryptu lub programu

6.6.2. Logowanie zdarzenia

6.6.3. Ukazanie okienka z wiadomością

6.6.4. Pobieranie oraz uruchamianie instalacji

6.7. Ma istnieć możliwość wskazania czasu oczekiwania na wykonanie akcji naprawczych.

6.8. Możliwość wymuszenia instalacji dowolnej aplikacji.

6.9. W wypadku niezgodności własnego systemu, oprogramowanie musi umożliwić zaaplikowanie dowolnego innego zestawu konfiguracji, w szczególności polityki firewallowej (zdefiniowanej

bardzo restrykcyjnie), polityki antywirusowej, polityki pobierania aktualizacji, polityki kontroli uruchamianych aplikacji i polityki kontroli urządzeń.

6.10. Musi być możliwe, nieuwzględnianie wyniku poszczególnego testu na wynik końcowy integralności komputera.

6.11. Musi istnieć możliwość stwierdzenia, że na komputerze znaleziono zagrożenie i nie można było takiego zagrożenia usunąć – na ten czas komputer powinien znaleźć się w kwarantannie.

6.12. Musi istnieć test integralności komputera, który sprawdzi czy komputer nie jest podłączony do Internetu poprzez dwie różne drogi, np. poprzez kabel sieciowy (Ethernet) i poprzez dostęp mobilny (WIFI, modem GSM, etc.)

7. Ochrona środowisk wirtualnych

7.1. Produkt musi umożliwiać identyfikacje środowiska wirtualnego, w którym działa, informacja na ten temat musi być widoczna w konsoli. Minimalnie identyfikowane środowiska to: Citrix, Microsoft, VMWare

7.2. Produkt musi umożliwiać w wypadku skanowania w czasie rzeczywistym oraz przy skanowaniu zaplanowanym, wykluczenie w środowisku wirtualnym wszystkich plików z tzw. złotego obrazu (Gold Image) - nie będą one nigdy poddawane skanowaniu

7.3. Produkt musi umożliwiać współdzielenie wyników skanowania zaplanowanego i na żądanie pomiędzy instancjami wirtualnymi - znalezienie już raz przeskanowanego tego samego pliku powoduje nieskanowanie go na systemie pytającym. Technologia ta powinna być dostępna, jako oprogramowanie instalowane w systemie operacyjnym Windows

7.4. Produkt musi umożliwiać prawidłowe rozliczenia licencji oferowanego systemu dla systemów wirtualnych typu desktop tzw. VDI, w szczególności tzw. „non-persistent”

7.5. Produkt musi umożliwiać przeskanowanie plików vmdk w poszukiwaniu zagrożeń

7.6. System musi posiadać specjalne, dedykowane sygnatury do ochrony środowisk wirtualnych. Sygnatury takie powinny się cechować przede wszystkim zmniejszonym zapotrzebowaniem na przestrzeń dyskową po zainstalowaniu oraz zmniejszonym zapotrzebowaniem na przepustowość sieci wymaganą do aktualizacji.

8. Architektura

8.1. Rozwiązanie ma mieć architekturę trój-warstwową. Klienci mają być zarządzani przez serwery, a konfiguracja rozwiązania ma być zapewniona poprzez graficzną konsolę administratora.

8.2. Rozwiązanie ma zapewniać wysoką skalowalność i odporność na awarie.

8.3. Komunikacja pomiędzy agentami i serwerem ma być szyfrowana.

8.4. Numery portów używane do komunikacji mają mieć możliwość konfiguracji przez użytkownika końcowego.

8.5. Agent ma się przełączać do innego serwera zarządzającego w przypadku niedostępności przypisanego serwera.

8.6. Serwery zarządzające mają móc replikować pomiędzy sobą informacje o agentach, ich konfiguracji oraz logi. Musi istnieć możliwość zdefiniowania kierunku replikacji logów (jednostronna lub dwustronna).

8.7. Musi istnieć możliwość zdefiniowania dowolnego klienta, jako lokalnego dostarczyciela aktualizacji – możliwość konfiguracji ilości przetrzymywanych aktualizacji, zajętości na dysku oraz konfiguracji prędkości ich pobierania z serwera zarządzającego.

8.8. Definiowanie lokalnego repozytorium musi zawierać warunki, jakie muszą być zachowane by dany komputer mógł stać się lokalnym repozytorium – warunkami muszą być przynajmniej: wersja systemu operacyjnego, adres komputera, nazwa komputera (z możliwością podania ją ze znakami specjalnymi, np.: komputer*), określonego wpisu w rejestrze.

8.9. Możliwość manualnego wskazania wybranej grupie komputerów konkretnego lokalnego dostarczyciela aktualizacji.

8.10. Możliwość uruchomienia dedykowanego narzędzia służącego do monitorowania klientów, którzy zostali lokalnymi dostarczycielami aktualizacji. Monitorowane jest ich zdrowie, ilość ściągniętych od nich danych, czy były to ściągnięte pełne definicje czy też definicje przyrostowe.

8.11. Możliwość ograniczenia pasma sieciowego od serwera zarządzającego do jego klientów w zależności od ściąganych definicji, aktualizacji klienckiej, podsieci, z której się łączą.

9. Moduł raportujący:

9.1. Produkt ma zapewniać graficzne raportowanie,

9.2. Wbudowane raporty maja pokazywać:

9.2.1. stan dystrybucji sygnatur antywirusowych, sygnatur heurystycznych oraz IDS/IPS

9.2.2. wersje zainstalowanych klientów

9.2.3. inwentaryzacje stacji roboczych (w tym wielkość dysku, zajętość dysku, wielkość pamięci RAM, wykorzystywany system operacyjny oraz procesor)

9.2.4. wykrytych wirusów, zdarzeń sieciowych, integralności komputerów

9.2.5. zainstalowane technologie i ich aktualny stan

9.3. Moduł raportowania ma pokazywać stan wykonywanych poleceń na komputerach

9.4. Możliwość zaplanowanego tworzenia raportów i przesyłania ich do danych kont pocztowych

9.5. Produkt musi umożliwiać automatyczne zbudowanie zapytań, które będą wykonywane o zdanym czasie i ich wynik będzie przechowywany w postacie kostek OLAP. Powstałe kostki muszą umożliwiać wykonywanie na nich typowych operacji takich jak zwijanie/agregacja danych, rozwijanie (bardziej szczegółowe dane), selekcja (wybór intersujących danych). Wszystkie te operacje muszą być wykonywane graficznie.

9.6. Produkt musi umożliwiać automatyczne budowanie trendów

9.7. Produkt musi umożliwiać automatyczne budowanie kluczowych wskaźników wydajności (KPI)

10. Moduł centralnego zarządzania:

10.1. Centralna instalacja, konfiguracja w czasie rzeczywistym, zarządzanie, raportowanie i administrowanie oprogramowaniem z pojedynczej konsoli

10.2. Centralna aktualizacja ochrony antywirusowej, zapory ogniowej i systemu wykrywania włamań przez administratora sieci,

10.3. Produkt ma wykrywać i raportować nieautoryzowane zmiany w konfiguracji produktu na stacji roboczej. Ma istnieć możliwość blokowania takich zmian.

10.4. Produkt ma zapewniać zarządzanie poprzez konsolę. Dostęp do konsoli ma być możliwy po wcześniejszej weryfikacji użytkownika. Produkt ma mieć możliwość definiowania wielu kont administracyjnych i niezależną konfigurację uprawnień.

10.5. Możliwość definiowania wielu niezależnych organizacji na jednym serwerze zarządzającym – informacje dostarczone do serwera zarządzającego nie będą dostępne pomiędzy organizacjami

10.6. Integracja z Microsoft Active Directory w celu importu użytkowników, listy maszyn, struktury jednostek organizacyjnych.

10.7. Konta administracyjne mają być tworzone na poziomie serwerów zarządzających i na poziomie organizacji definiowanych na serwerze.

10.8. Uprawnienia administratorów mają być ustawiane niezależnie dla każdego kontenera wewnątrz organizacji.

10.9. Możliwość utworzenia administratorów z uprawnieniami tylko do odczytu.

10.10. Konfiguracja agentów ma mieć strukturę drzewa, z mechanizmami dziedziczenia.

10.11. Uwierzytelnianie administratorów ma się odbywać w oparciu o wewnętrzną bazę danych lub z użyciem Microsoft Active Directory. Produkt ma mieć możliwość wykorzystania wielo-elementowego uwierzytelniania (np. z wykorzystaniem tokenów, certyfikatów itp.)

10.12. Dostęp do interfejsu produktu i listy funkcji dostępnych dla użytkownika ma być konfigurowany z poziomu centralnej konsoli zarządzającej.

10.13. Konfiguracja aktywna na stacji ma rozróżniać lokalizację agenta i według tego kryterium określać stosowany zestaw reguł/polityk dla agenta.

10.14. Lokalizacja ma być określana według istnienia lub nieistnienia: typu interfejsu sieciowego, numeru MAC domyślnej bramki, adresu IP, zakresu podsieci, wartości kluczy w rejestrze, komunikacji z serwerem zarządzającym, nazwy domeny, adresów serwerów WINS, DNS, DHCP, wyniku zapytania do serwera DNS.

10.15. Opis lokalizacji powinien zawierać możliwość tworzenia połączeń logicznych „I" oraz „LUB" na powyżej wymienionych elementach.

10.16. Paczki instalacyjne produktu mają pozwalać na dodanie własnej konfiguracji

10.17. W paczce instalacyjnej musi być zawarta funkcjonalność deinstalacji innych produktów bezpieczeństwa, która uruchomi się automatycznie przed instalacją produktu

10.18. Pełna funkcjonalność ma być zawarta w jednym pliku instalacyjnym

10.19. Nowe wersje oprogramowania mają być automatycznie dystrybuowane na stacje robocze w postaci różnicy między aktualnie zainstalowaną wersją na kliencie a nową wersją oprogramowania.

10.20. Produkt ma automatycznie wykrywać wszystkie urządzenia przyłączone do sieci komputerowej.

10.21. Możliwość zdefiniowania alertów administracyjnych zawierających zdarzenia:

10.21.1. błędnej autoryzacji do systemu zarządzania

10.21.2. dostępności nowego oprogramowania

10.21.3. pojawienia się nowego komputera

10.21.4. zdarzeń powiązanych z infekcjami wirusów

10.21.5. stanu serwerów zarządzających

10.22. Możliwość konfiguracji przepustowości pasma pomiędzy klientami a serwerem zarządzającym osobna dla pobieranych definicji przyrostowych, pełnych i pakietów aktualizacji

10.23. Oficjalna dokumentacja schematu bazy danych, z której korzysta system zarządzający

10.24. Pełna polska wersja językowa oprogramowania dla systemu zarządzania i stacji klienckich wraz z dokumentacją.

11. Platforma:

11.1. Oprogramowanie musi działać na systemach

11.1.1. Windows Vista (32-bit, 64-bit)

11.1.2. Windows 7 (32-bit, 64-bit; RTM and SP1)

11.1.3. Windows Embedded 7 Standard, POSReady, and Enterprise (32-bit and 64-bit)

11.1.4. Windows 8 (32-bit, 64-bit)

11.1.5. Windows Embedded 8 Standard (32-bit and 64-bit)

11.1.6. Windows 8.1 (32-bit, 64-bit), including Windows To Go

11.1.7. Windows 8.1 update for April 2014 (32-bit, 64-bit)

11.1.8. Windows 8.1 update for August 2014 (32-bit, 64-bit)

11.1.9. Windows Embedded 8.1 Pro, Industry Pro, and Industry Enterprise (32-bit and 64-bit)

11.1.10. Windows 10 (32-bit, 64-bit; RTM, November Update (2015), and Anniversary Update)

11.1.11. Windows Server 2008 (32-bit, 64-bit; R2, SP1, and SP2)

11.1.12. Windows Small Business Server 2008 (64-bit)

11.1.13. Windows Essential Business Server 2008 (64-bit)

11.1.14. Windows Small Business Server 2011 (64-bit)

11.1.15. Windows Server 2012

11.1.16. Windows Server 2012 R2

11.1.17. Windows Server 2012 R2 update for April 2014

11.1.18. Windows Server 2012 R2 update for August 2014

11.1.19. Windows Server 2016

11.2. Komponenty rozwiązania takie jak: firewall, zapobieganie włamaniom, kontrola urządzeń i aplikacji oraz kontrola integralności komputera muszą działać na wszystkich powyższych platformach 32 i 64-bitowych.

11.3. Serwer zarządzający musi działać na systemach:

11.3.1. Windows Server 2008 (64-bit)

11.3.2. Windows Server 2008 R2

11.3.3. Windows Server 2012

11.3.4. Windows Server 2012 R2

11.3.5. Windows Server 2016

12. Ochrona antywirusowa dla systemu Macintosh

12.1. Ochrona antywirusowa (z pominięciem funkcji reputacji), system IPS oraz blokada urządzeń ma działać na platformie Mac OS X 10.9, 10.10, 10.11, oraz macOS 10.12.

12.2. Klient dla system Mac ma być zarządzany przez ten sam serwer oraz z tej samej konsoli zarządzającej, co klienci Windows.

13. Ochrona antywirusowa dla systemu Linux

13.1. Ochrona antywirusowa z pominięciem funkcji reputacji ma działać na platformie:

13.1.1. CentOS 6U4, 6U5; 32-bit and 64-bit

13.1.2. Debian 6.0.5 Squeeze, Debian 8 Jessie; 32-bit and 64-bit

13.1.3. Fedora 16, 17; 32-bit and 64-bit

13.1.4. Oracle Linux (OEL) 6U2, 6U4, 6U5, 7

13.1.5. Red Hat Enterprise Linux Server (RHEL) 6U2 - 6U8, 7, 7.1, 7.2

13.1.6. SUSE Linux Enterprise Server (SLES) 11 SP1 - 11 SP3, 32-bit and 64-bit; 12

13.1.7. SUSE Linux Enterprise Desktop (SLED) 11 SP1 - 11 SP3; 32-bit and 64-bit

13.1.8. Ubuntu 12.04, 14.04, 16.04; 32-bit and 64-bit

13.2. Klient dla system Linux ma być zarządzany przez ten sam serwer oraz z tej samej konsoli zarządzającej, co klienci Windows.

CZĘŚĆ II – SZYFROWANIE DYSKÓW I WIADOMOŚCI

1. Wymagania ogólne:

1.1. System powinien pracować wydajnie w środowisku składającym się z minimum 5000 stacji roboczych

1.2. Współpraca z centrum certyfikacji Microsoft CA w zakresie wykorzystania oferowanego certyfikatu

1.3. Wykorzystanie techniki FDE (Full Disk Encryption) w procesie szyfrowania dysków twardych

1.4. System powinien posiadać mechanizmy uodparniające go na możliwe awarie takie jak np. zanik zasilania, zerwanie komunikacji z klientem – w trakcie takich stanów swojej pracy jak: szyfrowanie dysków, deszyfrowanie dysków oraz standardowa praca na zaszyfrowanym dysku.

1.5. Komunikacja klient – serwer musi być szyfrowana

1.6. System powinien mieć możliwość zarządzania klientami zainstalowanymi na komputerach nie należących do domeny oraz niebędących w firmowej sieci LAN.

1.7. Klient systemu pracujący na komputerze użytkownika nie powinien przyczyniać się do obniżenia ogólnej wydajności systemu rozumianej jako prędkość zapisu oraz odczytu danych. Weryfikacja spełnienia wymagania polegać będzie na zmierzeniu szybkości zapisu oraz odczytu danych z dysku twardego komputera/ów pochodzących z próbki, z zainstalowanym systemem operacyjnym Microsoft Windows 7 przed oraz po wykonaniu operacji szyfrowania dysku twardego. Test wypadnie pozytywnie, gdy przy zachowaniu tych samych ustawień systemu, po zaszyfrowaniu dysku, czas kopiowania pliku o rozmiarze 1GB pomiędzy zaszyfrowanymi partycjami na tym samym komputerze nie wzrośnie powyżej 20% od wartości sprzed zaszyfrowania.

1.8. Środowisko serwerowe

1.8.1. Współpraca z protokołem LDAP w zakresie pobierania danych z Active Directory

1.8.2. Współpraca z Microsoft Active Directory (w wersjach 2012, 2016 i 2019)

1.8.3. Możliwość pracy serwera zarządzającego w środowisku 64 bitowym

1.8.4. Możliwość pracy serwera zarządzającego w środowisku wirtualnym VMWare jako maszyna wirtualna

1.9. Środowisko klienckie

1.9.1. Wsparcie dla pracy w systemach

1.9.2. Microsoft Windows 7 (32 I 64 bity)

1.9.3. Microsoft Windows 10

1.9.4. Wsparcie dla w/w systemów klienckich osadzonych w wirtualnym środowisku VMWare

2. Wymagania dla serwera zarządzającego

2.1. Centralna konsola administracyjna

2.1.1. Umożliwiająca centralne zarządzanie klientami systemu

2.1.2. Udostępniająca mechanizmy raportowania (m.in. ogólny stan systemu, stan końcówek klienckich, zdarzenia w systemie)

2.1.3. Umożliwiająca bieżącą kontrolę stanu klientów systemu

2.1.4. Umożliwiająca administrację przydzielonymi rolami

2.1.5. Umożliwiająca tworzenie polityk bezpieczeństwa

2.1.6. Umożliwiająca dostosowanie uprawnień użytkowników do szyfrowania katalogów/plików

2.2. Administracja systemem oparta na rolach – rozdzielenie funkcji jakie w systemie mogą pełnić użytkownicy

2.3. Możliwość utworzenia wielu różniących się między sobą polityk bezpieczeństwa dla różnych grup użytkowników

2.4. Możliwość przypisania polityk bezpieczeństwa do użytkowników w zależności od informacji w AD (np. członkostwo w określonych Organizational Units)

2.5. Możliwość wymuszenia, zablokowania lub zgody na użycie Single – Sign – On (SSO) dla systemów Microsoft Windows XP, Vista, 7 w wersjach 32 oraz 64 bitowych, Windows 10

2.6. Możliwość konfiguracji uprawnień użytkowników systemu w zakresie szyfrowania, deszyfrowania oraz zarządzania innymi użytkownikami systemu (wraz z ich uprawnieniami)

2.7. Możliwość wymuszenia szyfrowania całego dysku/partycji startowej/partycji windows podczas instalacji oprogramowania na stacjach klienckich przy użyciu hasła/tokena/TPM

2.8. Blokada możliwości odszyfrowania dysku po określonej liczbie błędnie wprowadzonego hasła (dopuszczalna liczba błędnych prób logowania definiowana z poziomu Systemu) z możliwością dostępu do danych za pomocą Klucza korporacyjnego

2.9. Możliwość wymuszenia szyfrowania zewnętrznych pamięci masowych

2.10. Możliwość dostosowania do potrzeb i wymogów wyświetlanych komunikatów/tła tak aby przy wykorzystaniu funkcji pre-boot authentication można było przekazać osobom próbującym zalogować się do komputera dodatkowe informacje

2.11. Możliwość instalacji klienta w trybie silent – bez interakcji z użytkownikiem

2.12. Możliwość wymuszenia automatycznego szyfrowania dysku – bez interakcji z użytkownikiem – po instalacji klienta w trybie silent

2.13. Możliwość ukrywania/prezentacji ikony zainstalowanego klienta

2.14. Mysi być możliwość pobierania poprzez interfejs WWW kluczy do odszyfrowywania dysków. Funkcjonalność musi być dostępna dla uwierzytelnionych użytkowników np. operatorzy helpdesk.

2.15. System musi umożliwiać użycie sprzętowego szyfrowanie dysków Opal

2.16. System musi umożliwiać integrację z natywnymi mechanizmami szyfrowania – Bitlocker oraz FileVault.

2.17. Dla Bitlocker Integracja ma polegać na zarządzaniu kluczami kryptograficznymi i musi pozwalać na stworzenie polityki, która będzie blokowała możliwość odszyfrowania dystków komputerów, które nie łączyły się z serwerem zarządczy przez zadany okres czasu.

2.18. Musi istnieć możliwość wykorzystania sprzętowego szyfrowania poprzez użycie sprzętu zgodnego z Microsoft eDrive.

2.19. System musi umożliwiać uwierzytelnienie w pre-boot za pomocą karty SmartCard.

3. Wymagania w zakresie zabezpieczenia komputerów użytkowników oraz klienta systemu

3.1. Szyfrowanie całego dysku lub wybranych partycji z poziomu klienta systemu algorytmem AES128, AES256 (rekomendowane) gdzie klucz symetryczny użyty do szyfrowania całego dysku lub wybranych partycji jest zaszyfrowany hasłem

3.2. Obsługa polskiej klawiatury przy wykorzystaniu funkcji pre-boot authentication

3.3. Wsparcie dla klawiatury ekranowej w przypadku urządzeń przenośnych - tabletów

3.4. Deszyfrowanie dysków przy użyciu funkcji pre-boot authentication

3.5. Zabezpieczenie procesu szyfrowania dysku/partycji i danych w sytuacji restartu lub wyłączenia komputera w trakcie procesu szyfrowania

3.6. W przypadku przerwania procesu szyfrowania dysku/partycji na skutek np. awarii zasilania, wyłączenia komputera przez użytkownika lub inny, klient systemu powinien wznowić proces szyfrowania po następnym uruchomieniu komputera od miejsca, w którym szyfrowanie zostało przerwane

3.7. Odporność na uszkodzone sektory dyskowe

3.8. Szyfrowanie dysków twardych standardowych, SSD oraz hybrydowych

3.9. Szyfrowanie pamięci masowych podłączanych za pomocą portu USB w formie szyfrowania plików kopiowanych na te urządzenia. System musi automatycznie dystrybuować aplikację do deszyfracji.

3.10. Szyfrowanie plików lub katalogów za pomocą hasła lub certyfikatu nie może skutkować instalacją dodatkowego agenta systemu lub dodatkowej aplikacji

3.11. W przypadku wystąpienia sytuacji awaryjnej system ma zapewniać możliwość lokalnego – awaryjnego – dostępu do dysku i komputera przy wykorzystaniu mechanizmu pytanie – odpowiedź (self service)

3.12. Rozwiązanie musi umożliwiać dostęp do danych nawet w sytuacji, gdy uszkodzony zostanie preboot.

4. Wymagania w zakresie podpisywania i szyfrowania poczty elektronicznej oraz plików

4.1. Generowanie materiału kryptograficznego dla użytkowników o długości co najmniej RSA 2048 (rekomendowany RSA 4096)

4.2. Centralne przechowywanie kopi kluczy kryptograficznych centralnie na serwerze zarządzającym.

4.3. Możliwość importu materiału kryptograficznego użytkowników z poza organizacji.

4.4. Intuicyjne podpisywanie i szyfrowanie poczty elektronicznej za pomocą oprogramowania MS Outlook.

4.5. Podpisywanie i szyfrowanie plików materiałem kryptograficznym użytkownika.

4.6. Obsługa szyfrowania i podpisywania cyfrowego wiadomości oparte o standard Open PGP, S/MINE.

4.7. Możliwość awaryjnego odszyfrowania wiadomości kluczem administracyjnym.

4.8. Wysyłanie szyfrowanej poczty do odbiorców spoza organizacji nie posiadających własnego materiału kryptograficznego

4.9. Obsługa szyfrowanych wiadomości na urządzeniach mobilnych (system Android, iOS).

3. WYCENA

Odpowiedź na zapytanie o informację (RFI) winna zawierać specyfikację techniczną oferowanego oprogramowania oraz wycenę zakupu licencji i wsparcia w 3 wariantach, uwzględniających ilość oprogramowania będącego przedmiotem zapytania:

Warianty:

1. Licencje i wparcie na okres 12 miesięcy
2. Licencje i wparcie na okres 24 miesięcy
3. Licencje i wparcie na okres 36 miesięcy

Wykaz ilości oprogramowania:

Oprogramowanie firmy spełniające wymagania, określone w ust. 2.2. Specyfikacja techniczna – wymagania (RFI).

1. Ochrona antywirusowa – 8400
2. Szyfrowanie dysków – 3500
3. Szyfrowanie wiadomości – 500

Wycena RFI powinna uwzględniać koszty wdrożenia oraz przeszkolenia min 4 osób.

4. WYMAGANIA DOTYCZĄCE ODPOWIEDZI

1. Odpowiedź na zapytanie o informację należy przesłać drogą elektroniczną do dnia **25.02.2020** roku do godz. **12:00** na adres: Agnieszka.Gasior@energa.pl
2. Odpowiedź na zapytanie powinno zawierać, co najmniej:
   a. Wypełniony Arkusz wyceny zgodnie z **Załącznikiem nr 2,**
   b. Specyfikację oferowanego produktu.
3. Pytania dotyczące kwestii objętych niniejszym dokumentem można zadawać w terminie do dnia **18.02.2020** roku do godz. **12:00** kierując je do osoby uprawnionej do kontaktowania się z Wykonawcami zgodnie z pkt. 1 powyżej.
4. Zadawane pytania należy wpisać z wykorzystaniem szablonu określonego w **Załączniku nr 1** do Zapytania.
5. Pytania i udzielone przez EITE odpowiedzi zostaną przesłane do wszystkich Wykonawców w miarę możliwości niezwłocznie, bez ujawniania zadającego pytania, z zastrzeżeniem jak poniżej.

5. INFORMACJE DODATKOWE

1. Niniejszy dokument stanowi zapytanie informacyjnie (RFI), które nie stanowi zaproszenia do złożenia oferty w rozumieniu ustawy z dnia 23 kwietnia 1964 Kodeksu Cywilnego (tekst jednolity z 16 maja 2019 r., Dz. U. z 2019 r. poz. 1145 z późn. zm.).
2. Niniejsze Zapytanie o Informacje nie jest elementem jakiegokolwiek postępowania w rozumieniu ustawy z dnia 29 stycznia 2004r. Prawo zamówień publicznych (tekst jednolity z 11 września 2019 r., Dz. U. z 2019 r. poz. 1843 z późn. zm.).
3. Złożenie odpowiedzi na niniejsze Zapytanie o Informację jest jednoznaczne z wyrażeniem zgody przez podmiot składający odpowiedź na nieodpłatne wykorzystanie przez Zamawiającego

wszystkich wskazanych w odpowiedzi na Zapytanie o Informację danych do ewentualnego przygotowania przez Zamawiającego opisu przedmiotu zamówienia, szacunkowej wartości zamówienia, warunków umowy lub innych dokumentów niezbędnych dla postępowania zakupowego z zastrzeżeniem, że Zamawiający nie ujawni podmiotom trzecim tych danych, a także źródła ich uzyskania.

4. Każdy podmiot, który otrzymał niniejsze Zapytanie, samodzielnie ponosi wszelkie koszty w związku z udziałem w Zapytaniu. Za udział w Zapytaniu podmioty w nim uczestniczące nie otrzymują wynagrodzenia.
5. Prosimy o przedstawienie najbardziej korzystnej dla ENERGA Informatyka i Technologie Sp. z o.o. odpowiedzi.

6. ZAŁĄCZNIKI

Integralną częścią niniejszego Zapytania o informację są wymienione poniżej Załączniki

Załącznik nr 1 - Arkusz pytań

Załącznik nr 2 - Arkusz wyceny