Fundusze Europejskie Polska Cyfrowa | Rzeczpospolita Polska | Centrum Projektów Polska Cyfrowa | Unia Europejska Europejski Fundusz Rozwoju Regionalnego

ZAPYTANIE OFERTOWE

1. Zamawiający Gmina Raczki, Plac Kościuszki 14, 16-420 Raczki zaprasza do udziału w postępowaniu na zadanie: : „Dostawa sprzętu IT" w ramach realizacji Grantu: **„Cyfrowa gmina"** współfinansowanego przez Unię Europejską w ramach Europejskiego Funduszu Rozwoju Regionalnego, Program Operacyjny Polska Cyfrowa (POPC) na lata 2014-2020, pakiet REACT-UE

2. Przedmiot zamówienia obejmuje dostawę i montaż/uruchomienie sprzętu i oprogramowania IT zgodnego z OPZ stanowiącego załącznik do Zapytania.

Cena obejmuje wszystkie koszty niezbędne do realizacji zamówienia w tym także wszelkie koszty związane z transportem oraz z udzieloną gwarancją.

Wykonawca udzieli 2 letniej gwarancji liczonej od dnia przekazania na zakupione sprzęty zgodnie z gwarancją producenta z obowiązkiem podjęcia działań serwisowych w siedzibie Zamawiającego w terminie 2 dni od momentu skutecznego powiadomienia Wykonawcy przez Zamawiającego. W przypadku konieczności przekazania sprzętu do serwisu znajdującego się poza siedzibą Zamawiającego w ramach udzielonej gwarancji, Wykonawca zapewni nowy sprzęt zastępczy o parametrach nie gorszych od dostarczonego w ramach przedmiotowej umowy.

Zamawiający zawrze umowę z Wykonawcą dotyczącą realizacji Zamówienia.

3. Termin realizacji zamówienia: do 31.08.203 r.
4. Miejsce i termin złożenia oferty: ug@raczki.pl do dnia 14.04.2023r. do godz. 10^{00}.
5. Przy wyborze oferty zostaną zastosowane następujące kryteria oceny ofert:

Cena:

C = 100 pkt – najniższa cena

6. Termin otwarcia ofert: 14.04.2023r.
7. Warunki płatności: 14 dni od wystawienia faktury.
8. Osoba upoważniona do kontaktu z wykonawcami: Mariusz Zalewski tel. 875686426.
9. Sposób przygotowania oferty:

ofertę należy sporządzić w formie elektronicznej, w języku polskim z wykorzystaniem formularza stanowiącego załącznik do ogłoszenia. Do formularza należy dołączyć specyfikację oferowanego sprzętu w celu potwierdzenia spełniania minimalnych wymagań dostaw sprzętu.

10. W załączeniu do zaproszenia przesyłamy
    - formularz ofertowy
    - OPZ

WÓJT

Andrzej Szyndzielorz

Zatwierdzam 03.04.2023 r.
WÓJT
Andrzej Szymanowski

Fundusze Europejskie Polska Cyfrowa | Rzeczpospolita Polska | Centrum Projektów Polska Cyfrowa | Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Szczegółowy Opis Przedmiotu Zamówienia - Postępowanie Dostawa sprzętu IT dla grantu "Cyfrowa Gmina" realizowanego przez Gminę Raczki

1. **Dostawa urządzeń – (NAS – 1 szt., Dysk HDD – 2 szt., Dysk SSD – 2 szt., Szyny do serwerów 1szt. SWITCH -2 szt.)**

Minimalne wymagania:

1.	**NAS**	obudowa typu 2U, czterordzeniowy procesor 1,7 GHz, SODIMM DDR4 slot z 4GB pamięci RAM (obsługa do 16GB), 2x 10 Gigabit Ethernet (10G/2.5G/1G/100M),
2.	**Dyski**	Typ dysku - SSD Pojemność - minimum 4000GB Rodzaj dysku - wewnętrzny Interfejs - Serial ATA III Szybkość zapisu – 530 MB/s Szybkość odczytu – 560 MB/s
3.	**Dyski**	Typ dysku - HDD Pojemność - minimum 4000GB Rodzaj dysku - wewnętrzny Interfejs - Serial ATA III Prędkość obrotowa 7200 obr./min Pamięć cache –minimum 128 MB
4.	**Szyny do serwerów rack RAIL-B02**	Szyny do montażu serwerów 2Uw szafach RAIL B02
5.	**Switch**	Przeznaczenie – do szafy Typu RACK 19" Porty – 1GB – 24szt. Bufor pamięci – 512 KB

2. **UTM NASK (1szt ze stałym wparciem technicznym + licencja (12 miesięcy))**

Minimalne wymagania techniczne:

Lp.	**Nazwa komponentu**	**Wymagane minimalne parametry techniczne komputerów**	
1.	**Wydajność systemu**	Przepustowość Firewall-a (1518/512/64 bajtowe pakiety UDP)	5/5/5 Gbps
		Opóźnienie Firewall-a (64 bajtowe pakiety UDP)	2,97 µs
		Przepustowość Firewall-a (Pakiety na sekundę)	7,5 Mpps
		Sesje równoczesne (TCP)	700000

		Zasady Firewall-a	5,000
		Przepustowość IPsec VPN (512 bajtów)	4,4 Gbps
		Tunele Gateway-to-Gateway IPsec VPN	200
		Tunele Client-to-Gateway IPsec VPN	250
		Przepustowość SSL-VPN	490 Mbps
		Równoczesna liczba użytkowników SSL-VPN (Rekomendowane Maksimum, Tryb tunelowy)	200
		Inspekcja SSL CPS (IPS, HTTPS)	310
		Przepustowość Kontroli Aplikacji (HTTP 64K)	990 Mbps
		Przepustowość CAPWAP (HTTP 64K)	3,5 Gbps
		Wirtualne Domeny (Domyślnie/Maksimum)	10/10
		Maksymalna liczba wspieranych switch	8
		Maksymalna liczba AP (Całkowita/Tryb tunelowy)	16/8
		Maksymalna liczba tokenów	500
		Konfiguracje wysokiej dostępnośći	Aktywny/Aktywny, Aktywny/Pasywny, Grupowanie
2.	**Wydajność systemu – Enterprise Traffic Mix**	Przepustowość IPS	1 Gbps
		Przepustowość NGFW	800 Mbps
		Przepustowość ochrony przed zagrożeniami	600 Mbps
3.	**Specyfikacja sprzętowa**	- 1x GE RJ45 WAN/DMZ - 3x GE RJ45 - 1x GE RJ45 link - 1x Porty USB - 1x Konsola (RJ45)	
4.	**Licencja**	Sprzęt dostarczony w formie zakupu jednorazowego - 1 szt. Licencja – 12 miesięcy Urządzenia klasy NGFW z licencją odnawialną zapewniającą dostęp do nowych aktualizacji oprogramowania przez producenta. Urządzenia z licencją wieczystą nie będą brane pod uwagę z uwagi na ryzyko zaprzestania aktualizacji oprogramowania przez producenta o nowo wykryte	

		luki w oprogramowaniu.

3. **Specjalistyczne oprogramowanie ochrona antywirusowa i antyspyware**

1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami
2. Pomoc techniczna, interfejs oraz dokumentacja dostarczona i świadczona w języku polskim.
3. Wykrywanie zagrożeń i analiza procesów technikami heurystycznymi
4. Powiadomienia z modułu sprawdzającego procesy są wzbogacone o ścieżkę i identyfikator procesu nadrzędnego, a także o wiersz poleceń, który uruchomił proces. Jeśli ma to miejsce te dane są również przesyłane za pośrednictwem Syslog.
5. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
6. Wbudowana technologia do ochrony przed rootkitami.
7. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
8. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie".
9. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
10. Możliwość skanowania dysków sieciowych i dysków przenośnych.
11. Skanowanie plików spakowanych i skompresowanych.
12. Możliwość dodawania wykluczeń na podstawie

a. Plik
b. Folder
c. Rozszerzenie
d. Proces
e. Hash pliku
f. Hash certyfikatu
g. Nazwa zagrożenia
h. Wiersz poleceń
i. IP/maska

13. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express.
14. Skanowanie i oczyszczanie poczty przychodzącej POP3 "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
15. Automatyczna integracja skanera POP3 z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
16. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.
17. Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. Dodatkowo zdefiniowane są grupy stron przez producenta.

18. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
19. Możliwość definiowania czy pliki z kwarantanny mają być przesyłane do producenta i co jaki czas ma się ta czynność odbywać.
20. Program umożliwia skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS.
21. Program skanuje ruch HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.
22. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program będzie pytał o hasło.
23. Po kliknięciu prawym klawiszem myszy na ikonie programu i wybraniu opcji : O programie" możliwość zdefiniowania przez administratora danych do pomocy technicznej jak: adres strony pomocy, adres e-mail do administratora ochrony, numer telefonu do administratora ochrony.
24. W GUI programu na punkcie końcowym możliwość wyświetlenia aktualnej wersji produktu i aktualnej wersji silników.
25. W GUI programu możliwość wyświetlenia kiedy była przeprowadzana ostatnia aktualizacja z dokładnością co do dnia i sekundy jej uruchomienia.
26. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń.
27. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.
28. Praca programu musi być niezauważalna dla użytkownika.
29. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania bezpośrednio na stacji roboczej.
30. Stacje robocze mogą łączyć się do serwera administracyjnego za pośrednictwem sieci Internet.
31. Oprogramowanie klienckie posiada wbudowana funkcje do komunikacji z serwerem administracyjnym, ale nie dopuszcza się osobnego agenta instalowanego na stacji roboczej.
32. Możliwość odblokowania ustawień programu po wpisaniu hasła.
33. Oprogramowanie posiada możliwość odblokowania ustawień lokalnych konfiguracji po doinstalowaniu odpowiedniego modułu.
34. Wbudowany moduł kontroli urządzeń (możliwość blokowania całkowitego dostępu do urządzeń, podłączenia tylko do odczytu i w zależności do jakiego interfejsu w komputerze zostanie podłączone urządzenie).
35. Możliwość dodania zaufanych urządzeń bezpośrednio z konsoli administracyjnej, na podstawie wykrytych urządzeń lub wpisanych ręcznie ID urządzenia lub ID produktu.
36. Funkcja Ochrony danych umożliwia blokowanie wysyłanych przez http lub smtp jak: (adresy e-mail, Piny, Konta bankowe, hasła itp.
37. Funkcja Ochrony danych konfigurowana zdalnie przez administratora.
38. Jedna wersja instalacyjna na stacje robocze i serwery plików Windows.

39. Wbudowana zapora osobista, umożliwiająca tworzenie reguł na podstawie aplikacji oraz ruchu sieciowego.
40. Wbudowany IDS
41. Możliwość zainstalowania silnika pełnego, lekkiego ze sprawdzaniem reputacji plików w chmurze, lub wykorzystanie dodatkowej maszyny wirtualnej która przejmie rolę silnika skanującego.
42. Maszyna która przejmuję rolę silnika skanującego musi działać w trybach redundancji lub równej dystrybucji.
43. Aktualizacja maszyny skanującej musi obejmować oddzielną aktualizację nowych funkcji, ulepszeń, poprawek oraz oddzielną aktualizację systemu operacyjnego urządzenia wirtualnego.
44. Możliwość tworzenia list sieci zaufanych.
45. Możliwość dezaktywacji funkcji zapory sieciowej.
46. Możliwość ustawienie skanowania z niskim priorytetem zmniejszając obciążenie systemu w trakcie wykonywania tego procesu.
47. Dodatkowa funkcja ochrony przeciwko znanym zagrożeniom typu ransomware.
48. Mechanizm który wspiera powrót do ostatnich działających wersji produktu oraz sygnatur w przypadku wdrożenia wadliwej aktualizacji.
49. Użytkownik na punkcie końcowym ma możliwość opóźnienia restartu potrzebnego do zakończenia jednego lub wielu zadań (konfigurowalne w politykach bezpieczeństwa)
50. Automatyczne zezwolenie na dostęp dla użytkowników Active Directory z grupy security groups
51. Wymuszenie połączenia szyfrowanego dla punktów końcowych Windows oraz Linux do serwera zarządzającego.
52. System zarządzania ryzykiem– Zintegrowany z konsolą zarządzającą system który pozwala oszacować podatność środowiska na atak na podstawie punktów ryzyka. Punkty ryzyka powinny być przydzielane od 0 do 100 gdzie liczba mniejsza stanowi mniejsze ryzyko a liczba większa większe ryzyko. System ponadto musi posiadać:
    a) Funkcję która pozwala wykrywać błędne konfiguracje oraz naprawiać je lub ignorować z podziałem na typ błędnej konfiguracji:

        -Ochrony przeglądarki internetowej

        -Sieć i poświadczenia

        -Błędna konfiguracja systemu operacyjnego

        System ponadto musi określać nasilenie tych błędnych konfiguracji w oparciu o punkty procentowe.

    b) System zarządzania ryzykiem który powinien wykrywać luki w aplikacjach podając przy tym numer CVE tych luk.

    c) System który pozwala na śledzenie i wykrywanie niezwyczajnych działań jakie podejmuje użytkownik na punkcie końcowym wraz z poinformowaniem ilu użytkowników takie działanie dotyczy oraz jakie jest jego nasilenie.

d) System pozwala na skanowanie punktów końcowych pod kątem wykrywania ryzyka na podstawie harmonogramu lub pojedynczo utworzonego zadania.

e) System pozwala na raportowanie na ilu urządzeniach wykryto błędną konfigurację i luki w aplikacjach oraz jaka jest ilość takich podatności i ich nasilenie wyrażone w procentach.

f) System pozwala na raportowanie u ilu użytkowników wykryto podejrzane działania oraz jakie jest ich nasilenie

53. Wbudowana ochrona przed exploitami wyposażona w minimum 15 różnych technik wykrycia exploitów z możliwością włączenia lub wyłączenia każdej z nich oraz dająca możliwość dodania własnych procesów. Funkcja umożliwia również:

a) Możliwość wymuszenia funkcji DEP systemu Windows

b) Możliwość wymuszenia relokacji modułów (ASLR)

Uwaga: Ta warstwa zabezpieczeń dotyczy systemów opartych na systemie Windows.

54. Ochrona przed atakami sieciowymi – Mechanizm obronny przed atakującymi próbującymi uzyskać dostęp do systemu poprzez wykorzystanie luk w sieci. Funkcja ta musi obejmować ochroną przed technikami takimi jak:

-Wczesny dostęp

-Dostęp do poświadczeń

-Wykrycie

-Crimeware

55. Ochrona przed ransomware - możliwość wykrywania i blokowania ataków typu ransomware niezależnie od tego czy atak został przeprowadzony lokalnie lub zdalnie na punkcie końcowym oraz utworzenie kopii zapasowej plików a w przypadku ataku odzyskanie i przywrócenie ich do pierwotnej lokalizacji.

Formaty plików jakie mogą być odzyskane:

3fr|ai|arw|bay|cab|cdr|cer|cr2|crt|crw|dcr|der|dgn|dll|dng|doc|docm|docx|dwg|dxf|dxg|eps|erf|exe|indd|ini|jpe|jpeg|jpg|mdf|mef|mrw|msg|msi|nef|nrw|odb|odc|odm|odp|ods|odt|orf|p12|p7b|p7c|pdd|pdf|pef|pem|pfx|png|ppt|pptm|pptx|psd|pst|ptx|py|r3d|raf|rtf|rw2|rwl|sr2|srf|srw|tsf|wb2|wpd|wps|x3f|xlk|xls|xlsb|xlsm|xlsx|xml|

Oprogramowanie daje możliwość odzyskania plików na żądanie lub automatycznego odzyskiwania.

56. Ochrona proaktywna oparta o maszynowe uczenie która działa w fazie poprzedzającej wykonanie, ochrona ta musi wy wykrywać zagrożenia takie jak:

a) Ukierunkowane ataki

b) Podejrzane pliki i ruch w sieci

c) Exploity

d) Ransomware

e) Grayware

57. Moduł ochrony proaktywnej musi posiadać oddzielne działania jakie będzie podejmował dla plików i oddzielne dla ruchu sieciowego

58. Moduł ochrony proaktywnej musi działać w trybach które administrator może dowolnie zmieniać na:

a) Tolerancyjny

b) Normalny

c) Agresywny

59. Zintegrowany sandbox po stronie producenta który pozwala na analizę pliku

a) Plik może zostać wysłany automatycznie ze stacji roboczej jeżeli oprogramowanie uzna go za podejrzany lub ręcznie z poziomu konsoli przez administratora

b) Możliwość przesłania archiwum zabezpieczonego hasłem

c) Możliwość przesłania adresu URL

d) W przypadku przesłania wielu plików jednorazowo, możliwość detonacji próbek pojedynczo.

60. Wbudowany sandbox musi działać w trybie monitorowania i blokowania

61. Wbudowany sandbox musi oferować działania naprawcze takie jak dezynfekcja lub przeniesienie do kwarantanny

62. Wbudowany sandbox musi oferować opcję wstępnego filtrowania zawartości która skanuje pliki, argumenty wiersza poleceń i adresy URL pod kątem podejrzanego zachowania.

63. Wbudowany sandbox musi posiadać opcję która pozwala na dodanie określonych rozszerzeń do wyjątków, pliki z tym rozszerzeniem nie zostaną przesłane do sandboxa.

64. Minimalny rozmiar pliku jaki może zostać przesłany do sandboxa to 1KB

65. Maksymalny rozmiar pliku jaki może zostać przesłany do sandboxa to 50MB.

66. Telemetria - Możliwość przesyłania nieprzetworzonych danych bezpieczeństwa z punktów końcowych z systemem operacyjnym Windows do SIEM Splunk (wymaga TLS 1.2 lub wyższy).

67. Oprogramowanie pozwala na skanowanie punktów końcowych pod kątem wyszukiwania wskaźników zagrożeń, wskaźniki te obejmują:

a) Maszyny Wirtualne
b) Stacje robocze i serwery Windows
c) Ochrona Exchange

4.Licencje Oprogramowania serwerowego

Oprogramowanie

- Microsoft Windows Server CAL 2022 Device CSP – 5szt.
- Microsoft Windows Server Standard 2022 CSP, (16 core) – 1szt.
- Microsoft Windows Serwer CAL 2022 CSP– 20szt.

lub oprogramowanie równoważne.

Opis kryteriów równoważności oprogramowania licencyjnego:

1. Współpraca z procesorami o architekturze x64.
2. Instalacja i użytkowanie aplikacji 32-bit. i 64-bit. na dostarczonym systemie operacyjnym.
3. Możliwość budowania klastrów składających się z 64 węzłów.
4. Pojedyncza licencja musi obsłużyć serwer fizyczny wyposażony w 2 procesory oraz 16 rdzeni.
5. Praca w roli klienta domeny Microsoft Active Directory.
6. Możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie MicrosoftWindows Server 2022.
7. Możliwość federowania klastrów typu failover w zespół klastrów (Cluster Set) z możliwością przenoszenia maszyn wirtualnych wewnątrz zespołu.
8. Możliwość uruchomienia roli klienta i serwera czasu (NTP).
9. Możliwość uruchomienia roli serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory.
10. Możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory
11. Możliwość uruchomienia roli serwera stron WWW.
12. W ramach dostarczonej licencji zawarte prawo do użytkowania i dostęp do oprogramowania oferowanego przez producenta systemu operacyjnego umożliwiającego wirtualizowanie zasobów sprzętowych serwera.
13. W ramach dostarczonej licencji zawarte prawo do instalacji i użytkowania systemu operacyjnego na co najmniej dwóch maszynach wirtualnych.
14. W ramach dostarczonej licencji zawarte prawo do pobierania poprawek systemu operacyjnego.
15. Wszystkie wymienione parametry, role, funkcje, itp. systemu operacyjnego objęte są dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów).
16. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
17. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
18. Wbudowane wsparcie instalacji i pracy na wolumenach, które:
    a. pozwalają na zmianę rozmiaru w czasie pracy systemu,
    b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
    c. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
    d. umożliwiają zdefiniowanie list kontroli dostępu (ACL).

19. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość
20. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
21. Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET
22. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
23. Możliwość wykorzystania standardu http/2.
24. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
25. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
    a. klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
    b. dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.
26. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
27. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
28. Mechanizmy logowania w oparciu o:
    a. login i hasło,
    b. karty z certyfikatami (smartcard),
    c. wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM).
29. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla:
    a. określonych grup użytkowników,
    b. zastosowanej klasyfikacji danych,
    c. centralnych polityk dostępu w sieci,
    d. centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.
30. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
31. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
32. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
33. Dostępny, pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
34. Wsparcie dla środowisk Java i .NET Framework 4.x i wyższych – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
35. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
    a. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC.
    b. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
        - Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
        - Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,

- Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
- Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.

c. Zdalna dystrybucja oprogramowania na stacje robocze.
d. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej z możliwością dostępu minimum 65 tys. Użytkowników.
e. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:

- Dystrybucję certyfikatów poprzez http,
- Konsolidację CA dla wielu lasów domeny,
- Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
- Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509

f. Szyfrowanie plików i folderów.
g. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec)
h. Szyfrowanie sieci wirtualnych pomiędzy maszynami wirtualnymi
i. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
j. Serwis udostępniania stron WWW
k. Wsparcie dla protokołu IP w wersji 6 (IPv6).
l. Wsparcie dla algorytmów Suite B (RFC 4869).
m. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows.
n. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych.
o. Możliwość migracji maszyn wirtualnych między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
p. Możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności.
q. Mechanizmy wirtualizacji mające wsparcie dla:

- Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
- Obsługi ramek typu jumbo frames dla maszyn wirtualnych.
- Obsługi 4-KB sektorów dysków,
- Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra,
- Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.
- Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)
- Możliwość tworzenia wirtualnych maszyn chronionych, separowanych od środowiska systemu operacyjnego.

a. Możliwość uruchamiania kontenerów bazujących na Windows i Linux na tym samym hoście kontenerów.
b. Wsparcie dla rozwiązania Kubernetes.
c. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
d. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
e. Mechanizmy deduplikacji i kompresji na wolumenach do 64 TB.
f. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
g. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
h. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF
i. Mechanizm konfiguracji połączenia VPN do platformy Azure.
j. Wbudowany mechanizm wykrywania ataków na poziomie pamięci RAM i jądra systemu.
k. Mechanizmy pozwalające na blokadę dostępu nieznanych procesów do chronionych katalogów.
l. Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.
m. Możliwość instalacji i poprawnej pracy Systemu Bazodanowego (Microsoft SQL Server Enterprise).

36. W przypadku zaproponowania licencji równoważnych Wykonawca przeprowadzi na własny koszt instalację, konfigurację i integrację dostarczonego produktu. Wykonawca przeprowadzi migrację wszelkich danych i konfiguracji zapewniając identyczne funkcjonowanie całego środowiska w stosunku do aktualnego środowiska. Przerwa w działaniu aktualnie eksploatowanego środowiska produkcyjnego nie może wynieść więcej niż 7 godzin Dodatkowo w przypadku błędnego działania środowiska po instalacji licencji równoważnych Wykonawca zobowiązany będzie na własny koszt przywrócić środowisko do stanu poprawnego funkcjonowania, a w przypadku braku takiej możliwości do stanu pierwotnego oraz dostarczenia innego rozwiązania spełniającego wymagania OPZ.
37. Ponadto zastosowanie rozwiązania równoważnego nie może ograniczyć funkcjonalności posiadanego systemu przez Zamawiającego i nie może powodować konieczności ponoszenia dodatkowych kosztów dla Zamawiającego.

5. Wdrożenie

Przedmiotem niniejszego postępowania jest:

1. Montaż i przygotowanie NAS do działania w trybie zwirtualizowanego środowiska.
2. Przygotowanie scenariusza wirtualizacji środowiska, na którym docelowo ma pracować utworzony klaster w trybie zwirtualizowanym jako rozwiązanie klastrowe z uwzględnieniem usług obecnie wdrożonych u Zamawiającego - w ramach przygotowania tego scenariusza należy wykonać audyt obecnego środowiska pracy maszyn serwerowych z uwzględnieniem maszyn fizycznych i maszyn zwirtualizowanych, czego wynikiem ma być powstały scenariusz w terminie 7 dni.
3. Wdrożenie kontrolera domeny (szczegółowy opis w **Załączniku nr 1**)
4. Montaż i konfiguracja switcha do poprawnej obsługi kontrolera domeny.
5. Konfiguracja switchy w trybie wysokiej dostępności sieci.
6. Zakres prac wdrożeniowych w kolejności wykonania (szczegółowy opis w **Załączniku nr 2**)

7. Wykonanie dokumentacji powykonawczej.

Infrastruktura techniczna Systemu

Wykonawca zobowiązany jest do skonfigurowania i uruchomienia wybranych elementów infrastruktury technicznej, aby wypełnić wymagania postawione przed Systemem (Koncepcja wdrożenia).

Na potrzeby Systemu przewiduje się zastosowanie serwera fizycznego, NAS i przełącznika sieciowego oraz wykonaniem usługi konfiguracji środowiska wirtualnego opartego o wymagany hypervisor (wirtualizator).

Jeżeli do osiągnięcia wszystkich zakładanych celów wdrożenia Systemu (funkcjonalnych, wydajnościowych, niezawodności) niezbędne okaże się zastosowanie również jakichś innych elementów infrastruktury technicznej, to Wykonawca zobowiązany jest do niezwłocznego powiadomienia o tym fakcie Zamawiającego.

Załącznik nr 1

Wdrożenie kontrolera domeny Active Directory z usługami:

Część 1 - Założenia

W ramach wdrożenia zostanie przeprowadzona instalacja i wdrożenie kontrolera domenyumożliwiającego centralne zarządzanie istniejącą liczbą użytkowników, urządzeń, możliwymi dostępami oraz przede wszystkim bezpieczeństwem.

Do wdrożenia Active Directory w pełnym zakresie funkcjonalności wykorzystane zostanąstacje robocze z zainstalowanym systemem operacyjnym Windows w wersji Professional lub Enterprise.

Część 2 - Plan wdrożenia

Prace na serwerze:

- instalacja na serwerze usługi AD;
- konfiguracja DNS;
- przygotowanie - logiczny wygląd drzewa;
- wdrożenie - fizycznie las.

Prace na stacjach roboczych:

- migracja profili użytkownika z sieci lokalnej;
- dodanie stacji roboczych do AD;
- konfiguracja użytkowników.

Załącznik nr. 2

Zakres prac wdrożeniowych w kolejności wykonania

W ramach prac wdrożeniowych przeprowadzone zostaną następujące czynności:

- projekt realizacyjny:
    - analiza przedwdrożeniowa;
    - szczegółowa koncepcja wdrożenia;
- akceptacja koncepcji wdrożenia przez Zamawiającego;
- przygotowanie środowiska zgodnie z dokumentacją projektową:
    - konfiguracja NAS i serwera w oparciu o hypervisor;
    - przygotowanie scenariusza migracji;
- migracja środowiska wirtualnego:
    - realizacja scenariusza migracji;
    - migracja wirtualnych maszyn Zamawiającego;
    - weryfikacja poprawności migracji;
- dokumentacja powdrożeniowa wraz ze schematem połączeń;
- odbiór prac przez Zamawiającego.