Głogów Małopolski, data 21 października 2024 r.

Dotyczy postępowania pod nazwą „Zakup urządzeń i oprogramowania” w ramach projektu Poprawa cyberbezpieczeństwa w Gminie Głogów Młp” dofinansowanego w formie grantu z programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. Wzmocnienie krajowego systemu cyberbezpieczeństwa

Ogłoszenie o zamówieniu zostało opublikowane w Dzienniku Urzędowym Unii Europejskiej pod numerem OJ S 201/2024 15/10/2024

**Zmiana treści SWZ**

Zgodnie z art. 137 ust. 1 ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych (Dz.U. poz. 2019 ze zm.), zwanej dalej „p.z.p.”, zamawiający zmienia treść SWZ w następującym zakresie:

1. załącznik nr 1 do SWZ Rozdział 5.10 System NAS **zmienia się na:**

## System NAS – szt.1 – wymagania minimalne

|  |
| --- |
| 1. Dostarczone urządzenie musi posiadać, co najmniej 10 TB powierzchni netto przeznaczonej na przechowywanie unikalnych segmentów danych (backupów). Urządzenie powinno umożliwiać rozbudowę powierzchni do co najmniej 32 TB netto - powyższa wartość musi być możliwa do rozbudowania w ramach dostarczanego appliance sprzętowego z użyciem licencji programowej tzn. bez konieczności wymiany lub zakupu dodatkowych elementów sprzętowych. Niedopuszczalne jest użycie innych narzędzi, bramek czy tierowania do chmury w celu zwiększenia pojemności. Nie dopuszcza się konieczności dodawania przestrzeni poprzez fizycznych dysków – rozbudowa ma się odbywać jedynie na drodze dodawania licencji.
2. Technologia de-duplikacji musi wykorzystywać algorytm bazujący na zmiennym, dynamicznym bloku danych. Algorytm ten musi samoczynnie i automatycznie dopasowywać się do otrzymywanego strumienia danych. Oznacza to, że urządzenie musi dzielić otrzymany pojedynczy strumień danych na bloki o różnej długości. De-duplikacja zmiennym blokiem musi być wykonywana dla wszystkich danych bez względu na to jakim protokołem czy interfejsem dostępowym zostały dostarczone.
3. Unikalne bloki przed zapisaniem na dysk muszą być dodatkowo kompresowane.
4. Zdeduplikowane i skompresowane dane przechowywane w obrębie podsystemu dyskowego urządzenia muszą być chronione za pomocą technologii RAID 6 lub równoważnej
5. Proces de-duplikacji powinien odbywać się in-line – w pamięci urządzenia, przed zapisem danych na nośnik dyskowy. Zapisowi na system dyskowy muszą podlegać tylko unikalne bloki danych nie znajdujące się jeszcze w systemie dyskowym urządzenia.
6. Urządzenie musi posiadać nadmiarowe zasilanie i chłodzenie
7. Kontroler modułu musi posiadać minimum 2 procesory
8. Urządzenie musi wspierać technologię zapewniającą niezmienność składowanych danych (Niezmienny Snapshot lub Soft-WORM)
9. Jako interfejsy do przyjmowania danych backupowych, oferowane urządzenie musi posiadać:
10. 4 porty 10GbE SFP+, 4 porty 1 GbE
11. Urządzenie musi posiadać możliwość rozbudowy 12 dodatkowych portów 10/25 GbE.
12. Oferowany produkt musi posiadać wsparcie dla minimum następujących protokołów dostępowych:
	1. CIFS, NFS
	2. OST, RMAN SBT API,
	3. VDMS

jeśli wsparcie któregoś z protokołów wymaga dodatkowych licencji lub zasobów sprzętowych należy je uwzględnić w ofercie. 1. Urządzenie musi umożliwiać składowanie danych poprzez udostępnianie minimum 128 zasobów NAS w sieci Ethernet wykorzystując protokoły CIFS, NFS.

Musi być zapewniona jednoczesna obsługa dostępu protokołem CIFS i NFS dla tego samego udziału.1. Wymagane jest dostarczenie licencji, pozwalającej na obsługę protokołów CIFS, NFS, de-duplikacji na źródle. Licencje muszą być dostarczone na całe urządzenie i do pełnej pojemności urządzenia.
2. Oferowane urządzenie musi wspierać, co najmniej następujące aplikacje Micro Focus Data Protector, Veritas NetBackup oraz Backup Exec, Dell Networker, Atempo Time Navigator, Veeam, Acronis (Cyber Protect), Arcserve, Bacula Enterprise.
3. W przypadku współpracy z aplikacją Oracle RMAN, urządzenie musi umożliwiać de-duplikację na źródle (de-duplikację po stronie media serwera). Deduplikacja taka musi zapewniać by z serwerów do urządzenia były transmitowane tylko fragmenty danych nie znajdujące się dotychczas na urządzeniu.
4. Oferowany produkt musi umożliwiać replikację danych realizowaną między urządzeniami tej samej rodziny w układzie. Replikacja powinna umożliwiać szyfrowanie przesyłanych unikalnych (zdeduplikowanych) danych - długość klucza minimum 256-bit.
5. Replikacja musi być możliwa w trybie co najmniej:
	1. 1:1
	2. 1:2
	3. 2:1
	4. Wiele do wielu.
6. Całe rozwiązanie musi być objęte 36 miesięcznym okresem gwarancji z naprawą miejscu instalacji urządzenia i z gwarantowaną wizytą technika do końca następnego dnia roboczego od dnia zgłoszenia awarii do organizacji serwisowej. Uszkodzone dyski twarde nie podlegają zwrotowi organizacji serwisowej. Serwis gwarancyjny musi obejmować dostęp do poprawek i nowych wersji oprogramowania. Urządzenie musi posiadać posiad pojedynczy punkt kontaktu w przypadku każdego rodzaju problemów tj.: sprzętowych, z oprogramowaniem do przechowywania backupu oraz z systemem operacyjnym.
 |

1. załącznik nr 1 do SWZ Rozdział 5.11 „Instalacja, konfiguracja, wdrożenie” w zakresie podrozdziału „Rekonfiguracja elementów bezpieczeństwa sieciowego” zmienia się na:

## Instalacja, konfiguracja, wdrożenie – szt.1 – wymagania minimalne

|  |
| --- |
| Usługi informatyczne w zakresie wdrożenia, konserwacji i serwisu sprzętu informatycznego oraz oprogramowania. |
|  | **Usługi** | Celem prac jest przygotowanie środowiska teleinformatycznego, na potrzeby realizacji elementów cyberbezpieczeństwa, zbudowanego w oparciu o dostarczone urządzenia sprzętowe i oprogramowanie opisane w podmiotowym dokumencie.Część sprzętowa powinna zostać oparta na systemie wirtualizacji zasobów IT. Zamawiający umożliwi Wykonawcy dostęp do infrastruktury w ustalonym wcześniej terminie w celu dokonania analizy i przygotowania procedur wdrożenia, migracji do nowego środowiska. Dostęp do infrastruktury będzie możliwy pod nadzorem Zamawiającego i po spełnieniu warunków wynikających z Polityki Bezpieczeństwa i wymagań Zamawiającego.Zamawiający udzieli Wykonawcy wszelkich niezbędnych informacji niezbędnych do przeprowadzenia wdrożenia.**W ramach oferty Zamawiający wymaga przeprowadzenia wdrożenia na zasadach projektowych z pełną dokumentacją wdrożeniową**. Zamawiający wymaga następującego zakresu usług realizowanego w porozumieniu z Zamawiającym:* 1. Sporządzenia Planu Wdrożenia uwzględniającego fakt wykonania wdrożenia bez przerywania bieżącej działalności Zamawiającego oraz przewidującego rozwiązania dla sytuacji kryzysowych wdrożenia.
	2. Sporządzenia Dokumentacji Systemu według której nastąpi realizacja. Dokumentacja Systemu musi być uzgodniona z Zamawiającym i zawierać wszystkie aspekty wdrożenia. W szczególności:
		1. koncepcję techniczną projektu, która powinna zawierać opis mechanizmów działania systemu z wykorzystaniem dostarczonych i rozbudowywanych elementów sprzętowych.
		2. schematy połączeń
		3. mechanizmy działania głównych elementów sprzętowych:
* sieć LAN - przełączniki sieciowe
* klaster wirtualizacyjny
* system backupu i archiwizacji danych
* system serwerowy
* system macierzowy
	+ 1. iii. mechanizmy działania głównych elementów programowych:
* system NAC
* system EDR
* system zarzadzania siecią i jednostkami końcowymi.
	+ 1. testy systemu uwzględniające sprawdzenie wymaganych niniejszą specyfikacją funkcjonalności
		2. sposób odbioru uzgodniony z Zamawiającym
		3. listę i opisy procedur, wypełnianie których gwarantuje Zamawiającemu prawidłowe działanie systemu
		4. opis przypadków, w których projekt dopuszcza niedziałanie systemu
		5. realizacja wdrożenia nastąpi według Planu Wdrożenia po zakończeniu którego Wykonawca sporządzi Dokumentację Powykonawczą

Odbiór wdrożenia nastąpi na podstawie zgodności stanu faktycznego z Planem Wdrożenia. |
|  | **Montaż i fizyczne uruchomienie systemu** | **Zamawiający wymaga, aby Wykonawca zainstalował całości dostarczonego rozwiązania w pomieszczeniu serwerowni, jak i innych wskazanych miejscach co najmniej w zakresie:**1. Wniesienie, ustawienie i fizyczny montaż wszystkich dostarczonych urządzeń w szafach rack w pomieszczeniach (miejscach) wskazanych przez Zamawiającego z uwzględnieniem wszystkich lokalizacji.
2. Rozbudowa istniejących zasobów sprzętowych.
3. Urządzenia, które nie są montowane w szafach teleinformatycznych, powinny zostać zamontowane w miejscach wskazanych przez Zamawiającego, oraz skonfigurowane i dołączone do infrastruktury Zamawiającego.
4. Usunięcie opakowań i innych zbędnych pozostałości po procesie instalacji urządzeń.
5. Podłączenie całości rozwiązania do infrastruktury Zamawiającego.
6. Wykonanie procedury aktualizacji firmware dostarczonych elementów do najnowszej wersji oferowanej przez producenta sprzętu.
7. Dla urządzeń modularnych wymagany jest montaż i instalacja wszystkich podzespołów.
8. Wykonanie połączeń kablowych pomiędzy dostarczonymi urządzeniami w celu zapewnienia komunikacji – Wykonawca musi zapewnić niezbędne okablowanie (np.: patchordy miedziane min. kat. 6 UTP lub światłowodowe uwzględniające typ i model interfejsu w urządzeniu sieciowym).
9. Wykonawca musi zapewnić niezbędne okablowanie potrzebne do podłączenia urządzeń aktywnych do sieci elektrycznej (np.: listwy zasilające).
10. Wykonawca musi zapewnić niezbędne wkładki dla dostarczonych urządzeń np.: SFP, SFP+ miedzy innymi celem:
	1. Stworzenia połączeń sieci LAN pomiędzy przełącznikami.
	2. Podłączenia urządzeń serwerowo-macierzowych (serwery, macierze) do przełączników sieci LAN.
	3. Połączenia powinny być zrealizowane z zachowaniem redundancji i agregacji połączeń na poziomie co najmniej n+1.
	4. Połączenia musza wykorzystywać dostępną, największą przepustowość portu pomiędzy łączonymi urządzeniami.
 |
|  | **Instalacja i konfiguracja oprogramowania** | 1. Instalacja i konfiguracja dostarczonego oprogramowania do wirtualizacji wraz z wykreowaniem odpowiedniej liczby wirtualnych maszyn na potrzeby tworzonego rozwiązania IT z zachowaniem zgodności z ilością dostarczonych licencji.
2. Instalacja i konfiguracja oprogramowania do systemu wykonywania backupu i archiwizacji danych działającego na serwerze backupu.
3. Instalacja dostarczonego oprogramowania systemu serwerowego wraz z niezbędnymi usługami oraz instalacja wszystkich niezbędnych kodów dostępowych oraz licencji (wszelkie procedury rejestracyjne powinno zostać wykonane na danych dostarczonych przez Zamawiającego).
4. Instalacja i konfiguracja dostarczonych systemów operacyjnych dla serwerów wirtualnych.
5. Instalacja i konfiguracja oprogramowania EDR.
6. Instalacja i konfiguracja oprogramowania NAC.
7. Instalacja i konfiguracja systemu do zarzadzania siecią i jednostkami końcowymi.
 |
|  | **Konfiguracja przełączników/sieci LAN:** | Zamawiający wymaga stworzenia połączeń sieciowych pomiędzy wszystkimi lokalizacjami występującymi w projekcie według topologii gwiazdy. Centralnym punktem będzie serwerownia zlokalizowana w Urzędzie.Dostarczone przełączniki urządzaniami będą stanowiły centralny punkt wymiany danych sieciowych z punktu widzenia warstwy drugiej modelu ISO/OSI – L2 (warstwa łącza danych) oraz zapewnią wsparcie dla protokołu STP (protokół drzewa rozpinającego).Konfiguracja przełączników w zakresie:* 1. Przeprowadzenie audytu obecnej topologii oraz konfiguracji.
	2. Aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta urządzenia.
	3. Stworzenia odpowiednich konfiguracji STACK z wykorzystaniem dedykowanych modułów.
	4. Konfiguracja sieci wirtualnych VLAN – taka liczba sieci wirtualnych aby odseparować różne typy ruchu (ilość sieci VLAN należy określić w uzgodnieniu z Zamawiającym).
	5. Wymagane jest wydzielenie i skonfigurowanie co najmniej stref:
* SERWERY
* UŻYTKOWNICY WEWNĘTRZNI
* UŻYTKOWNICY ZEWNĘTRZNI
* MANAGEMENT
	1. Jeśli jest to konieczne – Zamawiający oczekuje rekonfiguracji adresacji IP w danych strefach (readresacja urządzeń, serwerów, komputerów leży po stronie Wykonawcy)
	2. Zamawiający wymaga skonfigurowania polityk ruchu pomiędzy strefami na urządzeniach firewall.
	3. Konfiguracja połączeń pomiędzy przełącznikami sieci LAN.
		1. Rozpięcie połączeń przełączników IDF na centralne przełączniki CORE z zachowaniem nadmiarowości z wykorzystaniem wszystkich dostępnych portów uplink.
		2. Z wykorzystaniem połączeń światłowodowych oraz miedzianych.
		3. Agregacja połączeń celem uzyskania pasma nx10Gbps w obu kierunkach ruchu.
		4. Należy wykorzystać wkładki o najwyższej możliwej przepustowości dla danego połączenia np.: dla portu o możliwej przepustowości 1/10Gbs (wkładka: SFP/SFP+), należy wykorzystać wkładki SFP+ o przepustowości 10Gbps.
	4. Konfiguracja sieci VLAN na wszystkich przełącznikach – konfiguracja propagacji sieci VLAN.
	5. Konfiguracja routingu pomiędzy sieciami VLAN na centralnym urządzeniu firewall - klaster;
	6. Zamawiający wymaga aby wszystkie sieci VLAN (L2) zostały rozpięte na warstwie L2 na urządzeniu firewall – (połączenie TRUNK).
	7. Zamawiający wymaga skonfigurowania mechanizmów bezpieczeństwa na dostarczonych przełącznikach LAN co najmniej w zakresie:
* Konfiguracja mechanizmów DHCP Snooping
* Konfiguracja mechanizmów Dynamic ARP Inspection
* Konfiguracja mechanizmów Port Security na wskazanych portach przełączników
* Konfiguracja mechanizmów 802.1x na wskazanych portach przełączników w oparciu o certyfikaty komputerów (konfiguracja Centrum Certyfikacji oraz polityk leży po stronie Wykonawcy) z wykorzystaniem dostarczonego oprogramowania NAC.
	1. Ustawienie serwera czasu dla urządzeń sieci LAN – przełączników sieciowych - na klaster firewall.
	2. Zamawiający wymaga instalacji i konfiguracji serwera logów dla urządzeń sieci LAN (maszyna wirtualna) – przełączników sieciowych, z graficznym interfejsem przeszukiwania. Zamawiający dopuszcza rozwiązania Open Source.
	3. Zamawiający wymaga instalacji i konfiguracji dedykowanego serwera monitorowania pracy urządzeń sieciowych z graficznym interfejsem przeszukiwania (maszyna wirtualna): przełączniki sieciowe, drukarki, UTM. Zamawiający dopuszcza rozwiązania Open Source.
	4. Wykonawcza skonfiguruje urządzenia aby raportowały, przesyłały dane do zainstalowanego serwera logów i monitorowania sieci.
	5. Testowanie obsługi ruchu sieciowego.
	6. Testowanie skuteczności zabezpieczeń.
 |
|  | **Rekonfiguracja elementów bezpieczeństwa sieciowego.**  | Modernizacja konfiguracji istniejących UTM (Fortigate) dla nowych urządzeń w zakresie.1. Aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta urządzenia.
2. Przygotowanie projektu włączenia nowych urządzenia do sieci LAN urzędu.
3. Re/Konfiguracja systemów Firewall:
	1. Konfiguracja podstawowych parametrów
	2. Konfiguracja translacji adresów NAT
	3. Konfiguracja mechanizmów ochrony wybranych sieci VLAN, do których przyłączone zostaną np. serwery, macierze, itp.
	4. Konfiguracja inspekcji określonych protokołów sieciowych;
	5. Konfiguracja reguł dostępu do określonych podsieci, chronionych przez moduł Firewall;
	6. Konfiguracja zarządzania Firewall przez dedykowaną stację zarządzającą bezpieczeństwem sieciowym;
	7. Testowanie działania bramy
4. Konfiguracja modułów należących do systemu wykrywania włamań IPS:
	1. Konfiguracja podstawowych parametrów
	2. Konfiguracja mechanizmów ochrony określonych sieci VLAN przez moduł wykrywania włamań;
	3. Konfiguracja reguł kontroli ruchu sieciowego przez moduły oraz sposobów reakcji na pojawienie się niepożądanego ruchu sieciowego;
	4. Konfiguracja zarządzania modułami przez dedykowaną stację zarządzającą bezpieczeństwem sieciowym;
	5. Testowanie działania ochrony IPS
5. Konfiguracja modułu ochrony antywirusowej, antyspyware, blokowania transferu plików, antyspamowa, filtrowania i blokowania odwołań do niepożądanych adresów URL.
	1. Przypisanie adresu IP do zarządzania.
	2. Konfiguracja inspekcji protokołów HTTP, HTTPS; SMTP, FTP, POP3
	3. Definicja reguł filtrowania/blokowania
	4. Integracja z systemem domenowym w celu weryfikacji nawiązywania połączenia poprzez nazwę użytkownika z domeny.
6. Konfiguracja tuneli SSL VPN celem zapewnienia bezpiecznego dostępu do sieci wewnętrznej.
7. Konfiguracja uwierzytelniania w oparciu o dostarczony moduł uwierzytelnienia.
8. Uruchomienie i skonfigurowanie dedykowanych oddzielnych instancji systemów bezpieczeństwa dla: dedykowanych, stworzonych na przelaniach sieci VLAN.
9. W miarę możliwości polityki dostępu powinny być budowane w oparciu o poświadczenia użytkowników (moduł uwierzytelnienia), nie zaś o adresy IP, czy MAC
10. W każdej instancji systemu bezpieczeństwa należy skonfigurować co najmniej 3 profile (wytyczne przekaże Zamawiający) dla każdej z poniższych funkcjonalności:
	1. kontrola dostępu - zapora ogniowa klasy Stateful Inspection
	2. ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS) umożliwiający skanowanie wszystkich rodzajów plików, w tym zip, rar
	3. ochrona przed atakami - Intrusion Prevention System [IPS/IDS]
	4. kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM.
	5. kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP)
	6. kontrola pasma oraz ruchu [QoS, Traffic shaping]
	7. Kontrola aplikacji oraz rozpoznawanie ruchu P2P
	8. Ochrona przed wyciekiem poufnej informacji (DLP)
	9. Filtra WWW (w oparciu o kategorie stron WWW oraz własną bazę URL)
	10. Inspekcja ruchu SSL
	11. Ochrony przez atakami na stacje klienckie
	12. Kontrola pasma
11. Konfiguracja szyfrowanych tuneli VPN (IPSec) pomiędzy lokalizacjami zdalnymi.
12. Konfiguracja logowania i raportowania.
 |
|  | **Serwery pod wirtualizację** | Zamawiający wymaga instalacji i konfiguracji dostarczonych serwerów celem stworzenia bazy sprzętowej dla klastra niezawodnościowego i wydajnościowego stworzonego na bazie dostarczonych serwerów i oprogramowania do wirtualizacji. |
|  | **Serwer backupu** | W ramach projektu przewiduje się wykorzystanie serwera backupu na miejsce przechowywanie backupu. Na serwerze należy zainstalować oprogramowanie do wirtualizacji – zarządzane z jednego centralnego miejsca, tego samego jak dla serwerów wirtualizacyjnych. System musi zostać podłączony do macierzy produkcyjnej, musie posiadać lokalne repozytoria danych na przestrzeni dyskowej, celem wykonywania backupu pełnych maszyn wirtualnych – przechowywanych na połowie zasobu dyskowego. Natomiast druga część zasobu musi zostać wykorzystana do wykonywania replikacji on-line maszyn wirtualnych na lokalna platformę wirtualizacyjną – na serwerze backupu. Takie podejście ma gwarantować zabezpieczenie kluczowych węzłów sieciowych (serwerów wirtualnych) na dwa sposoby tj. plik off-line maszyny wirtualnej oraz kopia on-line replikowania asynchronicznie według harmonogramu. Wykonywanie backupu musi być powiązane z procedurą sprawdzania poprawności jego wykonania oraz automatycznym raportowaniem do jednostki administracyjnej. Oprogramowanie backupu musi obsługiwać również bibliotekę taśmową i system NAS, gdzie będzie można skorzystać z replikacji danych – przesłania backupu dyskowego np.: na zasób taśmowy.Mechanizm podłączenia 1. Konfiguracja i podłączenie serwera backupu do zasobu dyskowego. Zamawiający wymaga takiego skonfigurowania dostępu do zasobu dyskowego, aby każdy wolumen dyskowy zasobu dyskowego był widziany przez każdy z serwerów wirtualizacyjnych poprzez wszystkie ścieżki (porty) udostępniane przez zasób dyskowy. Każdy wolumen dyskowy musi być dostępny dla każdego serwera wirtualizacyjnego w przypadku niedostępności (awarii) n-(n-1) ścieżek, gdzie n oznacza liczbę wszystkich dostępnych ścieżek (portów) udostępnianych przez zasób dyskowy.
2. Konfiguracja i podłączenie serwera backupu do sieci LAN Wnioskodawcy. Zamawiający wymaga, aby każdy z serwerów wirtualizacyjnych był podłączony do sieci LAN, co najmniej taką liczbą portów, by w przypadku niedostępności (awarii) n-(n-1) ścieżek, gdzie n oznacza liczbę wszystkich dostępnych ścieżek (portów) był zachowany dostęp do sieci LAN.
3. Konfiguracja sieci w infrastrukturze wirtualnej - konieczna jest konfiguracja wspierająca wirtualne sieci LAN w oparciu o protokół 802.1q.

Logiczny schemat rozbudowywanego systemu backup – stan docelowy. |
|  | **Macierz****dyskowa** | Macierz musi być wykorzystywana do gromadzenia i przechowywania „danych produkcyjnych” – wykorzystywanych przez oprogramowanie dziedzinowe. Musi zostać podłączona do środowiska wirtualizacyjnego (klaster serwerów).Ilość i wielkość udziałów dyskowych udostępnionych dla serwerów np.: wirtualizacyjnych zostanie ustalona z Zamawiającym na etapie analizy przedwdrożeniowej. |
|  | **Migracja danych** | Dotyczy przeniesienia obecnie wykorzystywanych i rozbudowywanych systemów informatycznych na nowe dostarczone rozwiązanie sprzętowe z wykorzystaniem wirtualizacji zasobów.Dane (systemy dziedzinowe) musza zostać przeniesione na nowe zasoby serwerowo-macierzowe. Zakres migracji zostanie ustalona z Zamawiającym na etapie analizy przedwdrożeniowej.Migracja danych musi uwzględniać uwspólnianie zasobów oraz weryfikacji ich poprawności i jakości technicznej min. w pełnym zakresie danych i rejestrów systemów dziedzinowych. |
|  | **Serwer SMTP** | Zamawiający wymaga zainstalowania oraz uruchomienia i skonfigurowania dedykowanego serwera SMTP. Serwer SMTP powinien być uruchomiony na dedykowanym wirtualnym serwerze pracującym pod kontrolą systemu Linux.Serwer SMTP będzie wykorzystywany na potrzeby wysyłania powiadomień systemowych między innymi z:* Urządzeń sieciowych
* Serwerów
* Macierzy dyskowej
* Systemu zarządzania kopiami zapasowymi
* Systemu wirtualizacji serwerów
* Aplikacji

Zamawiający wymaga zabezpieczenia serwera w taki sposób, aby uniemożliwić przesyłanie wiadomości z nieautoryzowanych źródeł. Zamawiający wymaga, aby wysyłane powiadomienia były poprawnie dostarczane na zewnętrzne konta email. |
|  | **Instalacja i konfiguracja serwera kopii zapasowych konfiguracji urządzeń sieciowych.** | 1. Zamawiający wymaga, aby wraz z uruchomieniem dostarczanych urządzeń sieciowych uruchomić serwer – repozytorium konfiguracji z dostarczanych urządzeń np.; przełączników sieciowych oraz innych urządzeń wspierających wykonywanie kopii zapasowych konfiguracji na zasób sieciowy.
2. Serwer musi być uruchomiony na dedykowanej maszynie (dopuszcza się maszynę wirtualną uruchomioną na infrastrukturze wirtualizującej Zamawiającego).
3. Serwer może działać w oparciu o dowolny system operacyjny, Zamawiający powinien uwzględnić cenę licencji w ofercie i dostarczyć ją we własnym zakresie.
4. Serwer może działać w oparciu o dowolne oprogramowanie bądź rozwiązanie autorskie Wykonawcy. Jeżeli takowa jest potrzebna, Zamawiający wymaga dostarczenia licencji. Cena licencji powinna być wliczona w cenę oferty.
 |
|  | **Uruchomienie środowiska wirtualizacyjnego.** | Zamawiający wymaga zaplanowania, uruchomienia oraz przetestowania środowiska wirtualizacyjnego, co najmniej w zakresie:1. Aktywacja licencji oprogramowania wirtualizacyjnego na stronie producenta.
2. Przygotowanie serwerów do instalacji oprogramowania wirtualizacyjnego – aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta.
3. Przygotowanie macierzy do podłączenia do systemu wirtualizacji – aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta.
4. Instalacja oprogramowania wirtualizacyjnego na dostarczonych serwerach.
5. Instalacja najnowszych poprawek do środowiska wirtualizacyjnego oferowanych przez producenta oprogramowania wirtualizacyjnego oraz przez producenta serwerów.
6. Konfiguracja i podłączenie serwerów wirtualizacyjnych do zasobu dyskowego. Zamawiający wymaga takiego skonfigurowania dostępu do zasobu dyskowego, aby każdy wolumen dyskowy zasobu dyskowego był widziany przez każdy z serwerów wirtualizacyjnych poprzez wszystkie ścieżki (porty) udostępniane przez zasób dyskowy. Każdy wolumen dyskowy musi być dostępny dla każdego serwera wirtualizacyjnego w przypadku niedostępności (awarii) n-(n-1) ścieżek, gdzie n oznacza liczbę wszystkich dostępnych ścieżek (portów) udostępnianych przez zasób dyskowy.
7. Konfiguracja i podłączenie serwerów wirtualizacyjnych do sieci LAN Wnioskodawcy. Zamawiający wymaga, aby każdy z serwerów wirtualizacyjnych był podłączony do sieci LAN, co najmniej taką liczbą portów, by w przypadku niedostępności (awarii) n-(n-1) ścieżek, gdzie n oznacza liczbę wszystkich dostępnych ścieżek (portów) był zachowany dostęp do sieci LAN.
8. Konfiguracja sieci w infrastrukturze wirtualnej - konieczna jest konfiguracja wspierająca wirtualne sieci LAN w oparciu o protokół 802.1q.
9. Przygotowanie koncepcji wirtualizacji fizycznych maszyn.
10. Instalacja i konfiguracja oprogramowania zarządzającego środowiskiem wirtualnym.
11. Konfiguracja klastra wysokiej dostępności:
	1. Konfiguracja mechanizmów HA – w przypadku awarii węzła klastra wirtualne maszyny, które są na nim uruchomione muszą zostać przeniesione na sprawny węzeł klastra bez ingerencji użytkownika.
	2. Konfiguracja mechanizmów przenoszenia uruchomionych wirtualnych maszyn pomiędzy węzłami klastra bez utraty dostępu do zasobów wirtualnych maszyn.
	3. Konfiguracja mechanizmów ochrony wirtualnych maszyn przed awarią fizycznego serwera.
12. Weryfikacja działania klastra wysokiej dostępności.
13. Migracja istniejącej infrastruktury do środowiska wirtualnego.
14. Konfiguracja uprawnień w środowisku wirtualizacyjnym – integracja z usługą katalogową
15. Konfiguracja powiadomień o krytycznych zdarzeniach (email).
 |
|  | **Rekonfiguracja systemu zarządzania kopiami zapasowymi.** | 1. Instalacja i rekonfiguracja oprogramowania zarządzającego wykonywaniem kopii zapasowych na dostarczonym serwerze.
2. Aktywacja oraz instalacja niezbędnych licencji.
3. Konfiguracja stacji zarządzającej.
4. Dołączenie klientów do system backupu.
5. Zdefiniowanie zadań backupu oraz przypisanie do nich harmonogramu automatycznego wykonywania:
	1. kopie wirtualnych maszyn muszą być wykonywane przy użyciu mechanizmów oferowanych przez dostarczone środowisko wirtualizujące;
	2. kopie wirtualnych maszyn muszą być wykonywane na dedykowany zasób dyskowy;
	3. kopie wirtualnych maszyn muszą być wykonywane automatycznie wg zadanego harmonogramu;
	4. kopie zapasowe muszą być wykonywane z zastosowaniem mechanizmów deduplikacji danych w celu zapewnienia inteligentnego zarządzania przestrzenią dyskową;
	5. musi istnieć możliwość odtworzenia:
		1. całej wirtualnej maszyny;
		2. dysku wirtualnej maszyny;
		3. pojedynczych plików wirtualnej maszyny (zamontowanie pliku z kopią zapasową w systemie operacyjnym gościa);
6. Zdefiniowanie powiadomień o przebiegu zadania (Zamawiający wymaga skonfigurowania powiadomień na wskazany adres email zawierających, co najmniej:
	1. Nazwę zadania backupu
	2. Status zakończenia zadania backupu /Powodzenie, niepowodzenie/
	3. Długość trwania zadania backupu
	4. Ilość zapisanych na taśmie danych
7. Zdefiniowanie powiadomień na wskazany adres email o zdarzeniach:
	1. Błąd urządzenia
	2. Uszkodzenie wewnętrznej bazy danych systemu zarządzania kopiami zapasowymi
	3. Brak miejsca w wewnętrznej bazie danych systemu zarządzania kopiami zapasowymi
	4. Konieczność przeprowadzenia oczyszczania wewnętrznej bazy danych systemu zarządzania kopiami zapasowymi
	5. Zdarzenia dotyczące licencji
	6. Zapełnienia mail-slotu
8. Uruchomienie testowych zadań backupu
9. Weryfikacja poprawności wykonania kopii zapasowej / weryfikacja działania powiadomień email
10. Uruchomienie testowych zadań odtworzenia danych
11. Miejscem przechowywania kopii zapasowych jest:
	1. serwer backupu.
	2. na etapie wdrożenia należy ustalić czasy RPO (okresu czasu przez jaki dane mogą być utracone w wyniku awarii) i RTO (okresu czasu w ciągu którego system, który uległ awarii powinien zostać przewrócony) z Zamawiającym

System musi zostać podłączony do klastra wirtualizacyjnego, celem wykonywania backupu pełnych maszyn wirtualnych – przechowywanych na serwerze backupu. |
|  | **System NAC** | System należy skonfigurować według zaproponowanych wytycznych przez Wykonawcę z uwzględnieniem wymagań Urzędu. Zakres konfiguracji musi zostać zaakceptowany i ustalony z administratorem.Po przeprowadzanej aktualizacji wymagane jest przeszkolenie administratora z całości systemu ze szczególnym uwzględnieniem nowych funkcjonalności.  |
|  | **System EDR** | Zamawiający wymaga podniesienia wersji aktualnie posiadanego oprogramowania antywirusowego posiadającego moduł XDR.System należy skonfigurować według zaproponowanych wytycznych przez Wykonawcę z uwzględnieniem wymagań Urzędu. Zakres konfiguracji musi zostać zaakceptowany i ustalony z administratorem.Po przeprowadzanej aktualizacji wymagane jest przeszkolenie administratora z całości systemu ze szczególnym uwzględnieniem nowych funkcjonalności.  |
|  | **System do zarzadzania siecią i jednostkami końcowymi** | System należy skonfigurować według zaproponowanych wytycznych przez Wykonawcę z uwzględnieniem wymagań Urzędu. Zakres konfiguracji musi zostać zaakceptowany i ustalony z administratorem.Po przeprowadzanej aktualizacji wymagane jest przeszkolenie administratora z całości systemu ze szczególnym uwzględnieniem nowych funkcjonalności.  |
|  | **Testowanie i modyfikacja parametrów infrastruktury sieciowej.** | 1. Testowanie mechanizmów bezpieczeństwa klastra wirtualizacyjnego.
2. Testowanie wydajności przesyłu i zapisu danych do środowiska LAN.
3. Testowanie mechanizmów replikacji danych.
4. Testowanie dostępu publicznego do zasobów.
5. Testy wydajnościowe połączeń pochodzących z Internetu i wychodzących z zasobów lokalnych do Internetu
6. Testowanie autoryzowanego dostępu do wewnętrznych zasobów.
7. Wprowadzanie koniecznych modyfikacji konfiguracji urządzeń sieciowych po przeprowadzonych testach
 |
|  | **Asysty stanowiskowe** | Asysta stanowiskowa ma obejmować 16 godzin szkoleniowych w ujęciu 8 godzin na jeden dzień. Całość powinna się zamknąć w okresie 2 dni i ma dotyczyć autorskiego rozwiązania zrealizowanego w ramach podmiotowego wdrożenia.Asysta musi być warunkiem dopuszczający do przekazania rozwiązania technicznego do wykorzystania produkcyjnego. Asysta stanowiskowa musi zostać odebrana i zatwierdzona protokołem odbioru sygnowanym przez obie strony projektu tj. wykonawcę oraz użytkownika końcowego. |
|  | **Termin wykonania prac instalacyjno-wdrożeniowych. Oddanie systemu do eksploatacji.** | Wszystkie wymienione prace wdrożeniowe muszą zostać wykonane wspólnie z przedstawicielem Zamawiającego, z każdego etapu prac powinien zostać sporządzony protokół. Powyższe czynności należy wykonać w okresie realizacji Zamówienia po wcześniejszym uzgodnieniu harmonogramu wdrożenia z Wnioskodawcą. **Wykonawca jest zobowiązany do zapewnienia wsparcia technicznego w postaci jednej osoby w siedzibie Zamawiającego w ciągu pierwszego dnia roboczego następującego po pracach wdrożeniowo – instalacyjnych w godzinach od 8.00 do 15.30.** W tym czasie przedstawiciel Wykonawcy:* zobowiązany jest do rozwiązywania problemów technicznych, które wystąpią na etapie oddawania systemu do eksploatacji.
* dokona prezentacji działania sytemu dla pracowników Zamawiającego z zakresu zastosowanych technologii oraz poprawnej eksploatacji wdrożonych rozwiązań, a w szczególności:
1. zastosowanej technologii serwerów
2. zastosowanej technologii pamięci masowej
3. wirtualizacji
4. systemu backupu
5. zastosowanych rozwiązań aplikacyjnych

Wykonawca zapewni również wparcie techniczne ze strony inżynierów w okresie trwania realizacji projektu. Wsparcie polegałoby na pomocy zdalnej lub telefonicznej przy rozwiązaniu problemów, które ewentualnie pojawią się podczas eksploatacji ww. rozwiązania. |
|  | **Opracowanie dokumentacji powykonawczej** | Zamawiający wymaga opracowania szczegółowej dokumentacji technicznej użytkownika (w formie papierowej i elektronicznej) obejmującej wszystkie etapy wdrożenia całości systemu. Wykonawca jest zobowiązany do przygotowania w formie papierowej i elektronicznej procedur eksploatacyjnych systemu.1. Wszelkie zmiany w stosunku do Dokumentacji systemu z podaniem ich powodów.
2. Konfiguracje urządzeń (lub opisy konfiguracji w przypadku sprzętu lub oprogramowania nieumożliwiającego eksportu konfiguracji do pliku tekstowego bądź posiadające rozproszoną konfigurację).
3. Dyski instalacyjne dostarczonego oprogramowania, jeżeli takowe występowały.
4. Kody dostępowe oraz klucze licencyjne, jeżeli takowe występowały.
5. Opis typowych czynności, prac administracyjnych, które pozwalają na codzienną obsługę dostarczonego sprzętu, systemów.
 |

Zgodnie z art. 137 ust. 2 p.z.p. zamawiający udostępnił na stronie internetowej prowadzonego postępowania informację o zmianie treści SWZ.

Zamawiający stwierdza zgodnie z art. 137 ust. 6 p.z.p., że zmiany treści SWZ są nieistotne dla sporządzenia oferty oraz nie wymagają od wykonawców dodatkowego czasu na zapoznanie się ze zmianą SWZ i przygotowanie ofert, dlatego zamawiający nie zmienia termin składania ofert.

Zgodnie z art. 513 pkt 1 p.z.p. mają Państwo prawo wnieść odwołanie. Odwołanie wnosi się do Prezesa Krajowej Izby Odwoławczej, zgodnie z art. 514 ust. 1 p.z.p. Odwołujący jest zobowiązany przekazać zamawiającemu odwołanie wniesione w formie elektronicznej albo postaci elektronicznej albo kopię tego odwołania, jeżeli zostało ono wniesione w formie pisemnej przed upływem terminu do wniesienia odwołania, w taki sposób, aby mógł on zapoznać się z jego treścią przed upływem tego terminu, zgodnie z art. 514 ust. 2 i 3 p.z.p.

Jako że informacja o zmianie treści SWZ została przekazana przy użyciu środków komunikacji elektronicznej oraz zamieszczona na stronie internetowej zamawiającego, to termin wniesienia odwołania do Prezesa Krajowej Izby Odwoławczej oraz przesłania kopii odwołania do zamawiającego to 10 dniach od zakomunikowania wykonawcom o zmianie terminu SWZ i zmianie terminu składania i otwarcia ofert, zgodnie z art. 515 ust. 1 pkt 1 lit. a p.z.p.