Załącznik nr 1 do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

CZĘŚĆ PIERWSZA:

Przedmiot obejmuje kompleksowe rozwiązanie, składające się z następujących komponentów:

1. Oprogramowanie antywirusowe
2. Oprogramowanie antyspamowe
3. Oprogramowanie do ochrony przed ransomware
4. Oprogramowanie typu XDR (Extended Detection and Response)
5. System NGFW – oprogramowanie NGFW (Next Gen FireWall) wraz z platformą sprzętową
6. Certyfikaty SSL serwisów internetowych
7. Serwer do wykonywania kopii zapasowych (w tym z usługą/licencją deduplikacji)
8. Oprogramowanie do zarządzania tożsamością I dostępem
9. Zarządzalne urządzenia sieciowe z obsługą VLAN, MACsec, standardu 802.1X (switch) - Przełącznik sieciowy 3 szt.
10. Oprogramowanie SIEM (Security Information and Event Management)
11. Szafa RACK do produktów i rozwiązań z zakresu bezpieczeństwa
12. Network Attached Storage (NAS)
13. Oprogramowanie typu Menadżer logów
14. Oprogramowanie do monitorowania infrastruktury informatycznej
15. System wirtualizacyjny dedykowany do systemów, na których zostanie zainstalowanych produkt z zakresu cyberbezpieczeństwa
16. System operacyjny i/lub licencje dostępowe (również rozbudowa licencji do już istniejącego systemu), na których zainstalowany będzie system lub wdrożone rozwiązanie z zakresu cyberbezpieczeństwa
17. Access Point WiFi z obsługą standardu 802.1x oraz WPA3-Enterprise
18. Urządzenie typu UPS do produktów i rozwiązań z zakresu bezpieczeństwa
19. UTM (Unified Threat Management) – 3 szt.
20. VPN (Virtual Private Network)

I. Informacje ogólne

1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa, wdrożenie, konfiguracja oraz uruchomienie infrastruktury teleinformatycznej i systemów bezpieczeństwa teleinformatycznego wraz z niezbędnym oprogramowaniem, licencjami oraz usługami towarzyszącymi, mającymi na celu podniesienie poziomu cyberbezpieczeństwa infrastruktury Zamawiającego.

Zakres zamówienia obejmuje w szczególności dostawę urządzeń infrastruktury sieciowej i serwerowej, systemów ochrony przed zagrożeniami cybernetycznymi, systemów monitorowania infrastruktury oraz bezpieczeństwa, systemów wykonywania kopii zapasowych, systemów zarządzania tożsamością i dostępem, rozwiązań zapewniających ciągłość działania infrastruktury teleinformatycznej oraz wykonanie niezbędnych prac instalacyjnych i konfiguracyjnych.

Szczegółowy zakres rzeczowy zamówienia określono w dalszej części niniejszego Opisu Przedmiotu Zamówienia.

2. Cel zamówienia

Celem realizacji zamówienia jest zwiększenie poziomu bezpieczeństwa systemów teleinformatycznych Zamawiającego poprzez wdrożenie kompleksowych rozwiązań obejmujących ochronę stacji roboczych i serwerów, zabezpieczenie infrastruktury sieciowej, centralizację monitorowania zdarzeń bezpieczeństwa, usprawnienie zarządzania tożsamością użytkowników, zapewnienie wysokiej dostępności usług oraz zwiększenie odporności infrastruktury na awarie i incydenty bezpieczeństwa.

Realizacja zamówienia ma zapewnić w szczególności:

- zwiększenie poziomu ochrony przed zagrożeniami cybernetycznymi;
- zapewnienie skutecznej ochrony sieci teleinformatycznej;
- wdrożenie mechanizmów monitorowania infrastruktury oraz zdarzeń bezpieczeństwa;
- zapewnienie bezpiecznego dostępu użytkowników do zasobów informatycznych;
- zapewnienie możliwości wykonywania oraz odtwarzania kopii zapasowych;
- zwiększenie niezawodności zasilania infrastruktury krytycznej;
- zapewnienie możliwości bezpiecznej pracy zdalnej użytkowników;
- zwiększenie dostępności usług teleinformatycznych.

3. Zakres realizacji zamówienia

W ramach realizacji zamówienia Wykonawca zobowiązany będzie do wykonania wszystkich czynności niezbędnych do osiągnięcia pełnej funkcjonalności dostarczanych rozwiązań, w szczególności:

- dostawy urządzeń, oprogramowania oraz licencji;
- wniesienia i montażu dostarczonych urządzeń;
- instalacji oraz konfiguracji wszystkich elementów systemu;

- integracji dostarczonych rozwiązań z istniejącą infrastrukturą Zamawiającego;
- uruchomienia wszystkich funkcjonalności wymaganych w OPZ;
- przekazania dokumentacji powdrożeniowej;
- przeprowadzenia instruktażu lub szkolenia administratorów w zakresie podstawowej obsługi wdrożonych rozwiązań.

4. Wymagania ogólne dotyczące oferowanych rozwiązań

Wszystkie oferowane urządzenia, oprogramowanie oraz licencje muszą:

1. być fabrycznie nowe, nieużywane oraz pochodzić z oficjalnego kanału dystrybucji producenta;
2. być wolne od wad prawnych oraz praw osób trzecich;
3. posiadać wszystkie wymagane licencje umożliwiające ich legalne użytkowanie przez Zamawiającego;
4. pochodzić z aktualnej oferty producenta i nie znajdować się na liście produktów wycofanych ze sprzedaży (End of Sale) ani produktów, dla których zakończono wsparcie producenta (End of Support), na dzień składania ofert;
5. zapewniać możliwość objęcia wsparciem technicznym producenta przez okres wymagany w niniejszym OPZ;

5. Wymagania dotyczące licencji

Jeżeli w ramach realizacji zamówienia wymagane jest dostarczenie licencji, Wykonawca zobowiązany jest dostarczyć licencje:

- bezterminowe lub terminowe zgodnie z wymaganiami określonymi dla poszczególnych pozycji OPZ;
- uprawniające Zamawiającego do korzystania z pełnej funkcjonalności oferowanego rozwiązania;
- wystawione zgodnie z zasadami licencjonowania producenta.

W przypadku oprogramowania subskrypcyjnego okres obowiązywania subskrypcji musi obejmować zakres od daty odbioru przedmiotu zamówienia do dnia 31.12.2026 r.

6. Wymagania dotyczące wdrożenia

Wykonawca zobowiązany jest do wykonania wszystkich prac instalacyjnych i konfiguracyjnych niezbędnych do uruchomienia dostarczonych rozwiązań.

W szczególności Wykonawca zobowiązany będzie do:

- instalacji dostarczonych urządzeń;
- konfiguracji zgodnie z wymaganiami Zamawiającego;
- integracji pomiędzy dostarczanymi rozwiązaniami;

- uruchomienia usług produkcyjnych.

Wszelkie czynności wdrożeniowe należy realizować w sposób minimalizujący wpływ na bieżące funkcjonowanie infrastruktury Zamawiającego.

7. Dokumentacja

Po zakończeniu realizacji zamówienia Wykonawca przekaże Zamawiającemu dokumentację powdrożeniową obejmującą co najmniej:

- wykaz dostarczonych urządzeń i licencji;
- numery seryjne urządzeń;
- zestawienie kluczy licencyjnych, o ile są stosowane;
- opis wykonanej konfiguracji;
- schemat logiczny wdrożonej infrastruktury;
- wykaz adresacji IP urządzeń objętych wdrożeniem (jeżeli dotyczy).

Dokumentacja zostanie przekazana w wersji elektronicznej w formacie PDF oraz w edytowalnym formacie umożliwiającym jej dalszą aktualizację.

8. Szkolenie administratorów

W ramach realizacji zamówienia Wykonawca przeprowadzi instruktaż lub szkolenie dla administratorów Zamawiającego obejmujące podstawową obsługę wdrożonych rozwiązań, w zakresie adekwatnym do dostarczonych systemów.

Szkolenie powinno obejmować w szczególności:

- podstawową administrację;
- monitorowanie pracy systemów;
- wykonywanie podstawowych czynności eksploatacyjnych;
- procedury zgłaszania awarii do producenta lub Wykonawcy.

9. Gwarancja i wsparcie techniczne

Jeżeli dla poszczególnych pozycji OPZ nie wskazano odmiennych wymagań, Wykonawca zapewni:

- gwarancję producenta lub Wykonawcy przez okres nie krótszy niż 24 miesiące od dnia podpisania protokołu odbioru końcowego;
- dostęp do aktualizacji oprogramowania i poprawek bezpieczeństwa przez okres obowiązywania wymaganych licencji lub subskrypcji;
- możliwość zgłaszania awarii w dni robocze;
- usuwanie wad zgodnie z warunkami gwarancji producenta lub Wykonawcy.

10. Zasady równoważności

W przypadku, gdy w dalszej części Opisu Przedmiotu Zamówienia wskazano nazwy producentów, modeli, znaków towarowych, patentów, pochodzenia lub innych oznaczeń identyfikujących konkretne rozwiązania, należy je traktować wyłącznie jako wskazanie standardu jakościowego, funkcjonalnego, technicznego lub eksploatacyjnego oczekiwanego przez Zamawiającego.

Zamawiający dopuszcza zaoferowanie rozwiązań równoważnych, pod warunkiem wykazania przez Wykonawcę, że oferowane rozwiązania spełniają wszystkie minimalne wymagania określone w niniejszym OPZ oraz zapewniają parametry techniczne, funkcjonalne, jakościowe i eksploatacyjne nie gorsze od rozwiązań wskazanych jako przykładowe.

Ciężar udowodnienia równoważności oferowanego rozwiązania spoczywa na Wykonawcy.

W przypadku zaoferowania rozwiązania równoważnego Wykonawca zobowiązany jest przedłożyć wraz z ofertą dokumenty umożliwiające ocenę spełnienia wymagań określonych przez Zamawiającego, w szczególności karty katalogowe, specyfikacje techniczne, dokumentację producenta lub inne dokumenty potwierdzające spełnienie wymaganych parametrów.

11. Dostawcy wysokiego ryzyka:

W ramach realizacji zamówienia Wykonawca zobowiązany jest dostarczyć rozwiązania (sprzęt, oprogramowanie, usługi), które nie są wytworzone ani dostarczane przez podmioty znajdujące się w wykazie dostawców wysokiego ryzyka publikowanym w Dzienniku Urzędowym Rzeczypospolitej Polskiej "Monitor Polski", na podstawie decyzji, o której mowa w art. 67b ust. 15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2026 r., poz. 20 ze zm., dalej „KSC”). Wykonawca na wezwanie Zamawiającego przedstawi wykaz producentów oraz kraj pochodzenia oferowanych kluczowych komponentów ICT.

Wykonawca ma obowiązek zweryfikować w zakresie dostarczanego przedmiotu zamówienia, że kody źródłowe i/lub infrastruktura chmurowa (jeśli dotyczy) nie są kontrolowane przez dostawcę wysokiego ryzyka, w rozumieniu KSC.

II. Szczegółowy opis przedmiotu zamówienia

Informacja wspólna dotycząca pozycji 1–4

Zamawiający dopuszcza realizację wymagań określonych w pozycjach 1–4 przy wykorzystaniu jednego zintegrowanego rozwiązania bezpieczeństwa, pod warunkiem zapewnienia wszystkich wymaganych funkcjonalności opisanych dla każdej z pozycji oraz możliwości centralnego zarządzania i administrowania całym środowiskiem. Dostarczone licencje muszą umożliwiać ochronę w sumie dla minimum 25 urządzeń końcowych.

1. Oprogramowanie antywirusowe

1.1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa, wdrożenie oraz konfiguracja systemu ochrony antywirusowej dla stacji roboczych i serwerów Zamawiającego wraz z centralnym systemem zarządzania.

1.2. Minimalne wymagania funkcjonalne

Oferowane rozwiązanie musi zapewniać co najmniej:

1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).

2. Rozwiązanie musi wspierać architekturę ARM64.

3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.

4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.

5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.

6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.

7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.

8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.

9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.

10. Rozwiązanie musi integrować się z Intel Threat Detection Technology.

11. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).

12. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.

13. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.

14. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.

15. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.

16. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:

• tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,

• tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,

• tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,

• tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,

• tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.

17. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.

18. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.

19. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.

20. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).

21. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.

22. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook.

23. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:

• tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,

• tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,

• tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,

• tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.

24. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.

25. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.

26. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.

27. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.

28. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.

29. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.

30. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.

Ochrona serwer

1. Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowsze oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL) 7,8 i 9, CentOS 7, UbuntuServer 18.04 LTS i nowsze, Debian 10, Debian 11 i Debian 12, SUSE Linux Enterprise Server (SLES) 15, Oracle Linux 8 oraz Amazon Linux.

2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.

3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.

4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.

5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.

6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.

7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.

8. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.

Dodatkowe wymagania dla ochrony serwerów Windows:

9. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.

10. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).

11. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.

12. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.

13. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.

14. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.

15. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.

16. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.

17. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.

Dodatkowe wymagania dla ochrony serwerów Linux:

18. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.

19. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.

20. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.

21. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.

Szyfrowanie

1. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 7/8/8.1/10 32-bit i 64-bit.

2. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault).

3. Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia.

4. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.

Ochrona urządzeń mobilnych opartych o system Android

1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.

2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.

3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).

4. Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM.

5. Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:

a. usunięcie zawartości urządzenia,

b. przywrócenie urządzenie do ustawień fabrycznych,

c. zablokowania urządzenia,

d. uruchomienie sygnału dźwiękowego,

e. lokalizację GPS.

6. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.

7. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:

a. nazwę aplikacji,

b. nazwę pakietu,

c. kategorię sklepu Google Play,

d. uprawnienia aplikacji,

e. pochodzenie aplikacji z nieznanego źródła.

Sandbox w chmurze

1. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.

2. Rozwiązanie musi wykorzystywać do działania chmurę producenta.

3. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi.

4. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.

5. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.

6. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.

7. Po zakończonej analizie pliku, rozwiązanie musi przesyłać wynik analizy do wszystkich wspieranych produktów.

8. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy.

9. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.

10. Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych.

11. Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzeć jakie pliki zostały wysłane do analizy oraz przez kogo.

12. Przeanalizowane pliki muszą zostać odpowiednio oznaczone.

13. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.

14. W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki.

15. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia.

2. Oprogramowanie antyspamowe

2.1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa i wdrożenie systemu ochrony poczty elektronicznej przed spamem, phishingiem oraz złośliwym oprogramowaniem.

2.2. Minimalne wymagania funkcjonalne

Oferowane rozwiązanie musi zapewniać co najmniej:

- analizę ruchu poczty elektronicznej;
- wykrywanie i blokowanie wiadomości spam;
- wykrywanie prób phishingu;
- analizę załączników pocztowych;
- skanowanie wiadomości pod kątem obecności złośliwego oprogramowania;
- filtrowanie wiadomości na podstawie reputacji nadawców;
- możliwość tworzenia białych i czarnych list;
- możliwość definiowania własnych reguł filtrowania;
- raportowanie wykrytych zagrożeń;
- centralne zarządzanie politykami ochrony.

2.3. Minimalne wymagania techniczne

Rozwiązanie powinno:

- współpracować z wykorzystywanym przez Zamawiającego systemem poczty elektronicznej;
- umożliwiać automatyczne aktualizowanie mechanizmów wykrywania zagrożeń;
- umożliwiać tworzenie raportów administracyjnych;
- umożliwiać integrację z centralną konsolą zarządzania.

3. Oprogramowanie chroniące przed ransomware

3.1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa i wdrożenie rozwiązania zapewniającego ochronę przed atakami typu ransomware oraz innymi zagrożeniami wykorzystującymi szyfrowanie danych.

3.2. Minimalne wymagania funkcjonalne

Rozwiązanie musi zapewniać co najmniej:

- wykrywanie charakterystycznych zachowań oprogramowania ransomware;
- analizę behawioralną procesów;
- automatyczne blokowanie procesu szyfrującego;
- możliwość zatrzymania procesu powodującego nieautoryzowaną modyfikację danych;
- ochronę katalogów wskazanych przez administratora;
- możliwość definiowania wyjątków;
- generowanie alertów o wykrytych incydentach;
- rejestrowanie wszystkich wykrytych zdarzeń;
- współpracę z centralną konsolą zarządzania.

3.3. Minimalne wymagania techniczne

Rozwiązanie powinno:

- działać na stacjach roboczych oraz serwerach;
- umożliwiać centralną konfigurację polityk;
- umożliwiać automatyczne aktualizacje;
- współpracować z rozwiązaniem antywirusowym.

4. System XDR

4.1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa i wdrożenie rozwiązania klasy Extended Detection and Response (XDR), umożliwiającego centralne wykrywanie, analizę oraz reagowanie na incydenty bezpieczeństwa.

4.2. Minimalne wymagania funkcjonalne

Rozwiązanie musi zapewniać co najmniej:

1. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.

2. Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego producenta.

3. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.

4. Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.

5. Wykluczenia muszą dotyczyć procesu lub procesu „rodzica".

6. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia.

7. Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika.

8. Serwer musi posiadać ponad 900 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator musi też posiadać możliwość utworzenia własnych reguł i edycji reguł dodanych przez producenta.

9. Serwer administracyjny musi oferować możliwość blokowania plików po sumach kontrolnych. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej.

10. Administrator musi posiadać możliwość weryfikacji uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku.

11. Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania.

12. Administrator musi posiadać możliwość weryfikacji uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny.

13. W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej.

14. W ramach przeglądania wykonanego skryptu lub pliku exe, administrator musi posiadać możliwość weryfikacji powiązanych zdarzeń dotyczących przynajmniej: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych.

15. Serwer administracyjny musi oferować możliwość przekierowania do konsoli zarządzającej produktu antywirusowego tego samego producenta, w celu weryfikacji szczegółów wybranej stacji roboczej. W konsoli zarządzającej produktu antywirusowego, administrator musi mieć możliwość podglądu informacji dotyczących przynajmniej: podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor,pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty

sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich.

16. Konsola administracyjna musi mieć możliwość tagowania obiektów.

17. Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń powershell.

5. System klasy Next Generation Firewall (NGFW) dla lokalizacji głównej

5.1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa, instalacja, konfiguracja i uruchomienie jednego centralnego urządzenia bezpieczeństwa sieciowego klasy Next Generation Firewall (NGFW), przeznaczonego do ochrony centralnej lokalizacji Zamawiającego.

Urządzenie musi zapewniać funkcje zapory sieciowej, ochrony przed zagrożeniami sieciowymi, kontroli aplikacji, filtrowania treści i stron internetowych, ochrony antywirusowej, bezpiecznej komunikacji VPN oraz rejestrowania zdarzeń bezpieczeństwa.

W ramach dostawy należy zapewnić kompletne urządzenie sprzętowe wraz z całym niezbędnym oprogramowaniem, licencjami, subskrypcjami i aktualizacjami wymaganymi do korzystania z wymaganych funkcji.

Zamawiający dopuszcza realizację funkcjonalności określonych w niniejszej pozycji oraz w pozycji 22 (System VPN) przy wykorzystaniu jednego rozwiązania, pod warunkiem spełnienia wszystkich wymagań określonych dla obu pozycji.

5.2. OBSŁUGA SIECI

- Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP.

5.3. ZAPORA KORPORACYJNA (Firewall)

1. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection.

2. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT.

3. Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).

4. Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie.

5. Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, usług internetowych (web services), użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia.

6. Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac.

7. Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall.

8. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł.

9. Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos.

10. Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego).

11. System musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe.

5.4. INTRUSION PREVENTION SYSTEM (IPS)

1. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.

2. Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy.

3. Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.

4. Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS.

5. Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia.

6. Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS.

7. Administrator ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP.

8. Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.

9. Moduł IPS ma zapewniać analizę protokołów przemysłowych co najmniej takich jak: Modbus, UMAS, S7 200-300-400, EtherNet/IP, CIP, OPC UA, OPC (DA/HDA/AE), BACnet/IP, PROFINET, SOFBUS/LACBUS, IEC 60870-5-104, IEC 61850 (MMS, Goose& SV).

10. Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych.

5.5. KSZTAŁTOWANIE PASMA (TrafficShapping)

1. Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.

2. Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP.

3. Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring).

Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.

5.6. OCHRONA ANTYWIRUSOWA

1. Urządzenie ma być dostarczone wraz z komercyjnym, zaawansowanym skanerem antywirusowym oraz umożliwiać skanowanie plików w oparciu o sandboxing zlokalizowany w Internecie na serwerach producenta i na terenie Unii Europejskiej. Nie dopuszcza się aby analiza sandboxingu była przeprowadzana na urządzeniu lub wymagała instalacji dodatkowego urządzenia lub oprogramowania. Nie dopuszcza się również żeby analiza sandboxingu była przeprowadzana przez firmy trzecie.

2. Skaner antywirusowy ma być dostarczany przez firmy trzecie (inne niż producent rozwiązania).

3. Administrator ma mieć możliwość określenia akcji w przypadku wykrycia zagrożenia bądź gdy analiza skanerem antywirusowym została zakończona błędem.

4. Skaner antywirusowy ma pochodzić od europejskiego producenta.

5. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.

Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu wykrycia infekcji.

5.7. OCHRONA ANTYSPAM

1. Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).

2. Ochrona antyspam ma działać w oparciu o:

a. - białe/czarne listy,

b. DNS RBL,

c. Skaner heurystyczny.

3. W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia.

4. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.

5.8. WIRTUALNE SIECI PRYWATNE (VPN)

1. Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).

2. Urządzenie ma wspierać co najmniej następujące typy sieci VPN:

a) PPTP VPN,

b) IPSec VPN,

c) SSL VPN.

3. SSL VPN ma działać w trybie tunelu.

4. Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem.

5. Klient SSL VPN ma być dostępny z poziomu portalu uwierzytelniania (captive portal)

6. Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).

7. Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf.

8. Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz RouteBased.

5.9. FILTR DOSTĘPU DO STRON WWW

1. Urządzenie ma posiadać wbudowany filtr URL.

2. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 77 kategorii tematycznych stron internetowych. Rozszerzony URL Filtering posiada miliony sklasyfikowanych stron internetowych.

3. Klasyfikacja URL musi się odbywać w oparciu o komunikację z serwerami producenta znajdującymi się w sieci Internet, a nie na bazie danych przechowywanej lokalnie w urządzeniu.

4. Administrator ma mieć możliwość dodawania własnych kategorii URL.

5. Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej:

a. blokowanie dostępu do adresu URL,

b. zezwolenie na dostęp do adresu URL,

c. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.

6. Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.

7. Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych.

8. Filtr URL musi uwzględniać komunikację po protokole HTTPS.

9. Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.

10. Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane.

11. Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch

5.10. UWIERZYTELNIANIE

1. Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o: lokalną bazę użytkowników (wewnętrzny LDAP),

2. zewnętrzną bazę użytkowników (zewnętrzny LDAP),

3. usługę katalogową Microsoft Active Directory.

4. Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP.

5. Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły: SSL,

6. Radius,

7. Kerberos.

8. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy.

9. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta.

10. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny.

11. Rozwiązanie musi mieć możliwość transparentnego uwierzytelniania użytkowników w ramach infrastruktury VDI (Virtual Desktop Infrastructure) poprzez dedykowanego agenta. Metoda ta musi wspierać co najmniej technologie Citrix Virtual Apps i Microsoft Remote Desktop Services (RDS).

12. Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP).

13. Wbudowany moduł 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH.

14. Rozwiązanie musi zapewniać Zero-Trust Network Access (ZTNA), dając dostęp do zasobów na podstawie analizy polityk bezpieczeństwa w oparciu co najmniej o weryfikację wersji systemu operacyjnego, statusu zapory sieciowej czy zainstalowanego programu antywirusowego na stacji roboczej.

5.11. ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP)

1. Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. LoadBalancing).

2. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy: równoważenie względem adresu źródłowego, równoważenie względem połączenia.

3. Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.

4. Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover).

5. Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza.

6. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów).

7. Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP.

5.12. ROUTING (TRASOWANIE)

1. Urządzenie ma umożliwiać statyczne trasowanie pakietów.

2. Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.

3. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing).

4. Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.

5. Rozwiązanie musi dawać możliwość wybrania predefiniowalnego obiektu typu blackhole.

5.13. ADMINISTRACJA URZĄDZENIEM

1. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.

2. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS.

3. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP.

4. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.

5. Urządzenie musi oferować możliwość wykorzystania wbudowanych profili administracyjnych określających dostęp do poszczególnych modułów systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis.

6. Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH)

7. Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania.

8. Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS.

9. Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup.

10. Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych.

11. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła.

12. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora (scriptrecording).

13. System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services).

14. Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników.

15. Urządzenie ma umożliwiać zapisywanie logów na wbudowanym dysku.

16. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).

17. Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX.

18. Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie: manualnego eksportu do pliku w dowolnym momencie czasu, automatycznego eksportu do serwerów producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu

19. Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzącego bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora.

20. Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.

21. Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego

5.14. RAPORTOWANIE

1. Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.

2. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.

3. System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego.

4. System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów.

5. System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu.

6. System raportowania ma umożliwiać eksport wyników raportu do formatu CSV.

7. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta.

8. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3.

9. Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).

5.15. POZOSTAŁE USŁUGI I FUNKCJE

1. Urządzenie ma umożliwiać stworzenie interfejsu zagregowanego w oparciu o protokół LACP.

2. Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.

3. Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay).

4. Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6.

5. Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci skonfigurowanych zarówno na interfejsach fizycznych jak i wirtualnych (VLAN) w zakresie określenia bramy, serwerów DNS, nazwy domeny).

6. Urządzenie ma posiadać usługę DNS Proxy.

7. Urządzenie ma posiadać wsparcie dla Spanning-treeprotocol (RSTP/MSTP).

8. Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN.

9. Urządzenie musi mieć zaimplementowane Open API.

Urządzenie ma posiadać dwie niezależne partycje np. w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware). W tym celu ma być możliwe zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie.

5.16. PARAMETRY SPRZĘTOWE

1. Urządzenie ma być wyposażone w dysk SSD o pojemności co najmniej 200 GB.

2. Urządzenie wyposażone jest w redundantne zasilanie z sygnalizacją pracy poszczególnych zasilaczy.

3. Liczba portów Ethernet 2,5Gbps – min. 8 z możliwością rozszerzenia do 16. Liczba portów światłowodowych 1Gbps – min. 2 z możliwością rozszerzenia do 10.

4. Urządzenie ma pozwalać na instalację modułu rozszerzeń z poniższej listy:

a) Moduł z 8 interfejsami miedzianymi 2,5Gbps

b) Moduł z 4 interfejsami miedzianymi 10Gbps.

c) Moduł z 8 interfejsami miedzianymi 1Gbps (4 pary interfejsów w trybie bypass).

d) Moduł z 8 interfejsami miedzianymi 1Gbps.

e) Moduł z 8 interfejsami światłowodowymi 1Gbps.

f) Moduł z 4 interfejsami światłowodowymi 10Gbps.

g) Moduł z 2 interfejsami światłowodowymi 25Gbps.

8. Przepustowość Firewall (1518 bajtów UDP) – minimum 18Gbps.

9. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 10Gbps.

10. Przepustowość filtrowania Antywirusowego – minimum 1.3 Gbps.

11. Liczba tuneli VPN IPSec – minimum 1400.

12. Liczba tuneli typu SSL VPN (tryb tunelu) – minimum 400.

13. Obsługa interfejsów 802.11q (VLAN) – minimum 1200.

14. Liczba równoczesnych sesji – minimum 600 000 i nie mniej niż 80 000 nowych sesji/sekundę.

15. Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive.

16. Liczba reguł filtrowania – minimum 16 000.

17. Liczba tras statycznego routingu – minimum 5 000.

18. Liczba tras dynamicznego routingu – minimum 9 000.

19. Możliwość instalacji w szafie RACK 19”, wysokość urządzenia 1U.

20. Urządzenie musi być wyposażone w moduł TPM.

UWAGI:

1. Kabel zasilający do zasilacza oraz inny niezbędny do prawidłowej pracy Urządzenia asortyment, będzie dostarczony przez wykonawcę w komplecie z urządzeniami.
2. Wszystkie komponenty Urządzenia muszą być fabrycznie nowe nie używane i nie refabrykowane oraz nie recertyfikowane.
3. Urządzenie musi być zaprojektowane i rozwijane na terenie Unii Europejskiej.
4. Urządzenie musi posiadać certyfikat EAL4+.

6. Certyfikaty SSL/TLS dla serwisów internetowych

6.1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa, wdrożenie oraz aktywacja certyfikatów SSL/TLS przeznaczonych do zabezpieczenia serwisów internetowych oraz usług udostępnianych przez Zamawiającego.

Zakres zamówienia obejmuje również wykonanie wszystkich czynności niezbędnych do prawidłowego wdrożenia certyfikatów, ich konfiguracji oraz uruchomienia.

6.2. Minimalne wymagania funkcjonalne

Dostarczone certyfikaty muszą zapewniać co najmniej:

- szyfrowanie komunikacji z wykorzystaniem protokołu TLS;
- potwierdzenie tożsamości właściciela domeny na poziomie Organization Validation (OV) lub równoważnym;
- zgodność z aktualnie obowiązującymi standardami bezpieczeństwa;
- możliwość wykorzystania na serwerach internetowych wykorzystywanych przez Zamawiającego;
- kompatybilność z najpopularniejszymi przeglądarkami internetowymi;
- możliwość odnowienia certyfikatów po zakończeniu okresu ich ważności.

6.3. Minimalne wymagania techniczne

Certyfikaty powinny:

- wykorzystywać algorytmy kryptograficzne zgodne z aktualnymi zaleceniami branżowymi;
- obsługiwać protokół TLS w aktualnie wspieranych wersjach;
- być wystawione przez publicznie zaufane centrum certyfikacji;
- umożliwiać instalację na wykorzystywanym przez Zamawiającego środowisku serwerowym.

7. Serwer do wykonywania kopii zapasowych

7.1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa, montaż, konfiguracja oraz uruchomienie serwera przeznaczonego do realizacji kopii zapasowych infrastruktury teleinformatycznej Zamawiającego wraz z oprogramowaniem umożliwiającym wykonywanie, przechowywanie oraz odtwarzanie kopii zapasowych maszyn wirtualnych, serwerów oraz danych.

Zamawiający dopuszcza realizację funkcjonalności sprzętowych i programowych przy wykorzystaniu jednego kompletnego rozwiązania.

7.2. Minimalne wymagania funkcjonalne

Oferowane rozwiązanie musi zapewniać co najmniej:

- wykonywanie pełnych, przyrostowych oraz różnicowych kopii zapasowych;
- wykonywanie kopii zapasowych maszyn wirtualnych bez konieczności ich wyłączania;
- deduplikację danych;
- kompresję danych;
- harmonogramowanie wykonywania kopii zapasowych;
- możliwość tworzenia wielu harmonogramów kopii;
- retencję kopii zapasowych;
- szyfrowanie repozytorium kopii zapasowych;
- weryfikację integralności wykonanych kopii;
- możliwość odtworzenia pojedynczych plików;
- możliwość odtworzenia całej maszyny wirtualnej;
- możliwość odtworzenia serwera na innej platformie sprzętowej;
- automatyczne powiadamianie administratorów o błędach wykonywania kopii zapasowych;
- centralne zarządzanie zadaniami backupu;
- możliwość rozbudowy przestrzeni dyskowej w przyszłości.

7.3. Minimalne wymagania techniczne – serwer

Oferowany serwer musi być fabrycznie nowy i pochodzić z bieżącej oferty producenta.

Minimalne wymagania:

Nazwa elementu, parametru lub cechy	Opis wymagań Serwerów
Obudowa	Do instalacji w szafie Rack 19”, wysokość nie więcej niż 1U, z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych. Możliwość instalacji ramienia do zarządzania kablami.
Procesor	Architektura x86, maksymalny TDP dla procesora – maksymalnie 150W. Wymagana ilość rdzeni dla procesora – 12. Minimalna częstotliwość pracy procesora 2.2GHz. Minimalna ilość kanałów procesora – 8. Ilość kości pamięci na kanał – 2. Wynik wydajności procesora nie powinien być niższy niż 286 punkty base w teście SPECrate 2017 Integer w konfiguracji dwuprocesorowej, opublikowanym przez

	SPEC.org (www.spec.org), dla serwera oferowanego producenta.
Liczba zainstalowanych procesorów	2
Płyta główna	Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera z możliwością zainstalowania do dwóch procesorów Intel Xeon wykonujących 64-bitowe instrukcje
Pamięć operacyjna	Zainstalowane minimum 128GB pamięci RAM o częstotliwości 6400MHz. Pamięć zainstalowana w kościach 32GB Minimum 32 sloty na pamięć. Możliwość rozbudowy do 8TB RAM.
Zabezpieczenie pamięci	Memory mirroring, ECC, SDDC, ADDDC
Procesor Graficzny	Zintegrowana karta graficzna z minimum 16MB pamięci osiągająca rozdzielczość 1920x1200 przy 60 Hz.
Rozbudowa dysków	Zainstalowane z tyłu obudowy dwa dyski NVMe M.2 o pojemności minimum 960GB każdy zabezpieczone sprzętowym RAID 1. Dyski muszą mieć możliwość wymiany na gorąco. Zainstalowane pięć dysków SSD klasy enterprise o pojemności nie mniejszej niż 3,84TB każdy. Wymagany jest wewnętrzny slot na kartę Micro SD.
Zasilacz	Minimum dwa redundantne zasilacze o mocy minimum 800W z certyfikatem minimum Titanium. Moc pojedynczego zasilacza musi być wystarczająca do zasilenia serwera w oferowanej konfiguracji.
Interfejsy sieciowe	Zainstalowane dwuportowa karta 10GBASE-T. Karta nie może zajmować żadnego ze slotów PCIe. Jeden port RJ-45 o przepustowości 1GbE dedykowany dla karty zarządzającej.
Sloty I/O	Serwer w momencie dostawy powinien posiadać 2 sloty PCIe Gen5 x8 z czego jeden High-Profile, 2 sloty OCP Gen5 oraz jeden slot PCIe wewnątrz obudowy serwera dedykowany pod kontroler dyskowy.
Dodatkowe porty	• z przodu obudowy: możliwość instalacji 2x USB 3 (z czego jeden z możliwością zarządzania serwerem) , zewnętrzny dedykowany port diagnostyczny, możliwość instalacji portu Mini DisplayPort

	• z tyłu obudowy: 2x USB 3, 1x VGA, 1x RJ-45 do zarządzania serwerem. Możliwość instalacji portu DB9. • wewnątrz obudowy: Możliwość instalacji portu USB 3 wewnątrz obudowy. Wszystkie tylne porty USB, port RJ-45 służący do zarządzania, tylny port VGA,, wewnętrzny port na kartę Micro SD powinny być umieszczone na osobnej dedykowanej płytce I/O, którą łączy się bezpośrednio z płytą główną serwera.
Chłodzenie	Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo minimum N+1
Zarządzanie	Wymagany wbudowany sprzętowy kontroler zdalnego zarządzania, który musi być umieszczony na osobnej dedykowanej płytce I/O (wspomnianej w sekcji Dodatkowe Porty). • Monitoring stanu systemu (komponenty objęte monitoringiem to przynajmniej: CPU, pamięć RAM, dyski, karty PCI, zasilacze, wentylatory, płyta główna • Pozyskanie nastepujacych informacji o serwerze: nazwa, typ i model, numer seryjny, nazwa systemu, wersja UEFI oraz BMC, adres ip karty zarzadzajacej, utylizacja cpu, utylizacja pamięci oraz komponentow I/O, lokalizacja • Logowanie zdarzeń systemowych oraz związanych z działaniami użytkownika. Każdy dziennik zdarzeń powinien mieć możliwość zapisu co najmniej 1024 rekordów. • Logowanie zdarzeń związanych z utrzymaniem systemu jak upgrade firmware, zmiana/instalacja sprzętu. System powinien umożliwiać zapisanie minimum 250 zdarzeń. • Wysylanie określonych zdarzeń poprzez SMTP oraz SNMPv3 • Update systemowego firmware • Monitoring i możliwość ograniczenia poboru prądu • Zdalne włączanie/wyłączanie/restart • Zapis video zdalnych sesji • Podmontowanie lokalnych mediow z wykorzystaniem Java client • Przekierowanie kosnoli szeregowej przez IPMI • Zrzut ekranu w momencie zawieszenia systemu

- Możliwość przejęcia zdalnego ekranu
- Możliwość zdalnej instalacji systemu operacyjnego
- Alerty Syslog
- Przekierowanie konsoli szeregowej przez SSH
- Wyświetlanie danych aktualnych I historycznych dla użycia energii oraz temperatury serwera
- Możliwość mapowania obrazów ISO z lokalnego dysku operatora
- Możliwość mapowania obrazów ISO przez HTTPS, SFTP, CIFS oraz NFS
- Możliwość jednoczesnej pracy do 6 użytkowników przez wirtualną konsolę
- wspierane protokoły/interfejsy: IPMI v2.0, SNMP v3, CIM, DCMI v1.5, REST API
- Wymaga się możliwości wykorzystania frontowego portu USB do celów serwisowych (komunikacja portu z karta zarządzającą) bez możliwości uzyskania jakiejkolwiek funkcjonalności na poziomie zainstalowanego systemu operacyjnego. Funkcjonalność ta musi być realizowana na poziomie sprzętowym i musi być niezależna od zainstalowanego systemu operacyjnego.
- Kontroler zarządzania musi posiadać 4Gb wewnętrznej pamięci (dopuszcza się zastosowanie karty Micro SD w celu uzyskania tej pojemności). Pamięć kontrolera zarządzania musi pełnić funkcję RDOC (Remote Disc on Card) oraz musi umożliwiać przechowywanie plików firmware.
- Monitorowanie zmian sprzętowych w celu wykrycia nieoczekiwanych zmian. Po wykryciu zmiany zapis w logu serwera lub uniemożliwienie boot'u.
- Możliwość synchronizacji konfiguracji i poziomów firmware pomiędzy serwerami.
- Możliwość monitorowania i zarządzania grupą serwerwów z poziomu kontrolera zarządzania pojedynczego serwera. Ilość serwerów możliwych do zarządzania – minimum 200.

Wraz z serwerem powinno zostać dostarczone dodatkowe oprogramowanie zarządzające umożliwiające:
- zarzadzanie infrastruktura serwerów i storage bez udziału dedykowanego agenta

- przedstawianie graficznej reprezentacji zarządzanych urządzeń

- możliwość skalowania do minimum 1000 urządzeń

- obsługę szyfrowanej komunikacji z zarządzanymi urządzeniami, wsparcie dla NIST 800-131A oraz FIPS 140-2

- wsparcie dla certyfikatów SSL tzw self-signed oraz zewnętrznych

- udostępnianie szybkiego podgląd stanu środowiska
- udostępnianie podsumowania stanu dla każdego urządzenia
- tworzenie alertów przy zmianie stanu urządzenia

- monitorowanie oraz tracking zużycia energii przez monitorowane urządzenie, możliwość ustalania granicy zużycia energii,

- konsola zarzadzania oparta o HTML 5

- dostępność konsoli monitorującej na urządzeniach przenośnych ze wsparciem dla systemu Android oraz iOS, aplikacja musi umożliwiać włączenie wyłączenie oraz restart urządzenia, musi również mieć możliwość aktywowania diody lokacyjnej na urządzeniu,

- automatyczne wykrywanie dołączanych systemów oraz szczegółowa inwentaryzacja

- możliwość podnoszenia wersji oprogramowania dla komponentów zarządzanych serwerów w oparciu o repozytorium lokalne jak i zdalne dostepne na stronie producenta oferowanego rozwiązania

- definiowanie polityk zgodności wersji firmware komponentów zarządzanych urządzań

- definiowanie roli użytkowników oprogramowania

- obsługa REST API oraz Windows PowerShell

- obsługa SNMP, SYSLOG, Email Forwarding

- autentykacja użytkowników: centralna (możliwość definiowania wymaganego poziomu skomplikowania danych autentykacyjnych) oraz integracja z MS AD oraz obsługa single sign on oraz SAML

- obsługa tzw Forward Secrecy w komunikacji z zarządzanymi urządzeniami

- przedstawianie historycznych aktywności użytkowników

-blokowanie możliwości podłączenia innego systemu zarzadzania do urządzeń zarządzanych

	- tworzenie dziennika zdarzeń ukończonych sukcesem lub bledem, oraz zdarzeń bedacych w trakcie. Możliwość definiowania filtrów wyświetlanych zdarzeń z dziennika. Możliwość eksportu dziennika zdarzeń do pliku csv - Obsluga NTP - przesyłanie alertów do konsoli firm trzecich - tworzenie wzorców konfiguracji zarządzanych urządzeń (definiowanie przez konsole albo kopiowanie konfiguracji z już zaimplementowanych urządzeń) - instalowanie systemów operacyjnych oraz wirtalizatorów Vmware i Hyper-V. Wymagana jest integracja konsoli zarządzania z konsolą wirtualizatora tak, aby zarządzanie środowiskiem sprzętowym mogło odbywać się z konsoli wirtualizatora. Wymaga się możliwości instalacji systemu na przynajmniej 20 nodach jednocześnie - możliwość automatycznego tworzenia zgłoszeń w centrum serwisowym producenta dla określonych zdarzeń wraz z przesylem plików diagnostycznych, Producent serwera ponadto powinien mieć w swojej ofercie narzędzia integrujące zarządzanie infrastrukturą z następującymi produktami: VMware vCenter, Microsoft AdminCenter, Microsoft SystemCenter, RedHat CloudForms, Splunk.
Funkcje zabezpieczeń	Możliwość instalacji czujnika otwarcia obudowy zintegrowanego z modułem zarządzania serwerem, hasło włączania, hasło administratora, moduł RoT (umieszczony na dedykowanej płytce I/O wspomnianej w sekcji Dodatkowe porty) wspierający TPM2.0 oraz Platform Firmware Resiliency (PFR)., Możliwość zainstalowania przedniego panelu zamykanego na klucz. Wbudowany w BIOS mechanizm umożliwiający usunięcie konfiguracji kart zarządzających, BIOS oraz danych ze wszystkich wewnętrznych urządzeń pamięci masowej. Możliwość automatycznego przywrócenia BIOS do wspieranej wersji w przypadku wykrycia nieautoryzowanej modyfikacji.
Urządzenia hot swap	Dyski twarde, zasilacze, wentylatory.
Obsługa	Możliwość instalacji serwera oraz serwisowania (instalacji oraz deinstalacji) komponentów takich jak: riser'ów PCIe, backplane'ów dysków twardych, kart rozszerzeń, wentylatorów, bez użycia dodatkowych narzędzi mechanicznych.

Diagnostyka	Możliwość przewidywania awarii dla procesorów, regulatorów napięcia, pamięci, dysków wewnętrznych, wentylatorów, zasilaczy, kontrolerów RAID Możliwość użycia aplikacji mobilnej na telefonie (iOS lub Android), do przeglądania awarii, konfigurowania ustawień i włączenia/wyłączenia serwera. Podłączenie telefonu powinno odbywać się poprzez dedykowany port USB na froncie serwera. Wymaga się aby serwer posiadał diody sygnalizacyjne awarię przy każdej kości pamięci RAM, każdej zatoce dyskowej, każdym zasilaczu.
Systemy operacyjne	Microsoft Windows Server 2022, 2025; Red Hat Enterprise Linux 9.x; SUSE Linux Enterprise Server 15 SP6; VMware vSphere (ESXi) 8.0 U3; Ubuntu 22.04, 24.04
Gwarancja	24 miesiące gwarancji producenta z oknem serwisowym 24x7, z reakcją NBD. Uszkodzone nośniki danych pozostają własnością zamawiającego. Możliwość wykupienia dodatkowego wsparcia, świadczonego przez producenta, z gwarantowanym czasem naprawy w ciągu 6 godzin. W przypadku braku funkcjonalności przewidywania awarii dla wszystkich komponentów wymienionych w punkcie Diagnostyka wymagane jest dostarczenie serwera nadmiarowego, mogącego zastąpić funkcjonalni jak i wydajnościowo wymagane powyżej maszyny. Wszystkie komponenty serwera powinny być sygnowane i zoptymalizowane do użycia przez producenta serwera..

7.4. Minimalne wymagania dotyczące oprogramowania backupowego

Oferowane rozwiązanie musi zapewniać:

- instalację na systemie Linux;
- zarządzanie z poziomu przeglądarki internetowej;
- możliwość wykonywania kopii zapasowych środowisk wirtualnych;
- możliwość wykonywania kopii przyrostowych;
- deduplikację blokową;
- kompresję danych;
- szyfrowanie danych;
- możliwość replikacji repozytoriów backupowych;
- możliwość automatycznego usuwania kopii zgodnie z polityką retencji;
- możliwość odtwarzania pojedynczych plików;
- możliwość odtworzenia całej maszyny wirtualnej;
- możliwość przywracania danych na inny serwer;

- obsługę harmonogramów wykonywania kopii zapasowych;
- możliwość uwierzytelniania administratorów;
- eksport logów do systemu SIEM lub menedżera logów;
- możliwość wykonywania kopii konfiguracji własnej.

8. Usługa katalogowa oraz system zarządzania tożsamością i dostępem (IAM)

8.1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa, wdrożenie oraz konfiguracja usługi katalogowej oraz systemu zarządzania tożsamością i dostępem (Identity and Access Management – IAM), umożliwiającego centralne zarządzanie użytkownikami, grupami, uwierzytelnianiem oraz autoryzacją dostępu do zasobów teleinformatycznych Zamawiającego.

Rozwiązanie powinno umożliwiać centralne zarządzanie tożsamościami użytkowników oraz integrację z pozostałymi elementami infrastruktury teleinformatycznej dostarczanej w ramach niniejszego postępowania, w szczególności z systemem operacyjnym serwerów, urządzeniami klasy NGFW, systemem VPN, systemem monitorowania infrastruktury oraz systemem SIEM.

8.2. Minimalne wymagania funkcjonalne

Oferowane rozwiązanie musi zapewniać co najmniej:

- centralne zarządzanie kontami użytkowników;
- centralne zarządzanie grupami użytkowników;
- możliwość tworzenia oraz zarządzania strukturą usługi katalogowej;
- możliwość definiowania polityk bezpieczeństwa użytkowników;
- możliwość definiowania polityk haseł, obejmujących między innymi minimalną długość, złożoność, historię oraz okres ważności haseł;
- możliwość wymuszania zmiany hasła przy pierwszym logowaniu;
- możliwość blokowania kont użytkowników po określonej liczbie nieudanych prób logowania;
- centralne uwierzytelnianie użytkowników;
- centralną autoryzację dostępu do zasobów;
- obsługę protokołów LDAP, LDAPS oraz Kerberos lub równoważnych;
- możliwość integracji z systemami operacyjnymi Microsoft Windows;
- możliwość integracji z urządzeniami sieciowymi wykorzystującymi zewnętrzne usługi uwierzytelniania;
- możliwość integracji z systemami VPN;
- możliwość integracji z urządzeniami klasy NGFW;
- możliwość wdrożenia mechanizmu jednokrotnego logowania (Single Sign-On – SSO);
- możliwość wdrożenia uwierzytelniania wieloskładnikowego (MFA) dla administratorów oraz wskazanych użytkowników;

- rejestrowanie zdarzeń związanych z logowaniem użytkowników oraz zmianami konfiguracji;
- możliwość przekazywania logów do systemu SIEM lub centralnego menedżera logów;
- możliwość tworzenia raportów dotyczących użytkowników, grup oraz aktywności.

8.3. Minimalne wymagania techniczne

Rozwiązanie musi:

- być objęte wsparciem producenta;
- umożliwiać zarządzanie z poziomu graficznego interfejsu administracyjnego;
- umożliwiać wykonywanie kopii zapasowych konfiguracji;
- umożliwiać odtworzenie konfiguracji po awarii;
- umożliwiać bezpieczną administrację z wykorzystaniem szyfrowanych połączeń;
- umożliwiać integrację z systemami monitorowania infrastruktury;
- umożliwiać integrację z systemem poczty elektronicznej w zakresie powiadomień administracyjnych;
- umożliwiać synchronizację tożsamości z usługą katalogową działającą w środowisku chmurowym, jeżeli Zamawiający zdecyduje się na jej wykorzystanie w okresie eksploatacji rozwiązania;
- zapewniać możliwość dalszej rozbudowy bez konieczności wymiany całego rozwiązania.

8.4. Wymagania dotyczące uwierzytelniania wieloskładnikowego (MFA)

Rozwiązanie musi umożliwiać wdrożenie mechanizmu uwierzytelniania wieloskładnikowego (MFA) dla administratorów oraz użytkowników wskazanych przez Zamawiającego.

Mechanizm MFA powinien umożliwiać wykorzystanie powszechnie stosowanych metod uwierzytelniania, takich jak:

- aplikacje generujące jednorazowe kody (TOTP);
- powiadomienia Push;
- klucze bezpieczeństwa zgodne z FIDO2/WebAuthn lub równoważne;
- jednorazowe kody weryfikacyjne.

Administrator powinien mieć możliwość definiowania zasad stosowania MFA dla wybranych użytkowników lub grup użytkowników.

9. Zarządzalny przełącznik sieciowy

9.1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa, instalacja oraz konfiguracja 3 szt. zarządzalnego przełącznika sieciowego przeznaczonego do pracy w infrastrukturze lokalnej sieci komputerowej Zamawiającego.

Każde urządzenie musi zapewniać możliwość budowy wydajnej i bezpiecznej sieci LAN, w tym obsługę segmentacji ruchu, zasilania urządzeń końcowych poprzez Ethernet oraz integracji z pozostałymi elementami infrastruktury sieciowej.

9.2. Minimalne wymagania funkcjonalne

Oferowane urządzenie musi zapewniać co najmniej:

- pracę w warstwie drugiej modelu OSI (L2);
- obsługę funkcji zarządzania siecią;
- możliwość konfiguracji poprzez interfejs webowy;
- możliwość konfiguracji poprzez interfejs CLI lub równoważny;
- obsługę sieci VLAN zgodnie ze standardem IEEE 802.1Q;
- możliwość tworzenia wielu logicznych segmentów sieci;
- obsługę trunkowania portów;
- obsługę agregacji połączeń (LACP zgodnie z IEEE 802.3ad);
- obsługę mechanizmów kontroli dostępu do sieci;
- obsługę mechanizmów Quality of Service (QoS);
- możliwość priorytetyzacji ruchu sieciowego;
- obsługę protokołu STP/RSTP/MSTP lub równoważnego;
- możliwość monitorowania wykorzystania portów;
- możliwość tworzenia kopii zapasowej konfiguracji;
- możliwość odtworzenia konfiguracji urządzenia;
- możliwość aktualizacji oprogramowania urządzenia;
- możliwość przesyłania logów do zewnętrznego systemu SIEM lub menedżera logów;
- możliwość monitorowania parametrów pracy urządzenia.

9.3. Minimalne wymagania techniczne

Oferowany przełącznik musi być fabrycznie nowy i spełniać minimum następujące wymagania:

Obudowa

- urządzenie przeznaczone do montażu w szafie Rack 19";
- wysokość maksymalnie 1U;
- wyposażone w elementy umożliwiające montaż w szafie Rack.

Porty sieciowe

Urządzenie musi posiadać:

- minimum 48 portów Ethernet RJ-45 10/100/1000 Mb/s;
- minimum 4 porty uplink SFP+ o przepustowości 10 Gb/s;
- możliwość jednoczesnej pracy wszystkich portów.

Zasilanie urządzeń końcowych PoE

Przełącznik musi posiadać funkcję Power over Ethernet:

- zgodność minimum ze standardem IEEE 802.3at (PoE+);
- możliwość zasilania urządzeń końcowych, w szczególności punktów dostępowych WiFi, telefonów IP oraz kamer IP;
- całkowity budżet mocy PoE nie mniejszy niż 300 W.

Wydajność

Urządzenie musi zapewniać minimum:

- przepustowość przełączania nie mniejszą niż 100 Gb/s;
- wydajność przekazywania pakietów nie mniejszą niż 70 Mpps;
- tablicę adresów MAC o pojemności minimum 16 000 wpisów.

9.4. Bezpieczeństwo

Przełącznik musi umożliwiać:

- filtrowanie ruchu na podstawie adresów MAC;
- kontrolę dostępu do portów;
- obsługę uwierzytelniania 802.1X lub równoważnego;
- ograniczanie dostępu do sieci nieautoryzowanym urządzeniom;
- izolację portów;
- zabezpieczenie przed pętlami sieciowymi;
- ochronę przed podstawowymi atakami typu broadcast storm;
- integrację z usługą katalogową w zakresie uwierzytelniania administratorów, jeżeli funkcjonalność jest wspierana.

9.5. Zarządzanie i monitoring

Urządzenie musi umożliwiać:

- zarządzanie lokalne;
- zarządzanie zdalne;
- konfigurację przez HTTPS;
- konfigurację przez SSH lub równoważny bezpieczny protokół;
- obsługę SNMP minimum w wersji 2c oraz 3;
- generowanie komunikatów Syslog;
- monitorowanie stanu portów;

- monitorowanie wykorzystania przepustowości;
- monitorowanie podstawowych parametrów pracy urządzenia.

10. System klasy SIEM (Security Information and Event Management)

10.1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa, wdrożenie oraz konfiguracja systemu klasy SIEM (Security Information and Event Management), przeznaczonego do centralnego zbierania, analizy oraz korelacji zdarzeń bezpieczeństwa pochodzących z infrastruktury teleinformatycznej Zamawiającego.

System musi umożliwiać wykrywanie zdarzeń mogących wskazywać na wystąpienie incydentów bezpieczeństwa, generowanie alertów oraz wspomaganie procesu analizy i reagowania na zagrożenia.

Zamawiający dopuszcza realizację funkcjonalności określonych w niniejszej pozycji oraz w pozycji 13 (Menedżer logów) przy wykorzystaniu jednego rozwiązania, pod warunkiem zapewnienia wszystkich funkcjonalności wymaganych dla obu pozycji.

10.2. Minimalne wymagania funkcjonalne

Oferowane rozwiązanie musi zapewniać co najmniej:

- centralne gromadzenie zdarzeń bezpieczeństwa z wielu źródeł;
- odbieranie logów z urządzeń sieciowych, systemów operacyjnych, aplikacji oraz systemów bezpieczeństwa;
- normalizację oraz indeksowanie zdarzeń;
- wyszukiwanie zdarzeń według różnych kryteriów;
- korelację zdarzeń pochodzących z różnych źródeł;
- wykrywanie anomalii oraz zdarzeń mogących świadczyć o naruszeniu bezpieczeństwa;
- definiowanie reguł detekcji zagrożeń;
- generowanie alertów bezpieczeństwa;
- możliwość definiowania poziomów ważności zdarzeń;
- tworzenie dashboardów bezpieczeństwa;
- tworzenie raportów dotyczących bezpieczeństwa;
- analizę aktywności użytkowników;
- analizę zdarzeń uwierzytelniania;
- analizę zdarzeń pochodzących z urządzeń sieciowych;
- analizę zdarzeń pochodzących z systemów ochrony endpointów;
- możliwość przekazywania powiadomień o incydentach;
- możliwość archiwizacji zdarzeń;
- możliwość ograniczania dostępu administratorów do określonych danych.

10.3. Minimalne wymagania dotyczące źródeł danych

System musi umożliwiać odbieranie zdarzeń co najmniej z:

- systemów operacyjnych Microsoft Windows;
- systemów Linux;
- urządzeń klasy NGFW;
- urządzeń UTM;
- przełączników sieciowych;
- punktów dostępowych WiFi;
- systemów ochrony endpointów;
- systemów wykonywania kopii zapasowych;
- systemów wirtualizacji;
- systemów monitorowania infrastruktury;
- usług katalogowych;
- aplikacji wspierających protokoły logowania.

10.4. Minimalne wymagania techniczne

System musi:

- umożliwiać pracę w środowisku lokalnym Zamawiającego;
- umożliwiać instalację na serwerze fizycznym lub wirtualnym;
- umożliwiać rozbudowę w przyszłości;
- posiadać mechanizmy zabezpieczające dostęp administracyjny;
- umożliwiać zarządzanie z wykorzystaniem przeglądarki internetowej;
- umożliwiać wykonywanie kopii zapasowych konfiguracji;
- umożliwiać eksport konfiguracji;
- umożliwiać integrację z zewnętrznymi systemami poprzez standardowe mechanizmy komunikacji;
- umożliwiać komunikację z wykorzystaniem protokołów Syslog, API lub równoważnych;
- umożliwiać integrację z systemami monitorowania infrastruktury.

10.5. Wymagania dotyczące detekcji i obsługi incydentów

System musi umożliwiać:

- tworzenie własnych reguł wykrywania zdarzeń;
- definiowanie warunków powodujących wygenerowanie alertu;
- klasyfikowanie zdarzeń według poziomu ryzyka;
- śledzenie historii zdarzenia;
- analizę powiązanych zdarzeń;

- identyfikację źródła zdarzenia;
- identyfikację użytkownika powiązanego ze zdarzeniem;
- eksport wyników analizy.

System powinien umożliwiać wykorzystanie gotowych reguł detekcji zagrożeń dostarczanych przez producenta lub społeczność użytkowników rozwiązania.

10.6. Wymagania dotyczące raportowania

System musi umożliwiać:

- tworzenie raportów okresowych;
- tworzenie raportów dotyczących incydentów bezpieczeństwa;
- tworzenie raportów dotyczących aktywności użytkowników;
- tworzenie raportów dotyczących zdarzeń administracyjnych;
- eksport raportów co najmniej do formatów PDF oraz CSV.

11. Szafa Rack 19"

11.1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa, montaż oraz wyposażenie szafy teleinformatycznej Rack 19" przeznaczonej do instalacji urządzeń aktywnych oraz pasywnych infrastruktury teleinformatycznej Zamawiającego.

Szafa musi umożliwiać bezpieczną instalację, eksploatację oraz późniejszą rozbudowę infrastruktury serwerowej i sieciowej.

11.2. Minimalne wymagania funkcjonalne

Oferowana szafa musi zapewniać:

- możliwość montażu urządzeń w standardzie Rack 19";
- możliwość instalacji urządzeń aktywnych, serwerów, przełączników, paneli krosowych oraz urządzeń zasilających;
- możliwość prowadzenia oraz uporządkowania okablowania strukturalnego;
- możliwość organizacji pionowej i poziomej przewodów;
- możliwość zabezpieczenia dostępu do urządzeń poprzez zamykane drzwi;
- możliwość rozbudowy wyposażenia wewnętrznego;
- możliwość montażu akcesoriów dodatkowych, takich jak:
  - listwy zasilające PDU,
  - organizery kabli,
  - półki Rack,
  - panele wentylacyjne,
  - panele krosowe.

11.3. Minimalne wymagania techniczne

Szafa musi spełniać następujące wymagania:

- typ szafy: wolnostojąca
- pojemność stelaża: 42U
- szerokość: 600mm
- głębokość: 1000mm
- maksymalna waga przeznaczona do umieszczenia/przechowywania przez urządzenie: 1500 kg
- materiał wykonania: stal
- rodzaj ramy: zamknięty
- konstrukcja drzwi tylnych: metal
- konstrukcja drzwi przednich: szkło hartowane
- zdejmowalne drzwi tylne: nie
- zdejmowalne drzwi przednie: tak
- zdejmowalne panele boczne: tak
- regulowane wymiary wejść kablowych na pokrywę górną i płytę dolną: tak
- możliwość otwierania drzwi na lewą lub prawą stronę: tak
- zamek: tak
- zamek klucza drzwi przednich: tak
- zamek na klucz panelu bocznego: tak
- relingi: tak
- regulowane nóżki (stopy): tak

12. Serwer NAS (Network Attached Storage)

12.1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa, instalacja, konfiguracja oraz uruchomienie serwera NAS przeznaczonego do centralnego przechowywania danych, udostępniania zasobów sieciowych oraz realizacji zadań związanych z przechowywaniem kopii zapasowych i danych operacyjnych Zamawiającego.

Urządzenie musi zapewniać wysoką dostępność, możliwość rozbudowy przestrzeni dyskowej oraz bezpieczne zarządzanie przechowywanymi danymi.

12.2. Minimalne wymagania funkcjonalne I techniczne

Oferowane rozwiązanie musi zapewniać co najmniej:

Procesor	Wielordzeniowy procesor o architekturze 64-bitowej osiągający minimum 4 tysiące punktów w teście PassMark.
Obudowa	Typu rack o wysokości maksymalnie 2U wraz z szynami przesuwnymi umożliwiającymi montaż w szafie rack w zestawie.
Pamięć RAM	Minimum 8GB DDR4 ECC. Model pamięci musi znajdować się na oficjalnej liście zgodności producenta – nie zezwala się na stosowanie zamienników.
Ilość obsługiwanych dysków	Minimum 8 dysków o maksymalnej pojemności nie mniejszej niż 20TB każdy, po podłączeniu modułów rozszerzających minimum 12 dysków.
Zainstalowane dyski	4 dyski o pojemności 16TB każdy zgodnych z listą kompatybilności oferowanego serwera oraz charakteryzujących się następującymi parametrami: - prędkość obrotowa: minimum 7200 RPM, - gwarancja: minimum 36 miesięcy, - MTBF: minimum 1 milion, - możliwość aktualizacji oprogramowania dysku bezpośrednio z poziomu systemu operacyjnego serwera NAS.
Interfejsy sieciowe	Minimum 4 porty 1GbE RJ-45. Minimum 2 porty 10GbE RJ-45. Obsługa agregacji łączy.
Porty	Minimum 2 porty USB 3.2. Minimum 1 gniazdo rozszerzenia służące do podłączania jednostek rozszerzających.
Wskaźniki LED	Status, HDD, zasilanie, LAN
Obsługa RAID	Podstawowy, RAID 0, 1, 5, 6, 10. Obsługa dysków zapasowych typu hot spare.
Funkcje RAID	Możliwość zwiększania pojemności poprzez wymianę dysków na większe. Migracja poziomu RAID w trybie online dla minimum RAID 1 i RAID 5.
Szyfrowanie	Możliwość szyfrowania wybranych udziałów sieciowych.
Protokoły	SMB, AFP, NFS, FTP, WebDAV, CalDAV, iSCSI, Telnet, SSH, SNMP
Usługi	1. Serwer VPN, Stacja monitoringu, Windows ACL, Integracja z Windows Active Directory, Firewall, Serwer plików, Szyfrowana replikacja zdalna na kilka serwerów w tym samym czasie, Usługa DDNS, Serwer i klient LDAP, Możliwość utworzenia kilku wolumenów w obrębie jednej macierzy RAID, migawki, możliwość tworzenia i uruchamiania maszyn wirtualnych bezpośrednio w systemie bez wykorzystywania zewnętrznych wirtualizatorów 2. Wykonywanie kopii zapasowych typu bare-metal komputerów lokalnych z systemem Windows 10 i 11 według harmonogramu z możliwością

	zarządzania tworzeniem zadań kopii zapasowych z poziomu centralnej konsoli dostępnej lokalnie oraz zdalnie, przywracania pojedynczych plików, folderów oraz całych obrazów dysku. Kopia musi być wykonywana w trybie przyrostowym z możliwością przechowywania minimum 32 wersji i zarządzania ich przechowywaniem w sposób automatyczny poprzez dedykowany algorytm. Dane z kopii zapasowych muszą być redukowane poprzez globalną deduplikację po stronie miejsca przechowywania. Licencja musi umożliwiać podłączanie kolejnych komputerów do systemu kopii zapasowej bez limitu. 3. Możliwość utworzenia klastra wysokiej dostępności (HA) z dwóch identycznych urządzeń pracującego minimum w trybie aktywny-pasywny. Wymagane jest, aby klaster obsługiwał w pełni automatyczne przełączanie awaryjne bez ingerencji administratora.
Zarządzanie dyskami	SMART, sprawdzanie złych sektorów.
Język GUI	Polski
Gwarancja i serwis	Minimum 24 miesiące gwarancji.
Waga bez dysków	Maksymalnie 15 kg
Typowy pobór mocy podczas pracy	Maksymalnie 130W
Certyfikaty	CE
System plików	Dyski wewnętrzne: BTRFS
Szyfrowanie	Mechanizm szyfrowania sprzętowego
Zasilacz	Redundantny zasilacz o mocy minimum 300W.
Chłodzenie	Minimum 2 wentylatory z możliwością regulowania prędkości obrotowej.

13. Centralny menedżer logów (Log Management)

13.1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa, wdrożenie oraz konfiguracja centralnego systemu zarządzania logami (Log Management), przeznaczonego do gromadzenia, przechowywania, indeksowania oraz udostępniania danych pochodzących z systemów i urządzeń infrastruktury teleinformatycznej Zamawiającego.

System musi umożliwiać centralizację logów z wielu źródeł oraz zapewniać możliwość ich późniejszego wyszukiwania, analizy oraz wykorzystania na potrzeby administracji, audytu i bezpieczeństwa.

Zamawiający dopuszcza realizację funkcjonalności określonych w niniejszej pozycji oraz w pozycji 10 (System SIEM) przy wykorzystaniu jednego rozwiązania, pod warunkiem zapewnienia wszystkich wymaganych funkcjonalności.

13.2. Minimalne wymagania funkcjonalne

Oferowane rozwiązanie musi zapewniać co najmniej:

- centralne odbieranie logów z wielu źródeł;
- przechowywanie logów w jednym repozytorium;
- indeksowanie zgromadzonych danych;
- szybkie wyszukiwanie zdarzeń według określonych kryteriów;
- filtrowanie zdarzeń według:
  - czasu,
  - źródła,
  - użytkownika,
  - adresu IP,
  - typu zdarzenia;
- możliwość definiowania źródeł logów;
- możliwość kategoryzacji oraz tagowania danych;
- możliwość definiowania okresu retencji danych;
- możliwość archiwizacji danych;
- możliwość eksportowania wybranych danych;
- możliwość tworzenia widoków oraz zestawień administracyjnych;
- możliwość tworzenia dashboardów prezentujących stan systemów;
- możliwość ograniczenia dostępu do logów według uprawnień użytkowników;
- możliwość rejestrowania zdarzeń administracyjnych systemu;
- możliwość integracji z systemem SIEM.

13.3. Minimalne wymagania dotyczące obsługiwanych źródeł logów

System musi umożliwiać odbieranie logów co najmniej z:

- systemów operacyjnych Microsoft Windows;
- systemów Linux;
- urządzeń klasy NGFW;
- urządzeń UTM;
- przełączników sieciowych;
- punktów dostępowych WiFi;
- usług katalogowych;

- systemów ochrony endpointów;
- systemów wykonywania kopii zapasowych;
- systemów NAS;
- systemów wirtualizacji;
- systemów monitorowania infrastruktury;
- aplikacji wykorzystujących standardowe mechanizmy logowania.

13.4. Minimalne wymagania techniczne

System musi:

- umożliwiać instalację w środowisku lokalnym Zamawiającego;
- umożliwiać instalację na serwerze fizycznym lub wirtualnym;
- umożliwiać rozbudowę przestrzeni przechowywania logów;
- umożliwiać konfigurację retencji danych;
- umożliwiać kompresję danych;
- umożliwiać zarządzanie z poziomu przeglądarki internetowej;
- posiadać mechanizmy kontroli dostępu administratorów;
- umożliwiać wykonywanie kopii zapasowych konfiguracji;
- umożliwiać odtworzenie konfiguracji po awarii;
- umożliwiać eksport danych w standardowych formatach.

13.5. Wymagania dotyczące komunikacji i integracji

System musi umożliwiać odbiór danych co najmniej poprzez:

- Syslog;
- Syslog over TLS lub rozwiązanie równoważne;
- API;
- dedykowane konektory lub agenty producenta.

System musi umożliwiać przekazywanie danych do innych systemów poprzez:

- API;
- Syslog;
- mechanizmy eksportu danych.

13.6. Minimalne wymagania dotyczące przechowywania danych

System musi umożliwiać:

- przechowywanie logów przez okres określony przez Zamawiającego;
- konfigurację różnych okresów retencji dla różnych źródeł danych;
- automatyczne usuwanie danych zgodnie z przyjętą polityką retencji;
- archiwizację danych historycznych;

- odtwarzanie dostępu do danych archiwalnych.

Wykonawca zobowiązany jest do konfiguracji parametrów retencji zgodnie z wymaganiami Zamawiającego.

13.7. Zarządzanie i monitoring systemu

System musi umożliwiać:

- monitorowanie stanu działania usługi;
- monitorowanie ilości odbieranych logów;
- monitorowanie błędów komunikacji ze źródłami danych;
- generowanie alertów administracyjnych;
- rejestrowanie działań administratorów;
- integrację z systemem monitorowania infrastruktury.

14. System monitorowania infrastruktury teleinformatycznej (NMS)

14.1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa, wdrożenie oraz konfiguracja systemu monitorowania infrastruktury teleinformatycznej (Network Monitoring System – NMS), przeznaczonego do bieżącego monitorowania dostępności, wydajności oraz stanu technicznego urządzeń i usług wykorzystywanych przez Zamawiającego.

System musi umożliwiać centralne monitorowanie infrastruktury IT, generowanie alarmów o nieprawidłowościach oraz prezentację aktualnego stanu środowiska teleinformatycznego.

14.2. Minimalne wymagania funkcjonalne

Oferowane rozwiązanie musi zapewniać co najmniej:

- centralne monitorowanie infrastruktury IT;
- monitorowanie urządzeń sieciowych;
- monitorowanie serwerów fizycznych i wirtualnych;
- monitorowanie usług systemowych;
- monitorowanie dostępności urządzeń;
- monitorowanie parametrów wydajnościowych;
- generowanie alertów o awariach i przekroczeniu wartości progowych;
- prezentację aktualnego stanu infrastruktury;
- tworzenie dashboardów administracyjnych;
- tworzenie raportów;
- gromadzenie danych historycznych;
- analizę trendów wykorzystania zasobów;
- możliwość definiowania własnych reguł monitorowania;

- możliwość definiowania progów alarmowych;
- możliwość konfiguracji zależności pomiędzy monitorowanymi elementami;
- możliwość potwierdzania i obsługi zgłoszonych alarmów.

14.3. Minimalne wymagania dotyczące monitorowanych elementów

System musi umożliwiać monitorowanie co najmniej:

Urządzenia sieciowe

- przełączników sieciowych;
- urządzeń klasy NGFW;
- urządzeń klasy UTM;
- punktów dostępowych WiFi;
- urządzeń wykorzystujących protokoły SNMP.

Systemy serwerowe

- serwerów fizycznych;
- serwerów wirtualnych;
- hostów wirtualizacji;
- systemów operacyjnych Microsoft Windows;
- systemów operacyjnych Linux.

Urządzenia infrastruktury

- urządzeń NAS;
- urządzeń backupowych;
- UPS;
- innych urządzeń posiadających interfejs monitorowania.

Usługi

System musi umożliwiać monitorowanie między innymi:

- dostępności usług sieciowych;
- dostępności portów TCP/UDP;
- usług HTTP/HTTPS;
- usług DNS;
- usług katalogowych;
- usług bazodanowych, jeżeli występują;
- usług systemowych.

14.4. Minimalne wymagania techniczne

System musi:

- umożliwiać pracę w środowisku lokalnym Zamawiającego;

- umożliwiać instalację na serwerze fizycznym lub wirtualnym;
- posiadać architekturę umożliwiającą dalszą rozbudowę;
- umożliwiać zarządzanie przez przeglądarkę internetową;
- umożliwiać tworzenie wielu kont administracyjnych;
- umożliwiać definiowanie różnych poziomów uprawnień;
- umożliwiać wykonywanie kopii konfiguracji;
- umożliwiać odtworzenie konfiguracji po awarii;
- umożliwiać przechowywanie danych historycznych;
- umożliwiać eksport danych.

14.5. Obsługiwane mechanizmy monitorowania

System musi umożliwiać monitorowanie urządzeń i usług poprzez minimum:

- SNMP w wersji minimum v2c oraz v3;
- ICMP;
- protokoły TCP/UDP;
- agentów instalowanych na systemach operacyjnych;
- API urządzeń i systemów;
- mechanizmy skryptowe umożliwiające rozszerzenie monitoringu.

14.6. Alertowanie i powiadomienia

System musi umożliwiać:

- definiowanie warunków generowania alarmów;
- określanie poziomów ważności zdarzeń;
- automatyczne powiadamianie administratorów;
- obsługę powiadomień poprzez minimum:
    - pocztę elektroniczną,
    - komunikaty systemowe,
    - integrację poprzez API lub rozwiązanie równoważne;
- rejestrowanie historii alarmów;
- eskalację powiadomień

14.7. Wizualizacja i raportowanie

System musi umożliwiać:

- tworzenie własnych dashboardów;
- prezentację stanu urządzeń w czasie rzeczywistym;
- prezentację wykresów historycznych;
- generowanie raportów dotyczących:

- dostępności urządzeń,
- wykorzystania zasobów,
- występujących awarii,
- trendów obciążenia.

14.8. Integracja z infrastrukturą Zamawiającego

System musi umożliwiać integrację z:

- systemem IAM;
- systemem SIEM;
- centralnym menedżerem logów;
- urządzeniami klasy NGFW;
- urządzeniami UTM;
- systemem wirtualizacji;
- systemem wykonywania kopii zapasowych;
- urządzeniami NAS;
- przełącznikami sieciowymi;
- systemami operacyjnymi serwerów.

15. Platforma wirtualizacyjna

15.1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa, wdrożenie oraz konfiguracja platformy wirtualizacyjnej przeznaczonej do uruchamiania i zarządzania maszynami wirtualnymi w infrastrukturze teleinformatycznej Zamawiającego.

Platforma musi umożliwiać konsolidację zasobów serwerowych, centralne zarządzanie środowiskiem wirtualnym oraz zapewniać możliwość uruchamiania systemów operacyjnych i aplikacji wykorzystywanych przez Zamawiającego.

15.2. Minimalne wymagania funkcjonalne

Oferowana platforma musi zapewniać co najmniej:

- możliwość tworzenia i uruchamiania maszyn wirtualnych;
- możliwość zarządzania zasobami procesora, pamięci RAM oraz przestrzeni dyskowej dla maszyn wirtualnych;
- możliwość tworzenia, uruchamiania, zatrzymywania oraz restartowania maszyn wirtualnych;
- możliwość wykonywania migawek (snapshotów) maszyn wirtualnych;
- możliwość klonowania maszyn wirtualnych;
- możliwość migracji maszyn wirtualnych;
- możliwość zarządzania zasobami wirtualnymi z poziomu centralnego interfejsu administracyjnego;

- możliwość zarządzania przez przeglądarkę internetową;
- możliwość definiowania ról i uprawnień administratorów;
- możliwość integracji z usługą katalogową Zamawiającego;
- możliwość rejestrowania zdarzeń administracyjnych;
- możliwość integracji z systemem monitorowania infrastruktury;
- możliwość integracji z systemem SIEM lub centralnym menedżerem logów;
- możliwość wykonywania kopii zapasowych maszyn wirtualnych z wykorzystaniem dostarczanego systemu backupowego.

15.3. Minimalne wymagania dotyczące obsługi maszyn wirtualnych

Platforma musi obsługiwać:

- systemy operacyjne Microsoft Windows Server;
- systemy operacyjne Microsoft Windows dla stacji roboczych;
- systemy operacyjne Linux;
- systemy wykorzystujące architekturę x86-64.

Platforma musi umożliwiać:

- przydzielanie zasobów CPU;
- przydzielanie pamięci RAM;
- przydzielanie przestrzeni dyskowej;
- konfigurację wirtualnych kart sieciowych;
- konfigurację wirtualnych przełączników sieciowych;
- obsługę urządzeń wirtualnych.

15.4. Minimalne wymagania dotyczące zarządzania

Platforma musi umożliwiać:

- centralne zarządzanie środowiskiem wirtualnym;
- zarządzanie wieloma hostami wirtualizacji, jeżeli środowisko zostanie rozbudowane;
- tworzenie kont administratorów;
- definiowanie poziomów dostępu;
- rejestrowanie działań administratorów;
- wykonywanie kopii konfiguracji;
- odtwarzanie konfiguracji;
- aktualizację komponentów platformy;
- monitorowanie wykorzystania zasobów.

15.5. Minimalne wymagania dotyczące sieci

Platforma musi umożliwiać:

- tworzenie wirtualnych przełączników sieciowych;
- separację ruchu poprzez VLAN zgodnie z IEEE 802.1Q;
- konfigurację wielu interfejsów sieciowych;
- integrację z przełącznikami sieciowymi;
- integrację z urządzeniami klasy NGFW;
- obsługę komunikacji pomiędzy maszynami wirtualnymi oraz siecią fizyczną.

15.6. Minimalne wymagania dotyczące pamięci masowej

Platforma musi umożliwiać:

- obsługę lokalnych zasobów dyskowych;
- obsługę przestrzeni dyskowych udostępnianych przez sieć;
- obsługę magazynów danych dla maszyn wirtualnych;
- migrację maszyn pomiędzy zasobami dyskowymi;
- wykonywanie migawek maszyn wirtualnych;
- integrację z systemem wykonywania kopii zapasowych.

15.7. Wymagania dotyczące bezpieczeństwa

Platforma musi zapewniać:

- mechanizmy kontroli dostępu administratorów;
- możliwość integracji z usługą katalogową;
- możliwość stosowania silnych haseł;
- możliwość stosowania uwierzytelniania wieloskładnikowego lub integracji z takim mechanizmem;
- szyfrowanie komunikacji administracyjnej;
- rejestrowanie zdarzeń administracyjnych;
- możliwość przekazywania logów do systemu SIEM lub menedżera logów.

15.8. Wymagania dotyczące wysokiej dostępności i rozbudowy

Platforma musi umożliwiać:

- dalszą rozbudowę środowiska;
- dodawanie kolejnych hostów wirtualizacji;
- centralne zarządzanie wieloma hostami;
- tworzenie środowiska odpornego na awarie poprzez mechanizmy dostępne dla danego rozwiązania.

Jeżeli rozwiązanie wspiera mechanizmy wysokiej dostępności (HA), Wykonawca zobowiązany jest do ich konfiguracji zgodnie z wymaganiami Zamawiającego.

16. System operacyjny serwerowy

16.1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa licencji systemu operacyjnego serwerowego wraz z wymaganymi licencjami dostępowymi, przeznaczonego do instalacji na serwerach fizycznych lub maszynach wirtualnych wykorzystywanych w infrastrukturze teleinformatycznej Zamawiającego.

System musi umożliwiać realizację usług serwerowych, w szczególności usług katalogowych, zarządzania użytkownikami, uwierzytelniania oraz integracji z pozostałymi elementami infrastruktury IT Zamawiającego.

Zamawiający aktualnie korzysta z oprogramowania typu Microsoft Windows Server 2022 Standard i wymagana dostarczenia licencji na oprogramowanie Microsoft Windows Server 2025 Standard lub nowszy lub równoważny serwerowy system operacyjny do instalacji na dostarczanym w ramach zamówienia serwerze. Wraz z systemem należy dostarczyć licencje dostępowe dla 10 użytkowników.

16.2. Minimalne wymagania funkcjonalne

Oferowany system operacyjny musi zapewniać co najmniej:

- możliwość instalacji na platformie fizycznej oraz wirtualnej;
- obsługę architektury x86-64;
- możliwość uruchamiania usług serwerowych;
- obsługę usług katalogowych;
- możliwość centralnego zarządzania użytkownikami i grupami;
- możliwość definiowania polityk bezpieczeństwa;
- możliwość zarządzania uprawnieniami użytkowników;
- możliwość integracji z urządzeniami sieciowymi wykorzystującymi mechanizmy LDAP/Kerberos lub równoważne;
- możliwość integracji z systemami monitorowania infrastruktury;
- możliwość integracji z systemami logowania i analizy zdarzeń;
- możliwość wykonywania kopii zapasowych konfiguracji oraz danych systemowych;
- możliwość aktualizacji bezpieczeństwa dostarczanych przez producenta.

16.3. Minimalne wymagania dotyczące usług katalogowych

System musi umożliwiać uruchomienie usługi katalogowej zapewniającej:

- centralne zarządzanie kontami użytkowników;
- centralne zarządzanie grupami;
- zarządzanie komputerami i urządzeniami w domenie;
- stosowanie zasad grupowych (Group Policy) lub rozwiązania równoważnego;
- centralne zarządzanie politykami bezpieczeństwa;
- uwierzytelnianie użytkowników;

- integrację z aplikacjami i urządzeniami wykorzystującymi standardowe mechanizmy katalogowe.

16.4. Minimalne wymagania dotyczące bezpieczeństwa

System musi umożliwiać:

- stosowanie polityk haseł;
- wymuszanie złożoności haseł;
- definiowanie okresu ważności haseł;
- blokowanie kont po określonej liczbie nieudanych prób logowania;
- rejestrowanie zdarzeń systemowych i bezpieczeństwa;
- przekazywanie logów do centralnego systemu logowania;
- stosowanie szyfrowanej komunikacji administracyjnej;
- ograniczanie uprawnień użytkowników i administratorów.

16.5. Licencjonowanie

W ramach zamówienia Wykonawca zobowiązany jest dostarczyć:

- licencję systemu operacyjnego serwerowego w wersji umożliwiającej realizację wymaganych funkcji;
- licencje dostępowe dla użytkowników (User CAL) w liczbie określonej przez Zamawiającego.

Licencje muszą umożliwiać legalne użytkowanie systemu w środowisku Zamawiającego zgodnie z warunkami licencyjnymi producenta.

16.6. Integracja z infrastrukturą Zamawiającego

System musi umożliwiać integrację z:

- usługą katalogową i systemem IAM;
- platformą wirtualizacyjną;
- systemem wykonywania kopii zapasowych;
- systemem monitorowania infrastruktury;
- systemem SIEM;
- centralnym menedżerem logów;
- urządzeniami klasy NGFW oraz VPN.

16.7. Wymagania wdrożeniowe

Wykonawca zobowiązany jest do:

- dostarczenia wymaganych licencji;
- instalacji systemu operacyjnego na wskazanej platformie;
- konfiguracji podstawowych parametrów systemu;
- konfiguracji usług wymaganych przez Zamawiającego;
- konfiguracji integracji z usługą katalogową;

- konfiguracji polityk bezpieczeństwa;
- konfiguracji logowania zdarzeń;
- wykonania aktualizacji systemu;

17. Punkt dostępowy sieci bezprzewodowej WiFi

17.1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa, instalacja, konfiguracja oraz uruchomienie punktów dostępowych sieci bezprzewodowej WiFi przeznaczonych do zapewnienia bezpiecznego dostępu bezprzewodowego do infrastruktury sieciowej Zamawiającego.

Urządzenia muszą umożliwiać budowę wydajnej sieci bezprzewodowej klasy biznesowej, zapewniającej obsługę użytkowników, urządzeń mobilnych oraz urządzeń IoT

17.2. Minimalne wymagania funkcjonalne

Oferowany punkt dostępowy musi zapewniać co najmniej:

- pracę w standardzie WiFi 6 zgodnym z IEEE 802.11ax;
- jednoczesną pracę w dwóch pasmach częstotliwości:
  - 2,4 GHz,
  - 5 GHz;
- obsługę technologii MIMO;
- obsługę wielu użytkowników jednocześnie;
- możliwość automatycznego doboru kanałów radiowych;
- możliwość automatycznej optymalizacji parametrów pracy sieci bezprzewodowej;
- możliwość tworzenia wielu sieci SSID;
- możliwość przypisywania różnych polityk bezpieczeństwa do różnych sieci SSID;
- możliwość separacji ruchu użytkowników;
- możliwość obsługi sieci gościnnej;
- możliwość ograniczenia dostępu do zasobów wewnętrznych;
- możliwość zarządzania centralnego lub rozproszonego;
- możliwość aktualizacji oprogramowania urządzenia;
- możliwość monitorowania stanu urządzenia.

17.3. Minimalne wymagania techniczne

Punkt dostępowy musi być fabrycznie nowy i przeznaczony do pracy ciągłej.

Standardy radiowe

Urządzenie musi obsługiwać:

- IEEE 802.11ax (WiFi 6);
- IEEE 802.11a/b/g/n/ac lub rozwiązania równoważne zapewniające kompatybilność wsteczną.

Pasma radiowe

Urządzenie musi posiadać:

- minimum jedno radio dla pasma 2,4 GHz;
- minimum jedno radio dla pasma 5 GHz.

Przepustowość

Urządzenie musi zapewniać:

- obsługę kanałów radiowych o szerokości minimum 80 MHz;
- możliwość obsługi transmisji wielostrumieniowej;
- sumaryczną przepustowość radiową odpowiednią dla urządzenia klasy biznesowej WiFi 6.

Interfejs sieciowy

Urządzenie musi posiadać:

- minimum jeden port Ethernet 1 Gb/s lub szybszy;
- obsługę zasilania PoE zgodnie minimum z IEEE 802.3at;
- możliwość współpracy z przełącznikami PoE dostarczanymi w ramach niniejszego zamówienia.

Anteny

Urządzenie musi posiadać:

- wbudowany system antenowy lub możliwość zastosowania anten zewnętrznych;
- konfigurację antenową zapewniającą pracę wielostrumieniową.

17.4. Bezpieczeństwo sieci bezprzewodowej

Urządzenie musi umożliwiać:

- obsługę zabezpieczeń WPA2 oraz WPA3;
- obsługę uwierzytelniania IEEE 802.1X;
- integrację z usługami katalogowymi;
- integrację z mechanizmami RADIUS;
- separację klientów bezprzewodowych;
- izolację sieci gościnnej;
- szyfrowanie transmisji bezprzewodowej;
- stosowanie różnych polityk dostępu dla różnych sieci SSID.

17.5. Zarządzanie i monitoring

Urządzenie musi umożliwiać:

- konfigurację lokalną lub centralną;
- zarządzanie poprzez interfejs webowy;
- bezpieczne zarządzanie poprzez HTTPS/SSH lub rozwiązania równoważne;

- monitorowanie parametrów pracy;
- monitorowanie liczby podłączonych użytkowników;
- monitorowanie wykorzystania kanałów radiowych;
- generowanie zdarzeń systemowych;
- przesyłanie logów do centralnego systemu logowania;
- monitorowanie poprzez SNMP lub API.

17.6. Integracja z infrastrukturą Zamawiającego

Punkty dostępowe muszą umożliwiać integrację z:

- przełącznikami sieciowymi PoE;
- usługą katalogową Active Directory lub rozwiązaniem równoważnym;
- systemem IAM;
- systemami RADIUS;
- urządzeniami klasy NGFW;
- systemem monitorowania infrastruktury;
- systemem SIEM i centralnym menedżerem logów.

18. Zasilacz awaryjny UPS

18.1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa, instalacja oraz konfiguracja zasilacza awaryjnego UPS przeznaczonego do zapewnienia bezprzerwowego zasilania urządzeń infrastruktury teleinformatycznej Zamawiającego.

UPS musi zapewniać ochronę urządzeń przed skutkami zaniku zasilania, spadków i wzrostów napięcia oraz umożliwiać bezpieczne podtrzymanie pracy urządzeń IT do czasu przywrócenia zasilania podstawowego lub uruchomienia awaryjnego źródła zasilania.

18.2. Minimalne wymagania funkcjonalne

Oferowane urządzenie musi zapewniać co najmniej:

- bezprzerwowe zasilanie odbiorników podłączonych do UPS;
- ochronę przed zanikiem napięcia;
- ochronę przed przepięciami;
- stabilizację parametrów napięcia wyjściowego;
- automatyczne przełączenie na zasilanie bateryjne;
- automatyczny powrót do pracy z zasilania podstawowego po jego przywróceniu;
- możliwość bezpiecznego zamknięcia systemów IT w przypadku długotrwałego zaniku zasilania;
- możliwość monitorowania parametrów pracy urządzenia

18.3. Minimalne wymagania techniczne

UPS musi być fabrycznie nowy i przeznaczony do pracy ciągłej.

Topologia urządzenia

UPS musi posiadać:

- technologię on-line z podwójną konwersją (double conversion) lub rozwiązanie równoważne zapewniające ciągłą ochronę odbiorników;
- automatyczny układ obejścia (bypass) umożliwiający pracę awaryjną urządzenia.

Parametry mocy

Urządzenie musi zapewniać:

- moc pozorną minimum 3 kVA;
- moc czynną minimum 2,7 kW;
- możliwość współpracy z urządzeniami IT klasy serwerowej.

Obudowa

UPS musi posiadać:

- możliwość montażu w szafie Rack 19";
- wysokość maksymalnie 2U lub rozwiązanie równoważne umożliwiające montaż Rack;
- możliwość pracy w konfiguracji Rack lub Tower.

Akumulatory

UPS musi posiadać:

- wewnętrzne moduły bateryjne;
- możliwość wymiany akumulatorów;
- zabezpieczenie przed głębokim rozładowaniem;
- automatyczne ładowanie baterii.

18.4. Parametry elektryczne

UPS musi zapewniać:

- napięcie wejściowe zgodne ze standardem 230 V AC;
- napięcie wyjściowe 230 V AC;
- częstotliwość 50 Hz;
- stabilne parametry wyjściowe;
- zabezpieczenie przeciążeniowe;
- zabezpieczenie zwarciowe.

18.5. Interfejsy komunikacyjne i zarządzanie

UPS musi umożliwiać:

- lokalne monitorowanie parametrów pracy;

- komunikację z systemami zarządzania;
- przekazywanie informacji o stanie urządzenia;
- monitorowanie:
  - poziomu naładowania baterii,
  - czasu podtrzymania,
  - obciążenia,
  - stanu pracy;
- generowanie alarmów.

Urządzenie musi umożliwiać integrację z systemem monitorowania infrastruktury oraz systemem logowania zdarzeń.

18.6. Funkcje bezpieczeństwa

UPS musi posiadać:

- zabezpieczenie przeciwprzepięciowe;
- zabezpieczenie przed przeciążeniem;
- zabezpieczenie przed zwarciem;
- zabezpieczenie akumulatorów;
- sygnalizację stanów alarmowych;
- możliwość awaryjnego odłączenia zasilania, jeżeli jest wymagana przez zastosowanie urządzenia.

18.7. Wymagania dotyczące współpracy z infrastrukturą

UPS musi umożliwiać zasilanie urządzeń infrastruktury teleinformatycznej, w szczególności:

- serwera backupowego;
- urządzeń sieciowych;
- urządzeń bezpieczeństwa;
- urządzeń pamięci masowej;
- urządzeń zarządzających infrastrukturą.

UPS musi umożliwiać współpracę z:

- systemem monitorowania infrastruktury;
- systemem logowania zdarzeń;
- systemem automatycznego zamykania systemów IT;

18.8. Wyposażenie dodatkowe

W ramach dostawy należy zapewnić:

- elementy umożliwiające montaż w szafie Rack;
- przewody zasilające i komunikacyjne wymagane do uruchomienia;

- oprogramowanie lub moduły umożliwiające zarządzanie urządzeniem;

19. Urządzenia UTM dla lokalizacji zdalnych

19.1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa, instalacja, konfiguracja oraz uruchomienie trzech urządzeń klasy UTM (Unified Threat Management) przeznaczonych do ochrony sieci komputerowych w trzech niezależnych lokalizacjach Zamawiającego.

Urządzenia muszą zapewniać ochronę ruchu sieciowego, kontrolę dostępu, zabezpieczenie przed zagrożeniami cybernetycznymi oraz możliwość bezpiecznej komunikacji pomiędzy lokalizacjami a centralną infrastrukturą Zamawiającego.

Każde urządzenie musi działać jako niezależna jednostka ochrony dla przypisanej lokalizacji.

19.2. OBSŁUGA SIECI

- Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP.

19.3. ZAPORA KORPORACYJNA (Firewall)

12. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection.

13. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT.

14. Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).

15. Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie.

16. Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, usług internetowych (web services), użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia.

17. Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac.

18. Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall.

19. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł.

20. Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos.

21. Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego).

22. System musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe.

19.4. INTRUSION PREVENTION SYSTEM (IPS)

11. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.

12. Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy.

13. Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.

14. Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS.

15. Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia.

16. Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS.

17. Administrator ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP.

18. Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.

19. Moduł IPS ma zapewniać analizę protokołów przemysłowych co najmniej takich jak: Modbus, UMAS, S7 200-300-400, EtherNet/IP, CIP, OPC UA, OPC (DA/HDA/AE), BACnet/IP, PROFINET, SOFBUS/LACBUS, IEC 60870-5-104, IEC 61850 (MMS, Goose& SV).

20. Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych.

19.5. KSZTAŁTOWANIE PASMA (TrafficShapping)

4. Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.

5. Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP.

6. Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring).

Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.

19.6. OCHRONA ANTYWIRUSOWA

6. Urządzenie ma być dostarczone wraz z komercyjnym, zaawansowanym skanerem antywirusowym oraz umożliwiać skanowanie plików w oparciu o sandboxing zlokalizowany w Internecie na serwerach producenta i na terenie Unii Europejskiej. Nie dopuszcza się aby analiza sandboxingu była przeprowadzana na urządzeniu lub wymagała instalacji dodatkowego urządzenia lub oprogramowania. Nie dopuszcza się również żeby analiza sandboxingu była przeprowadzana przez firmy trzecie.

7. Skaner antywirusowy ma być dostarczany przez firmy trzecie (inne niż producent rozwiązania).

8. Administrator ma mieć możliwość określenia akcji w przypadku wykrycia zagrożenia bądź gdy analiza skanerem antywirusowym została zakończona błędem.

9. Skaner antywirusowy ma pochodzić od europejskiego producenta.

10. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.

Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu wykrycia infekcji.

19.7. OCHRONA ANTYSPAM

5. Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).

6. Ochrona antyspam ma działać w oparciu o:

d. - białe/czarne listy,

e. DNS RBL,

f. Skaner heurystyczny.

7. W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia.

8. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.

19.8. WIRTUALNE SIECI PRYWATNE (VPN)

9. Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).

10. Urządzenie ma wspierać co najmniej następujące typy sieci VPN:

d) PPTP VPN,

e) IPSec VPN,

f) SSL VPN.

11. SSL VPN ma działać w trybie tunelu.

12. Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem.

13. Klient SSL VPN ma być dostępny z poziomu portalu uwierzytelniania (captive portal)

14. Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).

15. Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf.

16. Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz RouteBased.

19.9. FILTR DOSTĘPU DO STRON WWW

12. Urządzenie ma posiadać wbudowany filtr URL.

13. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 77 kategorii tematycznych stron internetowych. Rozszerzony URL Filtering posiada miliony sklasyfikowanych stron internetowych.

14. Klasyfikacja URL musi się odbywać w oparciu o komunikację z serwerami producenta znajdującymi się w sieci Internet, a nie na bazie danych przechowywanej lokalnie w urządzeniu.

15. Administrator ma mieć możliwość dodawania własnych kategorii URL.

16. Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej:

d. blokowanie dostępu do adresu URL,

e. zezwolenie na dostęp do adresu URL,

f. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.

17. Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.

18. Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych.

19. Filtr URL musi uwzględniać komunikację po protokole HTTPS.

20. Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.

21. Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane.

22. Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch

19.10. UWIERZYTELNIANIE

15. Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o: lokalną bazę użytkowników (wewnętrzny LDAP),

16. zewnętrzną bazę użytkowników (zewnętrzny LDAP),

17. usługę katalogową Microsoft Active Directory.

18. Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP.

19. Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły: SSL,

20. Radius,

21. Kerberos.

22. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy.

23. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta.

24. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny.

25. Rozwiązanie musi mieć możliwość transparentnego uwierzytelniania użytkowników w ramach infrastruktury VDI (Virtual Desktop Infrastructure) poprzez dedykowanego agenta. Metoda ta musi wspierać co najmniej technologie Citrix Virtual Apps i Microsoft Remote Desktop Services (RDS).

26. Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP).

27. Wbudowany moduł 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH.

28. Rozwiązanie musi zapewniać Zero-Trust Network Access (ZTNA), dając dostęp do zasobów na podstawie analizy polityk bezpieczeństwa w oparciu co najmniej o weryfikację wersji systemu operacyjnego, statusu zapory sieciowej czy zainstalowanego programu antywirusowego na stacji roboczej.

19.11. ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP)

21. Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. LoadBalancing).

22. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy: równoważenie względem adresu źródłowego, równoważenie względem połączenia.

23. Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.

24. Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover).

25. Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza.

26. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów).

27. Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP.

19.12. ROUTING (TRASOWANIE)

6. Urządzenie ma umożliwiać statyczne trasowanie pakietów.

7. Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.

8. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing).

9. Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.

10. Rozwiązanie musi dawać możliwość wybrania predefiniowalnego obiektu typu blackhole.

19.13. ADMINISTRACJA URZĄDZENIEM

22. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.

23. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS.

24. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP.

25. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.

26. Urządzenie musi oferować możliwość wykorzystania wbudowanych profili administracyjnych określających dostęp do poszczególnych modułów systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis.

27. Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH)

28. Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania.

29. Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS.

30. Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup.

31. Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych.

32. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła.

33. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora (scriptrecording).

34. System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services).

35. Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników.

36. Urządzenie ma umożliwiać zapisywanie logów na wbudowanym dysku.

37. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).

38. Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX.

39. Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie: manualnego eksportu do pliku w dowolnym momencie czasu, automatycznego eksportu do serwerów producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu

40. Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzącego bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora.

41. Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.

42. Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego

19.14. RAPORTOWANIE

10. Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.

11. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.

12. System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego.

13. System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów.

14. System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu.

15. System raportowania ma umożliwiać eksport wyników raportu do formatu CSV.

16. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta.

17. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3.

18. Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).

19.15. POZOSTAŁE USŁUGI I FUNKCJE

10. Urządzenie ma umożliwiać stworzenie interfejsu zagregowanego w oparciu o protokół LACP.

11. Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.

12. Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay).

13. Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6.

14. Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci skonfigurowanych zarówno na interfejsach fizycznych jak i wirtualnych (VLAN) w zakresie określenia bramy, serwerów DNS, nazwy domeny).

15. Urządzenie ma posiadać usługę DNS Proxy.

16. Urządzenie ma posiadać wsparcie dla Spanning-treeprotocol (RSTP/MSTP).

17. Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN.

18. Urządzenie musi mieć zaimplementowane Open API.

Urządzenie ma posiadać dwie niezależne partycje np. w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware). W tym celu ma być możliwe zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie.

19.16. PARAMETRY SPRZĘTOWE

5. Urządzenie ma być wyposażone w slot na kartę microSD.
6. Liczba portów Ethernet 2,5Gbps – min. 8. Liczba portów światłowodowych 1Gbps – min.1.
28. Przepustowość Firewall (1518 bajtów UDP) – minimum 9Gbps.
29. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 5Gbps.
30. Przepustowość filtrowania Antywirusowego – minimum 0.7 Gbps.
31. Liczba tuneli VPN IPSec – minimum 280.
32. Liczba tuneli typu SSL VPN (tryb tunelu) – minimum 280.
33. Obsługa interfejsów 802.11q (VLAN) – minimum 380.
34. Liczba równoczesnych sesji – minimum 300 000 i nie mniej niż 35 000 nowych sesji/sekundę.
35. Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive.
36. Liczba reguł filtrowania – minimum 8 000.
37. Liczba tras statycznego routingu – minimum 500.
38. Liczba tras dynamicznego routingu – minimum 9 000.
39. Urządzenie musi być wyposażone w moduł TPM.

UWAGI:

5. Kabel zasilający do zasilacza oraz inny niezbędny do prawidłowej pracy Urządzenia asortyment, będzie dostarczony przez wykonawcę w komplecie z urządzeniami.
6. Wszystkie komponenty Urządzenia muszą być fabrycznie nowe nie używane i nie refabrykowane oraz nie recertyfikowane.
7. Urządzenie musi być zaprojektowane i rozwijane na terenie Unii Europejskiej.
8. Urządzenie musi posiadać certyfikat EAL4+.

20. System bezpiecznej komunikacji VPN

20.1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa, konfiguracja oraz uruchomienie funkcjonalności bezpiecznej komunikacji VPN (Virtual Private Network), umożliwiającej realizację szyfrowanych połączeń pomiędzy lokalizacjami Zamawiającego, użytkownikami zdalnymi oraz zasobami infrastruktury teleinformatycznej.

Zamawiający dopuszcza realizację funkcjonalności VPN poprzez urządzenia klasy NGFW/UTM dostarczane w ramach pozycji 5 oraz 21 niniejszego OPZ, pod warunkiem zapewnienia wszystkich wymaganych funkcji.

20.2. Minimalne wymagania funkcjonalne

Rozwiązanie VPN musi zapewniać co najmniej:

- tworzenie szyfrowanych połączeń sieciowych;

- bezpieczną komunikację pomiędzy lokalizacjami Zamawiającego;
- bezpieczny dostęp użytkowników zdalnych do zasobów infrastruktury;
- kontrolę dostępu użytkowników korzystających z VPN;
- możliwość definiowania polityk dostępu;
- możliwość ograniczenia dostępu do wybranych zasobów;
- możliwość rejestrowania zdarzeń związanych z połączeniami VPN;
- możliwość integracji z usługą katalogową;
- możliwość integracji z mechanizmami MFA;
- możliwość monitorowania aktywnych połączeń.

20.3. Minimalne wymagania dotyczące VPN site-to-site

Rozwiązanie musi umożliwiać:

- tworzenie tuneli VPN pomiędzy lokalizacjami Zamawiającego;
- szyfrowaną transmisję danych pomiędzy sieciami lokalnymi;
- automatyczne zestawianie połączenia po awarii;
- monitorowanie dostępności tunelu;
- obsługę dynamicznej lub statycznej konfiguracji tras;
- definiowanie polityk dostępu pomiędzy lokalizacjami.

Rozwiązanie musi umożliwiać współpracę z urządzeniami NGFW/UTM dostarczanymi w ramach niniejszego zamówienia.

20.4. Minimalne wymagania dotyczące dostępu zdalnego użytkowników

Rozwiązanie musi umożliwiać:

- bezpieczny dostęp użytkowników zdalnych;
- uwierzytelnianie użytkowników;
- integrację z usługą katalogową Active Directory / Entra ID;
- integrację z mechanizmem MFA;
- możliwość nadawania uprawnień dostępu według użytkownika lub grupy;
- możliwość wymuszenia określonych zasad bezpieczeństwa dla połączeń zdalnych;
- możliwość odwołania dostępu użytkownika.

20.5. Wymagania bezpieczeństwa

Rozwiązanie VPN musi zapewniać:

- szyfrowanie transmisji danych;
- wykorzystanie aktualnych mechanizmów kryptograficznych;
- możliwość stosowania certyfikatów cyfrowych;
- możliwość uwierzytelniania wieloskładnikowego;

- ochronę przed nieautoryzowanym dostępem;
- rejestrowanie zdarzeń związanych z logowaniem i połączeniami.

20.6. Obsługiwane technologie

Rozwiązanie musi umożliwiać wykorzystanie standardowych technologii VPN, w szczególności:

- IPsec VPN;
- SSL VPN lub rozwiązanie równoważne;
- mechanizmy szyfrowania zgodne z aktualnymi standardami bezpieczeństwa.

W przypadku zastosowania rozwiązania równoważnego musi ono zapewniać kompatybilność z infrastrukturą Zamawiającego.

20.7. Zarządzanie i monitoring

System musi umożliwiać:

- zarządzanie konfiguracją VPN;
- monitorowanie aktywnych tuneli;
- monitorowanie użytkowników korzystających z VPN;
- przegląd historii połączeń;
- rejestrowanie zdarzeń;
- przekazywanie logów do systemu SIEM oraz centralnego menedżera logów;
- integrację z systemem monitorowania infrastruktury

20.8. Licencjonowanie

W ramach dostawy Wykonawca zobowiązany jest zapewnić:

- wszystkie wymagane licencje umożliwiające korzystanie z funkcjonalności VPN;
- możliwość korzystania z wymaganych klientów VPN;
- aktualizacje oraz wsparcie producenta rozwiązania, jeżeli jest wymagane przez zastosowane rozwiązanie.

CZĘŚĆ DRUGA:

Mobilny agregat prądotwórczy

1.1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa fabrycznie nowego, mobilnego agregatu prądotwórczego przeznaczonego do zapewnienia awaryjnego źródła zasilania dla infrastruktury Zamawiającego.

Agregat musi być przystosowany do pracy jako niezależne źródło zasilania oraz do współpracy z układem automatycznego załączania rezerwy (SZR) realizowanym w ramach pozycji 19 niniejszego OPZ.

W ramach dostawy należy dostarczyć kompletny agregat prądotwórczy wraz z homologowaną przyczepą umożliwiającą jego transport.

1.2. Minimalne wymagania funkcjonalne

Agregat musi:

- być fabrycznie nowy;
- być przeznaczony do pracy ciągłej oraz awaryjnej;
- umożliwiać pracę jako trójfazowe źródło zasilania;
- umożliwiać ręczne uruchomienie i obsługę;
- umożliwiać automatyczne uruchomienie poprzez zewnętrzny sygnał sterujący;
- umożliwiać współpracę z układem SZR;
- posiadać możliwość monitorowania podstawowych parametrów pracy;
- posiadać możliwość diagnostyki podstawowych stanów pracy i awarii;
- być przystosowany do transportu na homologowanej przyczepie.

1.3. Minimalne parametry elektryczne

Agregat musi posiadać co najmniej następujące parametry:

Parametr	Wymaganie minimalne
Moc znamionowa PRP	minimum 125 kVA
Moc znamionowa PRP	minimum 100 kW
Napięcie znamionowe	400/230 V
Częstotliwość	50 Hz
Liczba faz	3
Współczynnik mocy	cos φ = 0,8
Rodzaj paliwa	olej napędowy

Agregat musi zapewniać stabilne parametry napięcia i częstotliwości odpowiednie do zasilania odbiorników elektrycznych, w tym odbiorników nieliniowych oraz urządzeń wyposażonych w elektroniczne układy zasilania.

1.4. Silnik spalinowy

Agregat musi być wyposażony w silnik wysokoprężny (Diesel) spełniający co najmniej następujące wymagania:

- prędkość nominalna: 1500 obr./min;
- chłodzenie cieczą;
- minimum 4 cylindry w układzie rzędowym;
- turbodoładowanie;
- chłodnica powietrza doładowującego (aftercooler/intercooler) lub rozwiązanie równoważne;
- elektryczny system rozruchu;
- napięcie instalacji rozruchowej 12 V;
- układ zapewniający stabilizację częstotliwości napięcia wyjściowego;
- system diagnostyczny umożliwiający identyfikację podstawowych stanów awaryjnych;
- spełnianie obowiązujących wymagań dotyczących emisji spalin, minimum zgodnie z wymaganiami Stage V, jeżeli mają zastosowanie do oferowanego urządzenia.

1.5. Generator / alternator

Generator agregatu musi:

- być przystosowany do pracy z odbiornikami liniowymi i nieliniowymi;
- posiadać uzwojenia zapewniające ograniczenie zawartości harmonicznych napięcia wyjściowego;
- posiadać rozwiązanie umożliwiające ograniczenie nadmiernych prądów w przewodzie neutralnym;
- posiadać izolację minimum klasy H;
- posiadać uzwojenia zabezpieczone przed wpływem warunków środowiskowych;
- umożliwiać krótkotrwałe przyjęcie zwiększonego obciążenia podczas rozruchu odbiorników o dużym prądzie rozruchowym;
- spełniać wymagania właściwych norm dotyczących generatorów elektrycznych.

Dopuszcza się zastosowanie rozwiązania konstrukcyjnego równoważnego względem opisanych sposobów wykonania uzwojeń i wzbudzenia, pod warunkiem zapewnienia nie gorszych parametrów elektrycznych i użytkowych.

1.6. Obudowa i konstrukcja agregatu

Agregat musi być wykonany w wyciszonej obudowie zewnętrznej, przeznaczonej do pracy w warunkach zewnętrznych.

Obudowa musi:

- być wykonana z materiału odpornego na korozję i warunki atmosferyczne lub posiadać skuteczne zabezpieczenie antykorozyjne;
- posiadać powłokę malarską odporną na warunki zewnętrzne;

- być zabezpieczona przed wpływem opadów atmosferycznych;
- ograniczać poziom emisji hałasu;
- zapewniać dostęp serwisowy do podzespołów;
- posiadać zabezpieczenie ruchomych i obracających się części przed przypadkowym kontaktem;
- posiadać punkt uziemienia umożliwiający połączenie metalowych elementów z uziemieniem;
- posiadać rozwiązania umożliwiające podnoszenie urządzenia przy użyciu urządzeń dźwigowych.

Obudowa musi być wyposażona w drzwi umożliwiające dostęp do panelu sterowania. Drzwi panelu sterowania muszą być zamykane i wyposażone w przeszklony wizjer umożliwiający obserwację podstawowych wskazań bez konieczności otwierania drzwi.

1.7. Panel sterowania i diagnostyka

Agregat musi być wyposażony w mikroprocesorowy panel sterowania umożliwiający:

- sterowanie pracą agregatu;
- uruchamianie i zatrzymywanie agregatu;
- pracę w trybie ręcznym;
- pracę w trybie automatycznym;
- współpracę z układem SZR;
- programowanie podstawowych parametrów pracy;
- monitorowanie podstawowych parametrów pracy silnika i generatora;
- sygnalizację stanów alarmowych;
- diagnostykę podstawowych stanów awaryjnych;
- wyświetlanie informacji o stanie pracy urządzenia.

Panel musi umożliwiać co najmniej monitorowanie:

- napięcia;
- częstotliwości;
- prądu;
- mocy;
- czasu pracy;
- podstawowych parametrów silnika;
- stanu paliwa, jeżeli pomiar jest realizowany przez system sterowania;
- stanów alarmowych.

Agregat musi posiadać główny wyłącznik kompaktowy, pełniący funkcję głównego zabezpieczenia elektrycznego.

1.8. Funkcje dodatkowe agregatu

Agregat musi posiadać lub być wyposażony w:

- elektryczny system rozruchu;
- ręczny wyłącznik akumulatora;
- system podgrzewania umożliwiający prawidłowy rozruch w warunkach obniżonej temperatury;
- plastikowy zbiornik paliwa o pojemności minimum 200 litrów;
- wannę retencyjną zabezpieczającą przed przedostaniem się wycieków do środowiska;
- czteropolowy wyłącznik główny;
- układ automatycznego dociążania agregatu lub rozwiązanie równoważne, jeżeli jest wymagane dla prawidłowej eksploatacji układu oczyszczania spalin;
- centralny punkt podnoszenia;
- gumowe elementy amortyzujące;
- ramę wykonaną z konstrukcji stalowej.

1.9. Gniazda wyjściowe i zabezpieczenia

Agregat musi posiadać minimum następujące gniazda wyjściowe:

- 1 × 400 V CEE, minimum 63 A, 3P+N+PE, stopień ochrony minimum IP67;
- 1 × 400 V CEE, minimum 32 A, 3P+N+PE, stopień ochrony minimum IP67;
- 1 × 400 V CEE, minimum 16 A, 3P+N+PE, stopień ochrony minimum IP67;
- 1 × 230 V CEE, minimum 16 A, 2P+PE, stopień ochrony minimum IP67;
- 1 × 230 V, 16 A, typu Schuko lub równoważne, o stopniu ochrony minimum IP68.

Gniazda wyjściowe muszą posiadać zabezpieczenia odpowiednie do ich parametrów znamionowych.

Dla obwodów gniazdowych należy zapewnić:

- ochronę różnicowoprądową;
- zabezpieczenia nadprądowe;
- indywidualne zabezpieczenie poszczególnych obwodów, jeżeli wymagane dla zapewnienia selektywności i bezpieczeństwa instalacji.

Dopuszcza się zastosowanie wyłączników różnicowoprądowych z członem nadprądowym (RCBO) lub rozwiązania równoważnego.

Agregat musi posiadać również gniazdo umożliwiające zasilanie obwodów pomocniczych 230 V.

1.10. Poziom hałasu

Poziom hałasu agregatu nie może przekraczać:

- 76 dB(A) w odległości 1 m;
- 64 dB(A) w odległości 7 m,

lub wartości równoważnych wynikających z obowiązujących metod pomiarowych.

Gwarantowany poziom mocy akustycznej agregatu nie może przekraczać 93 dB(A), jeżeli parametr ten ma zastosowanie do oferowanego urządzenia

1.11. Wymagania dotyczące zgodności i dokumentacji

Agregat musi spełniać wymagania obowiązujących przepisów dotyczących:

- bezpieczeństwa maszyn;
- kompatybilności elektromagnetycznej;
- bezpieczeństwa urządzeń elektrycznych;
- emisji hałasu do środowiska;
- emisji zanieczyszczeń, jeżeli mają zastosowanie do oferowanego urządzenia.

1.12. Przyczepa transportowa

W ramach dostawy należy dostarczyć homologowaną przyczepę przystosowaną do transportu oferowanego agregatu.

Przyczepa musi posiadać co najmniej:

- minimum 2 osie;
- konstrukcję przystosowaną do montażu oferowanego agregatu;
- ramę stalową zabezpieczoną antykorozyjnie, w szczególności poprzez cynkowanie ogniowe lub rozwiązanie równoważne;
- wzmocnienia konstrukcji umożliwiające bezpieczny montaż agregatu;
- koła umieszczone poza obrysem ramy lub rozwiązanie zapewniające odpowiednią stabilność;
- urządzenie najazdowe z hamulcem postojowym;
- zaczep kulowy lub rozwiązanie zgodne z wymaganiami homologacyjnymi;
- koła dostosowane do dopuszczalnej masy całkowitej przyczepy;
- dyszel o stałej wysokości sprzęgu lub rozwiązanie równoważne;
- metalowe błotniki;
- chlapacze przeciwbłotne;
- minimum cztery podpory stabilizujące;
- wzmacniane koło manewrowe;
- kliny pod koła;
- oświetlenie zgodne z obowiązującymi przepisami;
- podpory z możliwością regulacji;
- zaczep transportowy zgodny z homologacją;
- dopuszczalną masę całkowitą nie większą niż 3500 kg, jeżeli wynika to z wymaganej klasy przyczepy.

Przyczepa musi posiadać homologację dopuszczającą ją do użytkowania zgodnie z obowiązującymi przepisami

1.13. Wymagania dotyczące współpracy z układem SZR

Agregat musi umożliwiać współpracę z układem automatycznego załączania rezerwy realizowanym w ramach pozycji 19 niniejszego OPZ.

W szczególności musi umożliwiać:

- zdalne otrzymanie sygnału uruchomienia;
- automatyczny rozruch;
- przekazanie informacji o gotowości agregatu do przejęcia obciążenia;
- zdalne zatrzymanie po zakończeniu pracy awaryjnej;
- pracę w trybie automatycznym;
- ręczne przejęcie sterowania w przypadku awarii automatyki.

Sposób komunikacji i sterowania musi zostać dobrany przez Wykonawcę z uwzględnieniem dostarczonego agregatu oraz układu SZR.

1.14. Wymagania dotyczące producenta

Producent agregatu musi posiadać system zarządzania jakością zgodny z ISO 9001 oraz system zarządzania środowiskowego zgodny z ISO 14001 lub równoważne, potwierdzone aktualnymi certyfikatami lub dokumentami równoważnymi (okazane Zamawiającemu na żądanie).

1.15. Gwarancja

Wykonawca udzieli gwarancji na agregat oraz przyczepę na okres minimum 12 miesięcy, z limitem eksploatacji agregatu minimum 1000 motogodzin, w zależności od tego, który warunek nastąpi wcześniej.

Gwarancja musi obejmować wszystkie elementy agregatu dostarczone w ramach zamówienia

1.16. Dostawa i wdrożenie

W ramach realizacji zamówienia Wykonawca zobowiązany jest do:

- dostawy agregatu na miejsce wskazane przez Zamawiającego;
- dostawy homologowanej przyczepy;
- ustawienia i przygotowania agregatu do eksploatacji;
- wykonania uruchomienia testowego;
- sprawdzenia podstawowych parametrów pracy;
- sprawdzenia możliwości współpracy z układem SZR;
- przekazania instrukcji obsługi i dokumentacji techniczno-ruchowej;
- przekazania dokumentów gwarancyjnych;
- przekazania dokumentów dotyczących zgodności i homologacji.

2. Wykonanie przyłącza elektrycznego dla agregatu wraz z układem automatycznego załączania rezerwy (SZR)

2.1. Przedmiot zamówienia

Przedmiotem zamówienia jest wykonanie kompletnego rozwiązania umożliwiającego automatyczne przełączenie zasilania podstawowego na awaryjne źródło zasilania w postaci agregatu prądotwórczego dostarczanego w ramach niniejszego zamówienia.

Zakres obejmuje w szczególności:

- wykonanie analizy istniejącej instalacji elektrycznej Zamawiającego;
- opracowanie rozwiązania technicznego;
- dobór wymaganych elementów instalacji;
- dostawę i montaż układu automatycznego załączania rezerwy (SZR);
- wykonanie niezbędnych prac instalacyjnych;
- wykonanie połączenia pomiędzy instalacją elektryczną budynku a agregatem;
- uruchomienie oraz sprawdzenie poprawności działania całego układu.

2.2. Minimalne wymagania funkcjonalne

Wykonane rozwiązanie musi zapewniać:

- automatyczne wykrycie zaniku lub nieprawidłowych parametrów zasilania podstawowego;
- automatyczne uruchomienie agregatu prądotwórczego;
- automatyczne przełączenie odbiorów na zasilanie awaryjne;
- automatyczny powrót na zasilanie podstawowe po jego przywróceniu;
- automatyczne zatrzymanie agregatu po zakończeniu pracy awaryjnej;
- bezpieczną współpracę instalacji elektrycznej budynku z agregatem;
- zabezpieczenie przed jednoczesnym połączeniem źródła podstawowego i awaryjnego.

2.3. Zakres prac projektowych i przygotowawczych

Wykonawca zobowiązany jest przed rozpoczęciem prac do:

- przeprowadzenia wizji lokalnej;
- analizy istniejącej infrastruktury elektrycznej;
- określenia możliwości technicznych wykonania przyłączenia agregatu;
- określenia wymaganych parametrów układu SZR;
- przygotowania dokumentacji technicznej niezbędnej do wykonania prac;
- uzgodnienia rozwiązania z Zamawiającym.

Jeżeli obowiązujące przepisy wymagają uzyskania dodatkowych uzgodnień lub dokumentacji, Wykonawca zobowiązany jest do ich przygotowania.

2.4. Minimalne wymagania dotyczące układu SZR

Układ automatycznego załączania rezerwy musi:

- być przeznaczony do współpracy z dostarczonym agregatem prądotwórczym;
- umożliwiać automatyczne sterowanie pracą agregatu;
- posiadać układy zabezpieczające przed nieprawidłową pracą;
- zapewniać separację elektryczną źródeł zasilania;
- umożliwiać ręczne sterowanie w przypadku awarii automatyki;
- posiadać sygnalizację podstawowych stanów pracy;
- być dobrany odpowiednio do parametrów instalacji elektrycznej Zamawiającego.

2.5. Zakres wykonania instalacji

Wykonawca zobowiązany jest wykonać wszystkie niezbędne prace umożliwiające prawidłowe działanie systemu, w szczególności:

- montaż urządzeń SZR;
- wykonanie połączeń elektrycznych;
- wykonanie tras kablowych, jeżeli są wymagane;
- wykonanie połączeń sterujących;
- wykonanie wymaganych zabezpieczeń;
- wykonanie oznaczeń instalacji;
- wykonanie niezbędnych pomiarów elektrycznych.

Zakres prac musi obejmować wszystkie elementy niezbędne do kompletnego i prawidłowego działania rozwiązania.

2.6. Wymagania bezpieczeństwa

Wykonana instalacja musi:

- spełniać wymagania obowiązujących przepisów i norm dotyczących instalacji elektrycznych;
- zapewniać ochronę przeciwporażeniową;
- zapewniać ochronę przeciwzwarciową i przeciążeniową;
- posiadać właściwe oznaczenia;
- posiadać dokumentację powykonawczą.

2.7. Testy i odbiór

Po wykonaniu prac Wykonawca zobowiązany jest przeprowadzić:

- test zaniku zasilania podstawowego;
- test automatycznego uruchomienia agregatu;
- test automatycznego przełączenia zasilania;
- test powrotu zasilania podstawowego;
- test zatrzymania agregatu;
- test zabezpieczeń układu.

Wykonawca zobowiązany jest przekazać Zamawiającemu:

- protokoły wykonanych pomiarów;
- dokumentację powykonawczą;
- schemat wykonanej instalacji;
- instrukcję eksploatacji.

2.8. Wymagania dotyczące doradztwa wykonawcy

Wykonawca zobowiązany jest zapewnić wsparcie techniczne oraz doradztwo w zakresie:

- wyboru optymalnego sposobu podłączenia agregatu;
- lokalizacji urządzeń;
- doboru parametrów układu SZR;
- sposobu prowadzenia instalacji;
- zapewnienia prawidłowej współpracy z istniejącą infrastrukturą elektryczną.

Rozwiązanie musi zostać dobrane z uwzględnieniem istniejących warunków technicznych obiektu oraz wymagań Zamawiającego.

CZĘŚĆ TRZECIA:

I. ZAKRES PRAC

1. Przeprowadzenie:
   a) audytu wdrożonego u Zamawiajacego systemu bezpieczeństwa informacji SZBI,
   b) analizy efektywności działań w zakresie monitorowania, pomiarów, analizy i oceny SZBI, w tym przegląd wskaźników ryzyka i zgodności.
2. Audyt powinien obejmować
   a) Analiza wstępna i określenie zakresu audytu
      - Zdefiniowanie obszarów, lokalizacji objętych SZBI.
      - Weryfikacja ewidencji obszaru przetwarzania informacji, w tym dokładność danych dotyczących lokalizacji, kondygnacji i adresów.
      - Sprawdzenie, czy zakres SZBI jest zgodny z wymaganiami norm ISO/IEC 27001 oraz potrzebami organizacji.
   b) Weryfikacja dokumentacji systemowej
      - Wprowadzenie do SZBI: Ocena, czy dokumentacja zawiera podstawowe zasady zarządzania bezpieczeństwem informacji i zgodność z cyklem PDCA (Plan-Do-Check-Act).
      - Terminy i definicje: Sprawdzenie, czy wszystkie istotne pojęcia są zdefiniowane i zgodne z normami.
      - Kontekst organizacji: Analiza czynników wewnętrznych i zewnętrznych oraz ich wpływu na SZBI, w tym analiza ryzyk.
   c) Zarządzanie ryzykiem
      - Ocena procesu identyfikacji i analizy ryzyk, w tym dokumentacji dotyczącej szacowania ryzyk.
      - Analiza działań zaradczych i korygujących dla zidentyfikowanych ryzyk.
   d) Zabezpieczenia i deklaracja stosowana
      - Weryfikacja, czy deklaracja stosowania zabezpieczeń jest zgodna z Załącznikiem A normy ISO/IEC 27001.
      - Ocena skuteczności wdrożonych zabezpieczeń oraz uzasadnienia ewentualnych wyłączeń.
   e) Dokumentacja operacyjna
      - Polityki i procedury: Sprawdzenie polityk bezpieczeństwa (np. kryptografii, zarządzania dostępem, bezpieczeństwa zasobów ludzkich) i ich zgodności z wymaganiami normatywnymi.
      - Ewidencje i rejestry: Ocena kompletności i aktualności ewidencji aktywów, obszarów przetwarzania informacji oraz rejestrów incydentów i zgłoszeń.
      - Zarządzanie dostępem: Sprawdzenie procedur przyznawania, zmiany i odbierania dostępu oraz zgodności z dokumentacją.
   f) Monitorowanie i doskonalenie SZBI
      - Ocena procesów monitorowania, analizy i oceny systemu w odniesieniu do zgodności z wymaganiami i celami bezpieczeństwa.
      - Weryfikacja raportów z monitorowania, przeglądów zarządzania i działań korygujących.
      - Analiza działań doskonalących, w tym ocena skuteczności realizowanych zmian.

g) Zarządzanie incydentami i ciągłości działania
- Ocena polityki zarządzania incydentami, w tym procedur zgłaszania, oceny i reagowania na incydenty.
- Sprawdzenie planów zarządzania ciągłością działania i odtwarzania po katastrofie, w tym testów i analiz RTO, RPO, MTPD i MBCO.

h) Audyty wewnętrzne
- Weryfikacja programu i planów audytów wewnętrznych, w tym ocena zgodności z wymaganiami ISO/IEC 27001.
- Sprawdzenie raportów z audytów wewnętrznych pod kątem ustaleń, zgodności i zaleceń.

i) Zgodność z przepisami i ochroną danych osobowych
- Ocena dokumentacji dotyczącej przetwarzania danych osobowych, w tym zgodności z RODO.
- Weryfikacja rejestrów czynności przetwarzania danych, ocen skutków dla ochrony danych oraz testów równowagi.

j) Dokumentacja operacyjna
- Analiza polityk i procedur dotyczących korzystania z systemów, urządzeń i sieci.
- Weryfikacja zasad postępowania z nośnikami informacji, tworzenia haseł i korzystania z Internetu oraz poczty elektronicznej.

k) Zarządzanie dostawcami
- Sprawdzenie polityk i procedur związanych z bezpieczeństwem informacji w relacjach z dostawcami.
- Ocena zgodności działań dostawców z wymaganiami organizacji.

II. ZGODNOŚĆ Z WYMAGANIAMI PRAWNYMI

1. Weryfikacja dokumentacji dotyczącej monitorowania i przestrzegania wymagań prawnych, regulacyjnych i umownych.
2. Analiza zgodności z politykami zgodności oraz audytami technicznymi.

III. DO ZADAŃ WYKONAWCY BĘDZIE NALEŻEĆ

1. Przeprowadzenie szczegółowej analizy i oceny SZBI, obejmującej:
   a) Identyfikację niezgodności i słabości w dokumentacji oraz wdrożeniu systemu.
   b) Przeprowadzenie wywiadów z wybranym personelem.
2. Przekazanie dla Kierownika/Dyrektora ZWiK w Wierzbicy oraz dla Zamawiającego podpisanego przez audytora raportu z audytu wdrożonego w ZWiK systemu bezpieczeństwa informacji SZBI zawierający:
   a) Ustalenia audytu: Identyfikacja mocnych stron, niezgodności oraz obszarów wymagających doskonalenia.
   b) Rekomendacje: Propozycje działań korygujących i doskonalących.
   c) Ocena zgodności z normami i przepisami: Wskazanie poziomu zgodności SZBI z wymaganiami ISO/IEC 27001 i regulacjami prawnymi.
3. Wykonawca udokumentuje wykonanie zadania poprzez okazanie protokołu odbioru.
4. Dokumentowanie realizacji zadania poprzez:
   a) Sporządzenie protokołu odbioru audytu.

b) Wskazanie osób odpowiedzialnych za wdrożenie działań pokontrolnych.

CZĘŚĆ CZWARTA:

Przedmiotem zamówienia jest:

1) opracowanie, wdrożenie, przegląd, aktualizacja Systemu Zarządzania Bezpieczeństwem Informacji, zwanego dalej „SZBI";
2) utrzymanie, zarządzanie i doskonalenie SZBI;
3) przeprowadzenie szkoleń dla personelu ZWiK w Wierzbicy w obszarze wdrożonego SZBI.

Celem realizowanego przedmiotu zamówienia jest opracowanie, wdrożenie, przegląd i aktualizacja SZBI w ZWiK w Wierzbicy z uwzględnieniem wymagań prawa krajowego i prawa Unii Europejskiej, możliwego do eksploatacji, zarządzania, utrzymania, doskonalenia i przygotowanego do audytu, którego przedmiotem będzie certyfikacja tego systemu za zgodność z wymogami Polskiej Normy PN-EN ISO/IEC 27001:2023-08 „*Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności -- Systemy zarządzania bezpieczeństwem informacji – Wymagania*".

W ramach realizacji przedmiotu zamówienia Wykonawca będzie również świadczył usługi konsultacyjno-doradcze w przedmiocie utrzymania, zarządzania i doskonalenia SZBI, w tym świadczenie usługi wsparcia w zakresie stosowania SZBI przez personel ZWiK w Wierzbicy.

Wykonawca przeprowadzi szkolenia dla personelu w obszarze wdrożonego SZBI.

Przedmiot zamówienia będzie realizowany w ramach projektu konkursu grantowego pn. „Cyberbezpieczne Wodociągi" w ramach Krajowego Planu Odbudowy i Zwiększania Odporności (dalej: konkurs „Cyberbezpieczne Wodociągi").

Opracowane w wyniku niniejszego postępowania dokumenty będą aktualizować stan bezpieczeństwa informacji, w tym zwłaszcza w kontekście zadań realizowanych w ramach konkursu „Cyberbezpieczne Wodociągi" i zgodnie z dokumentami opracowanymi w ramach ww. konkursu.

SZBI obejmie wszystkie informacje i procesy w organizacji Zamawiającego niezależnie od formy przetwarzania (w sposób zautomatyzowany lub niezautomatyzowany) oraz środków technicznych służących do tego przetwarzania (systemy teleinformatyczne, nośniki danych, sprzęt komputerowy itp.) z wyłączeniem obszaru przetwarzania informacji niejawnych wynikającego z obowiązujących przepisów prawa dotyczących ochrony informacji niejawnych.

Zamawiający wymaga, aby opracowane dokumenty składające się na wdrażany SZBI stanowiły spójne, powiązane ze sobą, przejrzyste, skuteczne, jednolicie oznaczone i przygotowane do bezpośredniego stosowania przez personel Zamawiającego regulacje wewnętrzne, oraz uwzględniały wszystkie zasoby lokalowe i budynkowe, materiałowe, sprzętowe i kadrowe pozostające w dyspozycji Zamawiającego.

Opracowana dokumentacja musi zostać zaprojektowana z uwzględnieniem systemowego, hierarchicznego układu kategorii i typów dokumentów wraz określeniem dla nich odpowiednich poziomów (np. strategiczny, normatywny, operacyjny) i wskazaniem ich klasyfikacji, wersjonowania, cyklu życia i relacji z innymi dokumentami SZBI. Opracowana dokumentacja musi zapewniać identyfikację i opis wytworzonego dokumentu (np. tytuł, data, autor lub numer referencyjny), sposób jego przeglądu i zatwierdzenia, sposób dystrybucji, klasyfikację i oznaczenie oraz kontrolę zmian.

Opracowana dokumentacja musi opierać się o jednolitą terminologię i jednolitą siatkę pojęciową.

Opracowana dokumentacja musi być sformułowana w sposób zrozumiały i adekwatny dla odbiorców oraz być spójna z terminologią stosowaną w powszechnie obowiązujących przepisach prawa i Polskich Normach wyszczególnionych w opisie przedmiotu zamówienia, a także uwzględniająca stan prawny obowiązujący w okresie realizacji przedmiotu zamówienia, w szczególności w zakresie obowiązków prawnych ciążących na Zamawiającym.

Opracowane dokumenty będą podlegały uzgodnieniu z Zamawiającym. Zamawiający zastrzega sobie prawo do weryfikacji przedkładanych dokumentów i wnoszenia do nich uwag, co do których Wykonawca będzie musiał przestawić stanowisko co do ich uwzględnienia lub nieuwzględnienia wraz z uzasadnieniem oraz uwzględnić uwagi w zakresie wskazanym przez Zamawiającego.

Zamawiający wymaga, aby opracowana dokumentacja SZBI w pierwszej kolejności obejmowała środki organizacyjne i techniczne wdrożone i stosowane u Zamawiającego, a środki organizacyjne i techniczne planowane do wdrożenia były możliwe do wdrożenia, eksploatowania i monitorowania ich skuteczności przez Zamawiającego oraz odpowiednie i proporcjonalne do oszacowanego ryzyka, uwzględniające najnowszy stan wiedzy, kosztów wdrożenia, wielkości Zamawiającego, prawdopodobieństwa wystąpienia incydentów, narażenia Zamawiającego na ryzyka, skutki społeczne i gospodarcze.

Zamawiający wymaga, aby opracowany i wdrożony u Zamawiającego SZBI obejmował systemy informacyjne wykorzystywane w procesach wpływających na świadczenie usług oraz systemy informacyjne wykorzystywane w procesie świadczenia usług przez Zamawiającego oraz wypełniał wymogi określone dotychczas w projektowanych przepisach projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) wdrażającego dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii zmieniającą rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającą dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz. Urz. UE L 333 z 27.12.2022, str. 80), zwaną dalej „dyrektywą NIS 2", w szczególności w zakresie obowiązków wyznaczonych dla tzw. „podmiotu kluczowego" w obszarze wdrożenia systemu zarządzania bezpieczeństwem informacji w systemie informacyjnym wykorzystywanym w procesach wpływających na świadczenie usługi oraz wymaganej dokumentacji dotyczącej bezpieczeństwa systemu informacyjnego wykorzystywanego w procesie świadczenia usługi.

Zamawiający wymaga, aby opracowany i wdrożony u Zamawiającego SZBI, podejmowane czynności związane w tym opracowaniem i wdrożeniem, a także opracowane dokumenty związane z jego późniejszą eksploatacją, monitorowaniem, przeglądem, utrzymaniem i doskonaleniem przez Zamawiającego, wypełniały wymogi określone w powszechnie obowiązujących przepisach prawa oraz Polskich Normach odnoszących się do zarządzania bezpieczeństwem informacji w organizacjach w szczególności:

1) ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2024 r. poz. 1557, 1717 oraz z 2025 r. poz. 1006 i 1019);
2) ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077 i 1222 oraz z 2025 r. poz. 1017 i 1069) (KSC);
3) rozporządzeniu Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. poz. 773) (KRI);

4) Polskiej Normie PN-EN ISO/IEC 27001:2023-08 *„Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności -- Systemy zarządzania bezpieczeństwem informacji – Wymagania”;*
5) Polskiej Normie PN-EN ISO/IEC 27002:2023-01 *„Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności -- Zabezpieczanie informacji”;*
6) Polskiej Normie PN-EN ISO/IEC 27005:2025-01 *„Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności -- Wytyczne do zarządzania ryzykami w bezpieczeństwie informacji”;*
7) Polskiej Normie PN-ISO 31000:2018-08 *„Zarządzanie ryzykiem -- Wytyczne”;*
8) Polskiej Normie PN-EN ISO 22301:2020-04 *„Bezpieczeństwo i odporność – Systemy zarządzania ciągłością działania -- Wymagania”;*
9) rozporządzeniu Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenia o ochronie danych) (Dz. Urz. UE L 119 z 4.05.2016, str. 1, Dz. Urz. UE L 127 z 23.05.2018, str. 2 oraz Dz. Urz. UE L 74 z 4.03.2021, str. 35).

Jeżeli w trakcie realizacji przez Wykonawcę przedmiotu zamówienia uwarunkowania prawne w zakresie bezpieczeństwa informacji, które dotyczą Zamawiającego, ulegną zmianie, Wykonawca zobowiązany będzie dostosować dokumentację SZBI do zaistniałych zmian.

Zamawiający wymaga, aby realizacja przedmiotu zamówienia obejmowała następujące czynności, realizowane w terminach i w sposób określony poniżej:

1) **etap pierwszy** obejmuje czynności planistyczno-analityczne niezbędne do opracowania i wdrożenia SZBI u Zamawiającego, polegające na:
   a) opracowaniu szczegółowego harmonogramu realizacji przedmiotu zamówienia,
   b) przeprowadzeniu koniecznych wywiadów z personelem Zamawiającego, realizującym zadania z zakresu objętego SZBI,
   c) analizie dostarczonych Wykonawcy wyników audytu KRI zrealizowanego przez Zamawiającego w ramach projektu konkursu grantowego pn. „Cyberbezpieczne Wodociągi” w ramach Krajowego Planu Odbudowy i Zwiększania Odporności (dalej: konkurs „Cyberbezpieczne Wodociągi”).
   d) analizie:
      – celów organizacji na podstawie zadań realizowanych przez ZWiK w Wierzbicy, ze szczególnym uwzględnieniem zagadnień cyberbezpieczeństwa i odporności organizacyjnej,
      – struktury organizacyjnej, w tym ról, zakresów odpowiedzialności i uprawnień w kontekście związanym z bezpieczeństwem informacji,
      – relacji funkcjonalnych i powiązań między komórkami organizacyjnymi, ze wskazaniem odpowiedzialności, przebiegu komunikacji i realizacji obowiązków związanych z bezpieczeństwem informacji,
      – zasobów osobowych zaangażowanych w obszar bezpieczeństwa informacji, w tym kompetencji, ról, uprawnień dostępowych i potrzeb szkoleniowych,
   e) określeniu i opracowaniu kontekstu dla opracowywania SZBI zawierającego uwarunkowania zewnętrzne dla tego systemu (uwzględniające m.in. uwarunkowania prawne, zobowiązania umowne związane z realizowanymi procesami i utrzymywanymi systemami teleinformatycznymi i inne, wynikające z realizowanej działalności Zamawiającego) oraz uwarunkowania wewnętrzne (m.in. strukturę

organizacyjną i model zarządzania, wewnętrzne akty prawne obowiązujące u Zamawiającego oraz zasoby kadrowe, sprzętowe i lokalowe, którymi dysponuje Zamawiający w ramach prowadzonej działalności), a także zidentyfikowanie i określenie wszystkich zainteresowanych stron związanych ze SZBI oraz ich wymagań w stosunku do SZBI,

f) przeprowadzeniu inwentaryzacji aktywów (zasobów) Zamawiającego objętych SZBI, w tym świadczonych przez zamawiającego usług, systemów informacyjnych wykorzystywanych w procesach wpływających na świadczenie usług oraz systemów informacyjnych wykorzystywanych w procesie świadczenia usług przez Zamawiającego wraz z określeniem ich właścicieli, poziomu krytyczności dla ciągłości działania Zamawiającego oraz zagrożeń, podatności i ryzyk związanych z ich eksploatacją przez Zamawiającego,

g) opracowaniu metodyki szacowania ryzyk zgodnej z wymogami Polskiej Normy PNEN ISO/IEC 27005:2025-01 „*Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności -- Wytyczne do zarządzania ryzykami w bezpieczeństwie informacji*” lub równoważne oraz przeprowadzenie szacowania ryzyk dla zidentyfikowanych ryzyk dla każdego zinwentaryzowanego aktywa (zasobu) z uwzględnieniem istniejących podatności oraz opracowanie raportu z procesu szacowania ryzyka określającego poziom ryzyk inherentnych, określenie planu postępowania z ryzykami na podstawie wdrożonych i stosowanych u Zamawiającego oraz planowanych i możliwych do wdrożenia środków technicznych i organizacyjnych oraz określenie poziomu ryzyk rezydualnych,

h) przeprowadzeniu analizy Business Impact Analysis (BIA) dla zinwentaryzowanych aktywów (zasobów) Zamawiającego,

i) opracowaniu i przedłożeniu Zamawiającemu raportu z podjętych czynności etapu pierwszego zawierającego:
– harmonogram, o którym mowa w lit. a powyżej,
– opis przeprowadzonych wywiadów, o których mowa w lit. b powyżej,
– rezultat analizy wyników tzw. audytu zerowego, przeglądu oraz koncepcję, o których mowa w lit. c powyżej,
– opracowane analizy i konteksty, o których mowa w lit. d i e powyżej,
– ewidencję zinwentaryzowanych aktywów (zasobów) Zamawiającego wraz z elementami, o których mowa w lit. f powyżej,
– wynik szacowania ryzyka wraz z planem postępowania z ryzykami i wdrożonymi oraz planowanymi do wdrożenia środkami technicznymi i organizacyjnym, o których mowa w lit. f powyżej, oraz wynik analizy Business Impact Analysis (BIA), o której mowa w lit. h powyżej;

2) **etap drugi** obejmuje opracowanie kompletnej dokumentacji SZBI, zapewniającej spełnienie przez Zamawiającego wszystkich wymogów normy ISO/IEC 27001:2023-08 oraz wynikającej z niej zabezpieczeń (A.5.1 – A.8.34), wraz z przeprowadzeniem mapowania jej powiązań z wymogami prawnymi i normatywnymi względem Zamawiającego, z uwzględnieniem wszystkich informacji uzyskanych podczas realizacji etapu pierwszego, w tym ww. audytu zerowego, obowiązującego stanu prawnego i stanu prawnego projektowanego w przepisach projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) wdrażającego dyrektywę NIS 2 oraz dobrych praktyk w obszarze bezpieczeństwa informacji, a następnie wdrożenie jej u Zamawiającego, zawierającej co najmniej:

a) politykę bezpieczeństwa informacji obejmującą co najmniej deklarację kierownictwa Zamawiającego, cele, zakres i kontekst ustanawianego SZBI oraz określenie zainteresowanych stron i ich wymagań w stosunku do SZBI, role i zakres odpowiedzialności pracowników Zamawiającego oraz poszczególnych komórek organizacyjnych związany z realizacją zadań przewidzianych przez wdrażany SZBI, strukturę dokumentacji wdrażanego SZBI oraz Deklarację Stosowania, o której mowa w Polskiej Normie PN-EN ISO/IEC 27001:2023-08 *„Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności - Systemy zarządzania bezpieczeństwem informacji – Wymagania" lub równoważne*,

b) polityki tematyczne, procedury, instrukcje, szablony, wzory wniosków i inne dokumenty, zwane dalej zbiorczo „politykami", mające na celu określenie stosowanych u Zamawiającego środków technicznych i organizacyjnych wynikających z Deklaracji Stosowania i uwzględniających zasady i zakres ich wdrożenia przewidziane w Polskiej Normie PN-EN ISO/IEC 27002:2023-01 „*Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności -- Zabezpieczanie informacji*" lub równoważne, zawierające niezbędne wzory dokumentów, które umożliwią Zamawiającemu stosowanie tych polityk w praktyce, w tym co najmniej:
- polityki zarządzania aktywami (zasobami) Zamawiającego, w tym zasady ich ewidencjonowania, przeglądu, klasyfikowania, oznaczania, akceptowalnego wykorzystywania oraz zakresu odpowiedzialności związanej z tym wykorzystywaniem, kontroli dostępu do aktywów (zasobów), oraz ich zwrotu,
– polityki zarządzania incydentami bezpieczeństwa informacji, w tym zbierania informacji o zagrożeniach i podatnościach dla systemów teleinformatycznych Zamawiającego, sposobów reagowania na te zagrożenia i zarządzania podatnościami, klasyfikowania incydentów bezpieczeństwa informacji, gromadzenia materiałów dowodowych, reagowania i ewidencjonowania incydentów bezpieczeństwa informacji oraz notyfikacji tych incydentów do właściwych podmiotów publicznych (CSIRT),
– polityki i niezbędne metodyki postępowania z ryzykiem bezpieczeństwa informacji oraz polityki dotyczące systematycznego szacowania ryzyka utraty integralności, dostępności oraz poufności informacji i ryzyka wystąpienia incydentu bezpieczeństwa informacji oraz szacowania ryzyk dla nowych aktywów (zasobów) Zamawiającego, skorelowane opracowanym przez Wykonawcę planem postępowania z ryzykiem oraz ze stosowanymi u Zamawiającego metodykami szacowania ryzyk w zakresie kontroli zarządczej oraz w zakresie ochrony danych osobowych,
– polityki nabywania, rozwoju, zmiany (z uwzględnieniem planowania i oceną potencjalnego wpływu zmian, autoryzacji zmian, informowania o zmianach, testów i akceptacji testów dla zmian, wdrażania zmian, w tym planów wdrożenia, zmian w sytuacjach awaryjnych, w tym procedury awaryjne, rejestru zmian, dostosowania dokumentacji operacyjnej i procedur użytkownika w razie potrzeby oraz dostosowanie planów ciągłości działania ICT w razie potrzeby), utrzymania, testowania i eksploatacji systemów teleinformatycznych, w tym w szczególności systemów informacyjnych wykorzystywanych w procesach wpływających na świadczenie usług oraz systemów informacyjnych wykorzystywanych w procesach świadczenia usług,

– polityki dotyczące bezpieczeństwa fizycznego i środowiskowego uwzględniające kontrolę dostępu, ze szczególnym uwzględnieniem bezpieczeństwa fizycznego serwerowni Zamawiającego,
– polityki bezpieczeństwa teleinformatycznego, w tym bezpieczeństwa systemów teleinformatycznych utrzymywanych i rozwijanych przez Zamawiającego oraz przez podmioty zewnętrzne na podstawie umów lub porozumień zawartych z Zamawiającym, obejmujące obszar zarządzania tymi systemami, bezpieczeństwa informacji przetwarzanych w chmurze, stosowania kontroli dostępu i kryptografii, zakresu obowiązków poszczególnych osób związanych z tym zarządzaniem i zarządzania sieciami,
– polityki bezpieczeństwa i ciągłość łańcucha dostaw produktów ICT, usług ICT i procesów ICT4, w rozumieniu rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz. Urz. UE L 151 z 07.06.2019, str. 15, z późn. zm.) od których zależy świadczenie usług w rozumieniu projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32), z uwzględnieniem związków pomiędzy bezpośrednim dostawcą sprzętu lub oprogramowania a Zamawiającym,
– polityki bezpieczeństwa osobowego obejmujące edukację z zakresu bezpieczeństwa informacji dla personelu Zamawiającego,
– polityki podstawowej cyberhigieny i podstawowych zasad bezpieczeństwa informacji dla personelu Zamawiającego,
– polityki bezpieczeństwa informacji w relacjach z podmiotami zewnętrznymi, w tym zewnętrznymi dostawcami produktów i usług ICT oraz zewnętrznymi dostawcami systemów teleinformatycznych, w tym zasady dostępu personelu tych podmiotów do systemów teleinformatycznych Zamawiającego,
– polityki monitorowania, przeglądu, doskonalenia, audytowania i okresowej oceny skuteczności SZBI, zawierającej w szczególności procedurę okresowego monitorowania i oceny skuteczności stosowanych środków technicznych i organizacyjnych służących zarządzaniu ryzykiem w ramach SZBI wraz z miernikami oceny skuteczności tych środków oraz program audytowania SZBI,
– polityki ochrony danych osobowych,
– polityki ciągłości działania w zakresie bezpieczeństwa informacji i niezakłóconego świadczenia usług, w tym plany ciągłości działania utrzymywanych systemów teleinformatycznych obejmujące testowanie tych planów, plany awaryjne oraz plany odtworzenia działalności po awarii wraz z udokumentowanymi planami zarządzania gotowością ICT i określeniem krytycznych systemów ICT oraz ich powiązania z procesami biznesowymi, parametrów parametrów RTO (Recovery Time Objective) i RPO (Recovery Point Objective),
– polityki komunikacji w ramach SZBI,
– polityki zarządzania dokumentacją SZBI
– polityki compliance, w tym ustanawiające sformalizowany proces zarządzania wymaganiami prawnymi, ustawowymi, regulacyjnymi i umownymi;

c) dokumentację dotyczącą bezpieczeństwa wszystkich zidentyfikowanych systemów informacyjnych wykorzystywanych w procesie świadczenia usług przez

Zamawiającego, obejmującą tzw. „dokumentację normatywną" w zakresie określonym przez projekt ustawy, o którym mowa we wprowadzeniu do wyliczenia.

Dokumentacja SZBI może polegać na aktualizacji poszczególnych polityk obowiązujących u Zamawiającego w trakcie realizacji przedmiotu zamówienia, o ile Zamawiający wyrazi na to zgodę.

Zamawiający dopuszcza aby zakres polityk, o których mowa w lit. b powyżej, był sporządzany przez Wykonawcę w sposób równoważny, o ile Wykonawca przedłoży Zamawiającemu opis i strukturę równoważnego zakresu polityk oraz sposobu uwzględniania w poszczególnych dokumentach zabezpieczeń, o których mowa w załączniku A do Polskiej Normy PN-EN ISO/IEC 27001:2023-08 „*Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności -- Systemy zarządzania bezpieczeństwem informacji – Wymagania*" oraz sposobu ich wdrożenia przewidzianego w Polskiej Normie PN-EN ISO/IEC 27002:2023-01 „*Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności -- Zabezpieczanie informacji*". Sporządzenie przez Wykonawcę równoważnego zakresu polityk musi być poprzedzone wyrażeniem zgody przez Zamawiającego.

Przedmiotowy etap obejmuje opracowanie i dostarczenie Zamawiającemu kompletu dokumentacji SZBI, weryfikację tej dokumentacji przeprowadzoną przez Zamawiającego, a następnie uczestnictwo w jej uzgodnieniach w ramach struktury organizacyjnej Zamawiającego. Zaleca się, aby Wykonawca dostarczał Zamawiającemu dokumentację sukcesywnie, tak by usprawnić ww. uzgodnienia. Wykonawca będzie zobowiązany do przedstawienia stanowiska odnośnie do uwzględnienia lub nieuwzględnienia uwag do dokumentacji oraz uwzględnienie ewentualnych zmian w dokumentacji zgodnie z wytycznymi Zamawiającego. Przedmiotowy etap obejmuje wdrożenie u Zamawiającego uzgodnionej z Zamawiającym dokumentacji.

3) **etap trzeci** obejmuje przeprowadzenie – w formie, zakresie i terminach uzgodnionych z Zamawiającym – szkoleń z zakresu opracowanej i wdrożonej dokumentacji SZBI, obejmujących w szczególności omówienie obowiązków spoczywających na poszczególnych grupach uczestniczących w tych szkoleniach oraz omówienie stosowanych środków organizacyjnych i technicznych przewidzianych w dokumentacji SZBI, dla:
    a) kadry kierowniczej Zamawiającego,
    b) pracowników biurowych u Zamawiającego niebędących kadrą kierowniczą Zamawiającego.
4) **etap czwarty** obejmuje utrzymanie, zarządzanie i doskonalenie wdrożonego SZBI u Zamawiającego, w tym świadczenie wsparcia w zakresie stosowania SZBI przez personel Zamawiającego. Polega na:
    a) weryfikacji stosowania środków organizacyjnych i technicznych przewidzianych w opracowanej dokumentacji SZBI oraz opracowanie wykazu środków organizacyjnych i technicznych, które są wdrożone i tych, które wymagają wdrożenia oraz podjęcie albo zaproponowanie ewentualnych czynności naprawczych i korygujących obejmujących zmiany we wdrożonej dokumentacji SZBI,
    b) świadczeniu usług informacyjno-konsultacyjno-doradczych w zakresie zarządzania, utrzymania i doskonalenia przez Zamawiającego wdrożonego SZBI,
    c) opracowanie planu utrzymania i doskonalenia wdrożonego SZBI wraz z harmonogramem, w formie wykresu Gantta, obejmującym szczegółowy wykaz zadań do podjęcia przez poszczególne osoby realizujące zadania z zakresu objętym SZBI przez okres 2 lat od dnia zakończenia realizacji przedmiotu zamówienia;

V. Harmonogram realizacji przedmiotu zamówienia

Szczegółowy harmonogram realizacji przedmiotu zamówienia, powinien zostać opracowany przez Wykonawcę i przedłożony do opinii Zamawiającego nie później niż 10 dni od dnia zawarcia umowy z Zamawiającym, przy czym etap pierwszy i etap drugi, o którym mowa powyżej muszą zostać zakończone w terminie nie dłuższym niż 2 miesiące od dnia zawarcia umowy z Zamawiającym.

VII. Organizacja realizacji przedmiotu zamówienia

Wyznaczony przez Wykonawcę kierownik projektu będzie realizował zadania z zakresu punktu kontaktowego pomiędzy Zamawiającym i Wykonawcą.

Każdy etap realizacji przedmiotu zamówienia będzie poprzedzony spotkaniem w terminie uzgodnionym z Zamawiającym w formie spotkania stacjonarnego albo za pośrednictwem środków komunikacji elektronicznej zapewniających transmisję spotkania w czasie rzeczywistym oraz wielostronną komunikację w czasie rzeczywistym umożliwiającą uczestnikom spotkania wypowiadanie się w jego toku, na którym kierownik projektu lub inna osoba wyznaczona przez Wykonawcę, przedstawi zakres planowanych do realizacji prac oraz prac zakończonych w etapie poprzedzającym spotkanie.

Wykonanie każdego z poszczególnych etapów zostanie potwierdzone przez Wykonawcę i Zamawiającego podpisanym obustronnie protokołem.

Wszystkie dokumenty sporządzone w ramach realizacji przedmiotu zamówienia będą sporządzone w języku polskim w formie elektronicznej i przekazywane na wskazany przez Zamawiającego adres poczty elektronicznej.

CZĘŚĆ PIĄTA:

1. Przedmiotem zamówienia jest przeprowadzenie szkolenia dla pracowników Zamawiającego w zakresie cyberbezpieczeństwa, dotyczącego praktycznego stosowania mechanizmów bezpieczeństwa korespondencji i zabezpieczania danych, w ramach projektu konkursu grantowego pn. „Cyberbezpieczne Wodociągi" realizowanego ze środków Krajowego Planu Odbudowy i Zwiększania Odporności (inwestycja C3.1.1) (dalej: konkurs „Cyberbezpieczne Wodociągi").
2. Zamawiający wymaga przeprowadzenia dwóch rodzajów szkoleń:
   1) dla wszystkich pracowników Zamawiającego (w tym kadry zarządzającej i informatyków) – szkolenia z zakresu podstawowego, dostosowane do wiedzy i świadomości przeciętnie rozeznanej osoby;
   2) dla kadry zarządzającej i informatyków – szkolenie z zakresu zaawansowanego, dostosowane do wiedzy specjalistycznej odbiorców szkolenia oraz dostosowane do zagrożeń, z którymi ta kategoria pracowników może się zetknąć wykonując swoją pracę.
3. Szkolenie powinno składać się z części teoretycznej i praktycznej.

Szkolenie dla pracowników Zamawiającego (zakres podstawowy):

4. Szczegółowy zakres szkolenia teoretycznego powinien obejmować co najmniej następujące zagadnienia:

4.1. Wprowadzenie do bezpieczeństwa cyfrowego w organizacji

- Omówienie zakresu niebezpieczeństw cybernetycznych, którym najczęściej poddane są instytucje administracji publicznej i samorządowej.
- Przegląd najczęstszych form ataków i ich konsekwencji dla instytucji administracji publicznej oraz metod zmniejszania potencjalnego ryzyka w realizacji bieżących zadań - na przykładach z ostatnich 6 m-cy.

4.2. Cyfrowe bezpieczeństwo fizyczne. Podstawowe zasady bezpieczeństwa fizycznego w kontekście możliwych ataków cyfrowych:

- Dostęp do obiektu instytucji administracji publicznej (ataki hackerskie typu "tailgating" i inne formy wejść i zagrożeń fizycznych).
- Zapewnienie bezpieczeństwa fizycznego dla dokumentów fizycznie umieszczonych w budynku instytucji.
- Dostęp fizyczny do sprzętu i oprogramowania IT w firmie, w tym zewnętrzne nośniki pamięci cyfrowej.

4.3. Cyberbezpieczeństwo:

- Podstawowe zasady higieny i bezpieczeństwa cyfrowego w jednostce administracji publicznej na przykładach: ataki wykorzystujące inżynierię społeczną, ataki złośliwym oprogramowaniem, próby wyłudzenia danych.
- Omówienie poszczególnych rodzajów cyberataków: phishing, spear phishing/whaling/CEO Fraud, Man-in-the-Middle, ransomware, DDoS, vishing.
- Korzystanie z poczty elektronicznej - szyfrowanie danych, budowanie bezpiecznych haseł, zagrożenie przejęcia poczty firmowej i prywatnej, możliwe symptomy infekcji komputera.
- Instalacja oprogramowania – skąd instalować i aktualizować.
- Uwierzytelnianie dwuskładnikowe – 2FA - powody, metody, narzędzia.

- Bezpieczeństwo haseł – wycieki, manager haseł.
- Metody zmniejszania potencjalnego ryzyka w realizacji bieżących zadań.
- Komunikacja kryzysowa – co należy zrobić w przypadku wystąpienia incydentu.

4.4. Bezpieczeństwo danych instytucji administracji publicznej – czynnik ludzki:

- Rozmowy o pracy w miejscach publicznych – zasady bezpiecznych rozmów, czego unikać, jak ograniczyć ryzyko.
- Udostępnianie zewnętrzne – zasady kwalifikacji, przesyłanie danych e-mailem, przenoszenie na pendriv-ie, korzystanie z nośników reklamowych, wykorzystanie folderów dzielonych i tymczasowych, szyfrowanie.
- Szyfrowanie danych.
- Makra – wykorzystanie do ataków, kiedy włączać makra, jak unikać zagrożeń.
- Usuwanie danych – jak zadbać o dane, jak przechowywać dane, miejsca przechowywania danych.
- BYOD.
- Korzystanie z publicznych sieci WIFI.
- RODO – podstawowe wymagania, jak działać zgodnie z RODO, na co zwracać uwagę w codziennej pracy.

4.5. Bezpieczna praca z przeglądarką:

- Strony szyfrowane – jak rozpoznać strony szyfrowane i nieszyfrowane, co mówi nam oznaczenie https i kłódka, jak sprawdzić, czy strona jest bezpieczna, pułapki https, nowe oznaczenia szyfrowania.
- Certyfikaty – co oznacza SSL, jak sprawdzić certyfikat strony, na co zwrócić uwagę.
- Ciasteczka.
- Wtyczki do przeglądarki.

4.6. Prywatne działania w sieci i ekspozycja na zagrożenia cyfrowe instytucji publicznej i samorządowej:

- Zagrożenia związane z używaniem poczty prywatnej do celów służbowych.
- Potencjalne konsekwencje dla Urzędu wynikające z przejęcia prywatnego konta pracownika na portalu społecznościowym.
- Zagrożenia wykorzystywania służbowych urządzeń mobilnych do celów prywatnych.
- Bezpieczeństwo psychiczne w używaniu portali społecznościowych.
- Wykorzystanie sztucznej inteligencji do ataków socjotechnicznych.

4.7. Sprzęt firmowy, praca zdalna:

- Na co warto zwrócić uwagę w kontekście bezpieczeństwa, pracując z domu lub w podróży.

Szkolenie dla kadry zarządzającej i informatyków (zakres zaawansowany):

5. Szczegółowy zakres szkolenia teoretycznego powinien obejmować co najmniej następujące zagadnienia:

5.1. **Moduł wprowadzający:**

- Cyberataki na świecie, w Europie i w Polsce, ze szczególnym uwzględnieniem cyberataków w sektorze zbiorowego zaopatrywania w wodę.
- Koszty cyberataków.
- Najczęstsze konsekwencje.
- Wpływ sytuacji geopolitycznej i gospodarczej na liczbę i rodzaj ataków.

- Prognozy.

5.2. **Moduł prawny:**

- Potencjalne roszczenia
- Odpowiedzialność cywilna członków organów spółki
- Odpowiedzialność administracyjną członków organów spółki
- Odpowiedzialność karna członków organów spółki
- Działania adresujące poszczególne ryzyka spółki oraz członków zarządu
- Zasady odpowiedzialności organów spółki w świetle ostatnich zmian kodeksu spółek handlowych (w tym business judgement rule)
- Możliwości transferu ryzyka
- Planowane zmiany w prawie

5.3. **Moduł procesowy**

- Procedury i obowiązki prawne w obszarze RODO
- Mechanizmy organizacyjne ograniczenia ryzyka
- w zakresie ochrony danych osobowych i poufności informacji
- Nowe obowiązki regulacyjne związane z cyberbezpieczeństwem
- Inne obowiązki prawne w konkretnej branży/rodzaju działalności (moduł do szkoleń zamkniętych)
- Procedury bezpieczeństwa
- Analiza ryzyka – co wziąć pod uwagę, jak przeprowadzić i udokumentować
- Procedury reagowania w kryzysie – co powinny objąć, na co zwrócić uwagę
- Plan ciągłości działania

5.4. **Moduł bezpieczeństwo IT**

- Różne płaszczyzny bezpieczeństwa
- Minimalna higiena bezpieczeństwa IT
- Testy bezpieczeństwa
- Stały monitoring – różne modele, różnice, jak działa
- Bezpieczeństwo w firmie i w domu
- Świadomość pracowników

5.5. **Moduł komunikacja kryzysowa**

- Procedury komunikacji kryzysowej

- Komunikacja kryzysowa: najważniejsze zasady
- Kanały komunikacji wewnętrznej i zewnętrznej
- Plany i scenariusze reakcji
- Zwalczanie nieprawdziwych informacji (procedura kryzysowa w odniesieniu do nieprawdziwych informacji oraz procedura żądania sprostowań itp.)

5.6. **Moduł kryzysowy**

- Pierwsze kroki po identyfikacji incydentu – co robić, a czego nie robić
- Obsługa incydentów naruszenia bezpieczeństwa – jak to działa od strony IT
- Zaszyfrowane lub skradzione dane - co można zrobić
- Obsługa incydentów – zapoznanie z procedurą i wymaganiami prawno-formalnymi dla różnego rodzaju incydentów
- Kwalifikacja incydentu i jego poziomu
- Kontrola z UODO – jak wygląda, jak się do niej przygotować, co robić, a czego się wystrzegać, proces pokontrolny
- Strategia odbudowy wizerunku (image fixing)

5.7. **Podsumowanie**

- Co warto zapamiętać?
- Co można zrobić już dziś?
- Nad czym pracować długoterminowo?

Uwagi dotyczące obu rodzajów szkoleń:

6. Oprócz szkolenia teoretycznego Wykonawca powinien zrealizować ćwiczenia praktyczne obejmujące tematykę szkolenia (np. w formie Qiuz/gry lub ćwiczenia).
7. Wykonawca zobowiązany jest przeprowadzić testy sprawdzające wiedzę – na wstępie szkolenia i na jego zakończenie. Po zakończeniu szkolenia, zostanie udostępniona ankieta ewaluacyjna szkolenia, a wynik ankiety w formie raportu zostanie przekazany Zamawiającemu.
8. Dokumentowanie prowadzonych zajęć i działań nastąpi poprzez prowadzenie list obecności, na drukach oznaczonych logotypami, przygotowanych przez Zamawiającego. Listy obecności zostaną przekazane Zamawiającemu niezwłocznie po przeprowadzeniu szkolenia.
9. Wykonawca jest zobowiązany w terminie do 7 dni kalendarzowych po zakończeniu realizacji Przedmiotu zamówienia dostarczyć certyfikaty ukończenia szkolenia, zgodnie z listą obecności.
10. Zamawiający wskazuje jako miejsce przeprowadzenia szkolenia siedzibę Zamawiającego lub inną lokalizację wskazaną przez Zamawiającego w odległości do 10 km od siedziby

Zamawiającego. Rezerwacja miejsca prowadzenia zajęć jest po stronie i na koszt Zamawiającego.

11. Ekran odpowiedniej wielkości lub rzutnik będzie udostępniony przez Zamawiającego. Zamawiający zapewni również dostęp do energii elektrycznej (gniazdko).
12. W szkoleniu będzie brało udział do 17 osób – pracownicy Zamawiającego, które zostaną podzielone na maksymalnie dwie grupy (jedna grupa zakres podstawowy i jedna grupa obejmująca kadrę zarządzającą oraz informatyków).
13. Wykonawca zobowiązuje się w terminie 7 dni od dnia podpisania umowy dostarczyć Zamawiającemu:
    1) proponowane terminy szkolenia;
    2) szczegółowy zakres merytoryczny szkolenia;
    3) dzienny harmonogram szkolenia.

    Wykonawca zobowiązany jest do współpracy i konsultacji z Zamawiającym oraz do wprowadzania poprawek w sporządzanej przez siebie dokumentacji zgodnie z sugestiami Zamawiającego na każdym etapie realizacji zamówienia. Szkolenia będą przeprowadzone po ostatecznej akceptacji dokumentacji przez Zamawiającego.
14. W ramach organizacji szkolenia Wykonawca zapewni:
    1) materiały szkoleniowe, obejmujące szczegółowy zakres merytoryczny szkolenia i harmonogram dzienny szkolenia (materiały zostaną przekazane każdemu uczestnikowi szkolenia w wersji elektronicznej – nieodpłatnie, na własność);
    2) oznakowanie w odpowiedni sposób materiałów szkoleniowych przekazanych uczestnikom (zgodnie z zasadami określony w konkursie „Cyberbezpieczne Wodociągi”; wszelkie materiały dostępne są na stronie: https://www.gov.pl/web/cppc/cyberbezpieczne-wodociagi w zakładce Materiały informacyjno-promocyjne);
    3) wydanie Zamawiającemu szkolenia zaświadczeń/certyfikatu o ukończeniu szkolenia dla każdego uczestnika;
    4) kadrę trenerską posiadającą wiedzę, doświadczenie i umiejętności adekwatne do rodzaju i zakresu merytorycznego szkolenia, zdolną do pełnej realizacji wymogów związanych z prowadzeniem szkolenia;