**TOM III**

**OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ)**

NAZWA ZAMÓWIENIA

Dostawa **serwerów** wraz z niezbędną **infrastrukturą**

**Zadanie jest realizowane w ramach projektu pn. : „Wdrożenie elektronicznych usług publicznych w zakresie gospodarki wodno-kanalizacyjnej oraz nekropolii na terenie Gminy Nowogrodziec” nr RPDS.02.01.01-02-0022/17**

## Spis treści

# 1. Zamawiający

Nazwa (firma) i adres Zamawiającego (Beneficjenta)

Hydro - Tech Spółka z o.o.
ul. Młyńska 3a
59 - 730 Nowogrodziec

wpisana do Krajowego Rejestru Sądowego pod nr 0000218357 prowadzonego przez Sąd Rejonowy dla miasta Wrocławia

NIP: 612-16-31-843
REGON: 230914302

Tel.: (075) 734-96-00
Faks: (075) 734-96-15

E-mail: hydro@nowogrodziec.pl,
Strona internetowa: www.hydrotech.info.pl, www.bip.hydrotech.ig.pl

# 2. Projekt

## 2.1. Nazwa projektu

„Wdrożenie elektronicznych usług publicznych w zakresie gospodarki wodno-kanalizacyjnej oraz nekropolii na terenie Gminy Nowogrodziec”

## 2.2. Numer projektu

RPDS.02.01.01-02-0022

## 2.3. Umowa o dofinansowanie

Umowa nr RPDS.02.01.01-02-0022/17-00 z dnia 21.03.2019 r.

## 2.4. Cel projektu

Usprawnienie realizacji procesów biznesowych obsługi klienta w zakresie usług publicznych dotyczących gospodarki wodno-ściekowej oraz zarządzania cmentarzami.

## 2.5. Opis projektu

Projekt „Wdrożenie elektronicznych usług publicznych w zakresie gospodarki wodno-kanalizacyjnej oraz nekropolii na terenie Gminy Nowogrodziec" nr RPDS.02.01.01-02-0022 obejmuje następujące zadania:

| Lp. | Nazwa Zadania / Podzadania | Źródło finansowania |
|---|---|---|
| **1.** | **Wykonanie i wdrożenie platformy e-cmentarze** | **RPO WD** |
| **2.** | **Wykonanie i wdrożenie platformy e-BOK** | **RPO WD** |
| **3.** | **Dostawa 1500 szt. nakładek na wodomierze i 2 szt. zestawów inkasenckich** | **RPO WD** |
| **4.** | **Dostawa serwerów wraz z niezbędną infrastrukturą** | **RPO WD** |

Opis działań planowanych do realizacji w ramach przedsięwzięcia:

1) Wdrożenie platformy e-cmentarze umożliwiającej elektroniczne przeszukiwanie zasobów gminnych cmentarzy, wnoszenie opłaty za miejsce na cmentarzu, zlecenie dodatkowych płatnych usług.
2) Zaprojektowanie, wykonanie i wdrożenie systemu informatycznego realizującego e-usługi: eBOK składający się z modułów: e-wodkan, e-faktury, e-zgłoszenie.
3) Dostawa 1500 szt. nakładek na wodomierze oraz 2-ch zestawów inkasenckich do radiowego odczytu wraz z oprogramowaniem do zdalnego (radiowego) odczytu wodomierzy.
4) Dostawa serwerów wraz z niezbędną infrastrukturą oraz montaż i uruchomienie ich w miejscu wskazanym przez Zamawiającego (siedziba spółki).

# 3. Dostawa sprzętu IT

Wymagania dotyczące przedmiotu zamówienia:

1) Oferowany sprzęt musi być: fabryczne nowy, nie może być obciążony prawami na rzecz osób trzecich, sprzedawany przez legalny kanał dystrybucji na rynek polski lub rynki wielu krajów, w tym na rynek polski, kompletny (z pełnym okablowaniem, materiałami startowymi, niezbędnym wyposażeniem np.: baterie, złącza, zasilacze, wtyczki i itp.), gotowy do pracy, aktualne produkowany na rynku, o parametrach nie gorszych niż wymagane przez Zamawiającego,
2) Zamawiający nie dopuszcza jakiejkolwiek ingerencji poza producentem w dostarczony sprzęt przed dostawą do Zamawiającego,
3) Wykonawca wraz z dostawą sprzętu dostarczy instrukcje obsługi/użytkowania w języku polskim lub języku angielskim

4) Wykonawca wraz z dostawą sprzętu dostarczy karty gwarancyjne (odrębne dla każdego urządzenia), zgodne z wymogami SIWZ.
5) Dostawa sprzętu obejmuje transport, wniesienie, uruchomienie i konfigurację, a także sprawdzenie poprawności działania urządzeń (czynności, które należy wykonać, aby oferowane urządzenia były podłączone, uruchomione i poprawnie działające),
6) Przedmiot zamówienia będzie dostarczony transportem Wykonawcy, na jego koszt i ryzyko,
7) Ewentualne szkody powstałe w związku z wnoszeniem i montażem sprzętu, zostaną usunięte na koszt Wykonawcy.
8) Dostarczone elementy oraz dostarczone wraz z nimi oprogramowanie muszą pochodzić z oficjalnych kanałów dystrybucyjnych producentów, zapewniających w szczególności realizację uprawnień gwarancyjnych.
9) Cały dostarczony sprzęt musi zostać wyprodukowany zmontowany nie dalej niż 12 miesięcy przed dniem dostarczenia.
10) Wykonawca zobowiązany jest do znakowania dostarczanych urządzeń i sprzętu plakietkami informującymi o dofinansowaniu projektu ze środków Regionalnego Programu Operacyjnego Województwa Dolnośląskiego na lata 2014-2020 zgodnie z obowiązującymi wytycznymi. Projekty plakietek informacyjnych muszą zostać zaakceptowane przez Zamawiającego.
11) Na infrastrukturze musi zostać zainstalowane odpowiednie wymagane do poprawnej pracy systemu oprogramowanie w tym oprogramowanie serwerowe oraz oprogramowanie zarządzające i monitorujące.

## 3.1. Zestaw komputerowy (2 sztuki)

Każdy z 2-ch zestawów komputerowych będzie zawierał następujące elementy:

1.1. Jednostka robocza o parametrach nie gorszych niż:

- CPU i7 najwyższa dostępna generacja, min 6 rdzeni
- ilość zainstalowanych dysków – 2 szt.
- pojemność jednostkowa dysku –240 GB SSD
- typ dysku – SATA 1TB
- sprzętowy sterownik macierzy RAID0
- pamięć RAM – 16GB
- rodzaj pamięci – DDR4, RDIMM 2400MHz
- ilość portów sieciowych – 2 szt.
- typ kart sieciowych - 1Gigabit
- interfejs karty graficznej HDMI
- napęd DVD-RW – tak
- ilość interfejsów USB 2.0 – 2 szt.
- Ilość interfejsów USB 3.0 – 2 szt., zewnętrzne USB 2.0 - 4 szt.

- system operacyjny w języku polskim 64bit z możliwością połączeń zdalnych minimum 1 w jednym czasie - z zestawem nośników

1.2. UPS - minimalne wymagania::

- umożliwiający nieprzerwaną pracę urządzeń, o których mowa w pkt. 1.1 oraz 1.3 niniejszego rozdziału przez 1h
- z funkcją BY-PASS
- wyposażony w wyświetlacz LCD z możliwością podglądu:
    - obciążenia
    - poziomu naładowania akumulatorów
    - pobieranej energii
    - oprogramowanie monitorujące zasilanie (zabezpieczenie przeciw przepięciowe i przeciw wyładowaniom atmosferycznym)

1.3. Monitor - minimalne wymagania:

- przekątna 24”
- rozdzielczość 1920x1080 (full HD)
- format obrazu 16:9
- technologia podświetlenia LED
- rodzaj interfejsu HDMI

1.4. Klawiatura bezprzewodowa

1.5. Mysz optyczna, bezprzewodowa, podłączana poprzez port USB, min. dwuklawiszowa, z rolką.

1.6. Gwarancja, która będzie obejmować fazę realizacyjną przedsięwzięcia do jednego roku z podstawową gwarancją w reżimie NBD on-site (czas reakcji następny dzień roboczy) i trwać min. 5 lat.

1.7. System operacyjny Windows 10 Pro PL 64-bit

1.8. Oprogramowanie biurowe: pakiet MS Office Professional 2019 w skład którego wchodzą co najmniej programy biurowe Word, Excel, Outlook, OneNote, PowerPoint i Publisher – lub równoważny pakiet biurowy

## 3.2. Szafa rack 19" (1 sztuka)

W ramach wdrożenia **szafę należy umieścić w klimatyzowanym pomieszczeniu technicznym Wykonawcy** w sposób umożliwiający swobodny dostęp do przednich i tylnych drzwi a jeżeli boki szafy również będą demontowane to tak aby można było swobodnie dokonać demontażu w celach konserwacyjnych. Szafa musi zostać wypoziomowana i a zasilanie do wnętrza szafy ma zostać doprowadzone w odpowiednim oplocie/peszlu aby zminimalizować ryzyko uszkodzenia kabla.

| Lp. | Wymagane minimalne parametry techniczne |
|---|---|
| 1. | Szafa wysokość wewnętrzna minimum 40U |
| 2. | szafa przeznaczona do zastosowań wewnątrz pomieszczeń serwerowych |
| 3. | Drzwi przednie perforowane otwierane na klamkę z zamkiem |
| 4. | drzwi tylne stalowe perforowane dwuskrzydłowe uchylne z zamkiem |
| 5. | drzwi boczne demontowane na zatrzaskach z możliwością montażu zamka |
| 6. | Szafa musi zawierać co najmniej dwie półki do umieszczenia urządzeń typu Tower montowane jednocześnie do przednich i tylnych szyn rack. |
| 7. | Wymiary szafy powinny uwzględniać najdłuższy z elementów w niej instalowany – nie dopuszcza się pozostawienia niezamkniętych lub zdemontowanych drzwi. |
| 8. | Gwarancja na urządzenie minimum 3 lata - NDB Next Business Day - serwis u klienta następnego dnia roboczego po zgłoszeniu usterki. |
| 9. | minimalne, niezbędne wyposażenie – min 2 listwy zasilające po 6 gniazd, panel wentylacyjny z min 2 wentylatorami |

## 3.3. Serwery wirtualizacji (2 sztuki)

Serwery muszą zostać połączone i skonfigurowane do współpracy z macierzą z wykorzystaniem witalizatora aby zapewnić wysoką dostępność uruchomionych systemów gości. Wirtualizator w ramach dostawy musi zostać zainstalowany i skonfigurowany do pracy z systemami zamawiającego, w tym również należy dokonać migracji obecnie wykorzystywanych systemów tj., TYTAN SQL firmy TYTAN odpowiadający za proces sprzedaży, SYMFONIA firmy SAGE zapewniające obsługę Zamawiającego w zakresie księgowości, kadr i płac oraz THB SEZaM korelujący czynsze i zasoby.

| Lp. | Wymagane minimalne parametry techniczne |
|---|---|
| 1. | Montaż w szafie RACK |
| 2. | Minimalna ilość RAM: 32GB |
| 3. | Półprzewodnikowy nośnik pamięci (w trybie dual) pozwalający na uruchomienie hypervisora systemu wirtualizacji o pojemności minimum 32GB (jeżeli hypervisor wymaga |

| | |
|---|---|
| | większej pojemności to ma zostać zastosowana adekwatna do pełnego uruchomienia środowiska wirtualizacji) |
| 4. | Karta sieciowa dwuportowa, pozwalająca na połączenie iSCSI z macierzą dyskową (równoważnie dopuszcza się zastosowanie połączenia FC) |
| 5. | Jeden fizyczny procesor zgodny z architekturą x86 |
| 6. | Procesor z min. 6 fizycznymi rdzeniami |
| 7. | Gwarancja na urządzenie minimum 3 lata - NDB Next Business Day - serwis u klienta następnego dnia roboczego po zgłoszeniu usterki. |

## 3.4. Hypervisor systemu wirtualizacji (1 sztuka)

Hypervisor ma zostać uruchomiony na klastrze serwerów **(3.3 Serwery wirtualizacji (2 sztuki))** z zdefiniowanym miejscem przechowywania systemów zwirtualizowanych na macierzy dyskowej **(3.5 Macierz dyskowa (1 sztuka)).**

| **Lp.** | **Wymagane minimalne parametry techniczne** |
|---|---|
| 1. | Hypervisor dostarczony w ramach postępowania może być otwarto źródłowy lub komercyjny lecz w tym wypadku wymaga dostępu do poprawek i aktualizacji przez okres 5 lat. |
| 2. | W ramach wdrożenia należy zainstalować i skonfigurować na opisanych w pkt. **3.3 Serwerach wirtualizacji (2 sztuki)** instancję Hypervisora z automatycznym – w przypadku awarii – uruchomieniem systemów gości na działającym serwerze (klaster niezawodnościowy). A także uruchomić podstawową instancję systemu zwirtualizowanego zawierającego system operacyjny (wraz z licencją jeżeli wybrany system będzie tego wymagał) pełniący funkcję serwera SYSLOG zbierającego informacje z systemów Zamawiającego takich jak: UTM, WAF oraz jeżeli to możliwe z macierzy i UPS (np. poprzez połączenie USB, zbieranie zdarzeń do dziennika logów). Rejestry syslog powinny być replikowane/przesyłane na urządzenie backupowe, w którego posiadaniu jest Zamawiający.<br><br>Wdrożenie systemu uznaje się za zrealizowane gdy wszystkie systemy niezbędne do prezentacji treści na portalu e-BOK, zostaną uruchomione na odpowiedniej liczbie systemów gości w ramach Hypervisora, którego konfiguracja zapewni dostępność nawet w przypadku awarii jednego z serwerów klastra niezawodnościowego. W przypadku realizacji systemu e-BOK poza lokalizacją sieci wewnętrznej Zamawiającego powyższego zapisu nie stosuje się. |
| | Wykonawca zapewni Gwarancję na przeprowadzone prace wdrożeniowe minimum 3 lata - NDB Next Business Day - serwis następnego dnia roboczego po zgłoszeniu usterki. |

## 3.5. Macierz dyskowa (1 sztuka)

Macierz będzie stanowiła punkt wspólny lokalizacji danych i serwerów wirtualnych uruchamianych na serwerach. System wirtualizatora należy skonfigurować w taki sposób aby codziennie wykonywana była kopia zapasowa serwerów gości a pliki archiwizacyjne replikowane były również na urządzenie kopii zapasowej posiadane przez Zamawiającego. Retencja danych powinna zakładać przetrzymywanie przynajmniej jednej kopii tygodniowej oraz minimum 3 miesięcy wstecz (jedna pełna kopia na miesiąc).

| Lp. | Wymagane minimalne parametry techniczne |
|---|---|
| 1. | Montaż w szafie RACK |
| 2. | Pozwalająca na montaż minimum 12 dysków 3,5” |
| 3. | Pojemność przestrzeni dyskowej minimum 1TB w RAID 1 z wykorzystaniem dysków o prędkości obrotowej minimum 10krpm |
| 4. | Karta iSCSI posiadająca minimum 4 porty (równoważnie dopuszcza się zastosowanie karty FC) |
| 5. | Port Ethernet dedykowania do zarządzania |
| 6. | Gwarancja na urządzenie minimum 3 lata - NDB Next Business Day - serwis u klienta następnego dnia roboczego po zgłoszeniu usterki. |

## 3.6. Zasilacz UPS (1 sztuka)

Zasilacz w ramach dostawy ma zostać zainstalowany w szafie i podłączony kompletem przewodów zapewniając zasilanie wszystkich urządzeń służących do dostarczania systemów i aplikacji sieciowych takich jak: serwery, macierz, UTM, WAF, Ochrona E-mail.

| Lp. | Wymagane minimalne parametry techniczne |
|---|---|
| 1. | Montaż w szafie RACK lub wolnostojący (preferowany wolnostojący) |
| 2. | Wydajność urządzenia pozwala na utrzymanie zasilania przez czas minimum 10min przy założeniu obciążenia na poziomie 3000W |
| 3. | Komplet okablowania umożliwiający podłączenie zasilania zarówno jednostki UPS jak i wszystkich urządzeń zainstalowanych w szafie rack |
| 4. | Zapewnienie odpowiednich listew zasilających montowanych do szyn RACK 19” pozwalających na podłączenie wszystkich urządzeń zainstalowanych w szafie rack |
| 5. | Gwarancja na urządzenie (z wyłączeniem baterii akumulatorów) minimum 3 lata - NDB Next Business Day - serwis u klienta następnego dnia roboczego po zgłoszeniu usterki. |

## 3.7. UTM nowej generacji zabezpieczający sieć i serwery usług wraz z subskrypcją sygnatur bezpieczeństwa (1 sztuka)

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS. Powinna istnieć możliwość dedykowania administratorów do poszczególnych instancji systemu.

Wdrożenie ma obejmować skonfigurowanie urządzenia do pracy w zakładzie zarówno pod kątem dostarczanych systemów WAF jak i polityk bezpieczeństwa użytkowników komputerów osobistych, serwerów wewnętrznych, serwerów aplikacji oraz usług dostarczanych do klientów Zamawiającego w przestrzeni DMZ.

| Lp. | Wymagane minimalne parametry techniczne |
|---|---|
| 1. | System musi wspierać IPv4 oraz IPv6 w zakresie:<br>• Firewall.<br>• Ochrony w warstwie aplikacji.<br>• Protokołów routingu dynamicznego. |
| 2. | Monitoring i wykrywanie awarii<br>• Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.<br>• Monitoring stanu realizowanych połączeń VPN. |
| 3. | Interfejsy:<br>• System realizujący funkcję Firewall musi dysponować minimum 10 portami Gigabit Ethernet RJ-45.<br>• W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q. |
| 4. | Parametry wydajnościowe:<br>• W zakresie Firewall'a obsługa nie mniej niż 1,2 mln. jednoczesnych połączeń oraz 30 tys. nowych połączeń na sekundę.<br>• Przepustowość Stateful Firewall: nie mniej niż 3 Gbps<br>• Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 500 Mbps<br>• Wydajność szyfrowania IPSec VPN: nie mniej niż 2 Gbps<br>• Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 400 Mbps<br>• Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 180 Mbps.<br>• Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 135 Mbps. |
| 5. | Funkcje Systemu Bezpieczeństwa: |

| | |
|---|---|
| | W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:<br>• Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.<br>• Kontrola Aplikacji.<br>• Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.<br>• Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.<br>• Ochrona przed atakami - Intrusion Prevention System.<br>• Kontrola stron WWW.<br>• Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3, IMAP.<br>• Zarządzanie pasmem (QoS, Traffic shaping).<br>• Analiza ruchu szyfrowanego protokołem SSL.<br>• Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). |
| 6. | Polityki, Firewall<br>• Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.<br>• System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:<br>o Translację jeden do jeden oraz jeden do wielu.<br>o Dedykowany ALG (Application Level Gateway) dla protokołu SIP.<br>• W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. |
| 7. | Routing i obsługa łączy WAN<br>• W zakresie routingu rozwiązanie powinno zapewniać obsługę:<br>o Routingu statycznego.<br>o Policy Based Routingu.<br>o Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.<br>• System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN. |
| 8. | Kontrola Antywirusowa<br>• Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).<br>• System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. |

| | |
|---|---|
| | • System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).<br>• System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze. |
| 9. | Ochrona przed atakami<br>• Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.<br>• System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.<br>• Baza sygnatur ataków powinna zawierać minimum 6500 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.<br>• Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.<br>• System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.<br>• System musi dysponować sygnaturami do ochrony przed atakami na systemy przemysłowe SCADA.<br>• Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.<br>• Wykrywanie i blokowanie komunikacji C&C do sieci botnet. |
| 10 | Kontrola aplikacji<br>• Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.<br>• Baza Kontroli Aplikacji powinna zawierać minimum 2500 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.<br>• Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.<br>• Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.<br>• Administrator systemu musi mieć możliwość definiowania wyjątków oraz |

| | |
|---|---|
| | własnych sygnatur. |
| 11 | Zarządzanie<br>• Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.<br>• Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. |
| 12 | Logowanie<br>• Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.<br>• W przypadku kiedy usługa logowania i raportowania realizowana jest w chmurze, wykonawca musi dostarczyć stosowne licencje upoważniające do składowania logów przez okres co najmniej jednego roku. Chmura musi znajdować się w Europejskim Obszarze Gospodarczym.<br>• Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.<br>• Musi istnieć możliwość logowania do serwera SYSLOG. |
| 13 | Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:<br>• ICSA lub EAL4 dla funkcji Firewall.<br>• ICSA dla funkcji IPS lub NSS Labs w kategorii NGFW.<br>• ICSA dla funkcji SSL VPN.<br>lub równoważne, przeprowadzone przez niezależne Laboratoria testujące systemy bezpieczeństwa informatycznego. |
| 14 | Licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen Sygnatury ochrony systemów przemysłowych SCADA a także Logowanie do usługi realizowanej w chmurze **na okres 5 lat**. |

| | |
|---|---|
| 15 | System musi być objęty **serwisem gwarancyjnym producenta przez okres 5 lat**, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie co najmniej 8/5.<br><br>Opcjonalnie, system może być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 60 miesięcy.<br><br>Dla zapewnienia wysokiego poziomu usług podmiot realizujący serwis rozszerzony musi posiadać certyfikat ISO 9001 lub równoważny w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe muszą być przyjmowane w języku polskim w trybie co najmniej 8/5 [maksymalnie 24/7] przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim.<br><br>*Wykonawca w ramach rozszerzonego wsparcia technicznego w Formularzu oferty:*<br><br>*a) Oświadcza, że serwis rozszerzony na rzecz Zamawiającego świadczony będzie przez Producenta lub Autoryzowanego Dystrybutora oraz podaje*<br><br>*- adres strony internetowej serwisu,*<br><br>*- numer infolinii telefonicznej,*<br><br>*b) oświadcza, iż podmiot serwisujący posiada Certyfikat ISO 9001 lub równoważny w zakresie świadczenia usług serwisowych.* |

Wadliwość rozumie się jako uszkodzenie fizyczne, mechaniczne lub funkcjonalne powodujące iż produkt nie jest zdatny do użytku lub jego użytkowanie w zdefiniowanym obszarze funkcjonalnym jest nieprawidłowe lub znacznie odbiegające od normy przyjętej dla tego modelu urządzeń, które pojawiło się w procesie produkcyjnym i ujawniło w okresie gwarancyjnym. Zakres zobowiązań producenta musi być ujęty w ogólnej umowie licencyjnej produktu.

## 3.8. Web Application Firewall stanowiący zabezpieczenie portalu usług zlokalizowanego na serwerach wraz z subskrypcją sygnatur bezpieczeństwa na 5 lat (1 sztuka)

System ochrony aplikacji webowych oraz Firewall XML - którego zadaniem będzie wykrywanie i blokowanie ataków celujących w aplikacje webowe a następnie alarmowanie w wyniku wystąpienia określonych zdarzeń. System powinien umożliwiać lokalne logowanie oraz raportowanie w oparciu o zestaw predefiniowanych wzorców raportów. Musi istnieć możliwość implementacji systemu in-line w trybach Reverse Proxy lub Transparentnym, jak również implementacji w trybie nasłuchu.

Wdrożenie obejmować będzie konfigurację systemu zapewniającą **objęcie ochroną strony głównej Zamawiającego wraz z e-BOK oraz projektowanymi e-usługami**. Jeżeli będzie to wymagane należy przenieść stronę WWW do zasobów hypervisora wraz z uruchomieniem systemu operacyjnego i skonfigurowaniem odpowiednich usług serwera HTTP oraz skonfigurowaniem polityk na urządzeniu UTM.

| Lp. | Wymagane minimalne parametry techniczne |
|---|---|
| 1. | Tryb auto-uczenia – przyspieszający i ułatwiający implementację |
| 2. | Podział obciążenia na kilkanaście serwerów (loadbalancing) |
| 3. | Akceleracja SSL dla wybranych serwisów w centrum danych |
| 4. | Możliwość analizy poszczególnych rodzajów ruchu w oparciu o profile bezpieczeństwa (profil to obiekt określający zbiór ustawień zabezpieczających aplikacje) |
| 5. | Firewall XML realizujący z możliwością routingu w oparciu o kontent, walidacją schematów XML oraz weryfikacją WDSL. |
| 6. | Firewall aplikacji webowych chroniący przed takimi zagrożeniami jak:<br>• SQL and OS Command Injection.<br>• Cross Site Scripting (XSS).<br>• Cross Site Request Forgery.<br>• Outbound Data Leakage.<br>• HTTP Request Smuggling.<br>• Buffer Overflow.<br>• Encoding Attacks.<br>• Cookie Tampering / Poisoning.<br>• Session Hijacking.<br>• Broken Access Control.<br>• Forceful Browsing /Directory Traversal.<br>• Ochrona przed innymi zagrożeniami specyfikowanymi przez listę OWASP.<br>• DoS w warstwie aplikacji.<br>• Ochrona przed atakami typu Brute force. |
| 7. | Rozwiązanie musi obsługiwać przepustowość dla ruchu http - min **25 Mbps** |
| 8. | Aktualizacja baz sygnatur powinna być systematycznie aktualizowana zgodnie ze zdefiniowanych harmonogramem |
| 9. | System realizujący funkcje podstawowe musi obsługiwać minimum 4 interfejsy sieciowe oraz 1 wirtualny procesor |
| 10 | Możliwość logowania do zewnętrznego serwera syslog |
| 11 | Obsługa powiadomień o zdarzeniach systemowych oraz incydentach bezpieczeństwa e-mailem |
| 12 | Licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych i serwisów. Powinny one obejmować: Skanowanie aplikacji, Kontrolę antywirusową, sygnatury ochrony dla aplikacji www oraz bazy reputacyjne adresów IP na okres **5 lat.** |
| 13 | System musi być objęty serwisem gwarancyjnym producenta polegającym na naprawie w przypadku jego wadliwości oraz serwisem wsparcia technicznego w trybie 8/5 przez okres **5 lat**. |

## 3.9. Prace konfiguracyjne oraz wdrożeniowe w zakresie uruchomienia systemów na platformach sprzętowych

W ramach niniejszego zamówienia zostanie wykonana usługa instalacji dostarczonego przez Wykonawcę Sprzętu komputerowego oraz konfiguracji środowiska obejmująca konfiguracje urządzeń sieciowych u Zamawiającego w tym:

1. fizyczna instalacja w szafach Rack serwerów i infrastruktury,
2. instalacja, podłączenie, konfiguracja elementów sieciowych i serwerowych,
3. konfiguracja systemów operacyjnych oraz baz danych,
4. testy poprawności działania systemów.

**Konfiguracja urządzeń**

Szczegółowe informacje dotyczące konfiguracji poszczególnych elementów systemu mogą być ograniczone prawem autorskim Wykonawców, a jednocześnie ich publiczne ujawnienie może wiązać się ze znacznym obniżeniem bezpieczeństwa systemu jako całości. Zamawiający, po podpisaniu umów z Wykonawcami systemów **e-BOK, e-cmentarze**, przekaże Wykonawcy **pełną informację związaną z fizycznym połączeniem poszczególnych urządzeń z dokładnością do poszczególnych portów**. Jednocześnie zakres ingerencji Wykonawcy wewnątrz poszczególnych systemów musi stać się przedmiotem odrębnych ustaleń pomiędzy nim a Zamawiającym lub Wykonawcą poszczególnych systemów.

## 3.10. Termin realizacji

**Termin dostawy serwerów wraz z niezbędną infrastrukturą oraz montaż i uruchomienie ich w miejscu wskazanym przez Zamawiającego (siedziba spółki)- 30 dni** od dnia podpisania umowy