## Załącznik nr 1 do SIWZ

Przedmiot Zamówienia

1. Wstęp

2. Opis przedmiotu zamówienia

* Przedmiotem zamówienia jest dostawa usług opartych o zarządzane i administrowane środowiska teleinformatyczne w architekturze chmury obliczeniowej
* Zamawiający szacuje, że maksymalna liczba uruchamianych maszyn wirtualnych nie przekroczy 10 instancji.

2.1. Wymagania prawne

|  |  |
| --- | --- |
| Wymagania | Spełnia (TAK/NIE) |
| Usługa chmury obliczeniowej i sposób przetwarzania danych musi spełniać wymogi prawa polskiego w tym Ustawy o Ochronie Danych Osobowych (Dz. U. z 2014 r., poz. 1182 z późn. zm.). |  |
| Sposób świadczenia usług musi być zgodny z wymogami Rozpąrządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności (Dz. U. z 2012 r., poz. 526 z późn. zm.)., minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, a w szczególności realizować wymagania dotyczące niezaprzeczalności, integralności danych oraz monitorowania zdarzeń w oferowanym rozwiązaniu. |  |
| Dostawca usług chmury obliczeniowej musi posiadać przynajmniej certyfikat ISO 27001. |  |
| Dostawca Centrum danych musi posiadać przynajmniej certyfikat ISO 27001. |  |
| Na wniosek Zamawiającego Wykonawca zapewni przekazanie kopii aktualnych certyfikatów ISO 27001 poświadczonych za zgodność z oryginałem. |  |
| Wykonawca dostarczy pełną informację o wszystkich fizycznych lokalizacjach serwerów, na których przetwarzane są lub mogą być przetwarzane dane. |  |
| Wykonawca bez uzyskania pisemnej zgody Zamawiającego nie może zmienić fizycznej lokalizacji danych. |  |
| Wykonawca musi umożliwić dostęp do dokumentacji dotyczącej zasad bezpieczeństwa oraz środków technicznych przyjmowanych w centrach przetwarzania danych. |  |
| Wykonawca usługi jest zobowiązany przekazać pełną informację dotyczącą podwykonawców i współpracujących instytucji mających udział w realizacji usługi chmurowej. Przekazana informacja powinna umożliwić pełną ocenę wszystkich podwykonawców oraz umożliwić ocenę roli każdego z tych podmiotów jako przetwarzającego dane osobowe. |  |
| Każdy z podwykonawców traktowany jako podprzetwarzający dane osobowe powinien być związany takimi samymi „klauzulami umownymi” (zgodnie z zaleceniami GIODO <http://www.giodo.gov.pl/163/id_art/1519/j/pl> ) jak Wykonawca. Wykonawca powinien zarządzać całym łańcuchem podwykonawców i ich uprawnieniami. |  |
| Zamawiający - pozostaje wyłącznym administratorem danych osobowych przekazanych do chmury. Niedopuszczalna jest sytuacja, w której jakikolwiek Wykonawca lub podwykonawca usługi decydowałby o celach i sposobach przetwarzania danych. |  |
| Wykonawca jest zobowiązany do raportowania wszystkich incydentów bezpieczeństwa danych, ze szczególnym uwzględnieniem tych, które dotyczyć mogą danych osobowych. Wykonawca zobowiązany jest również do udzielenia wszelkiej możliwej pomocy przy zwalczaniu skutków takich incydentów bezpieczeństwa. |  |
| Wykonawca niezwłocznie i nie później jak 7 dni kalendarzowych od dnia zakończenia świadczenia usługi musi trwale usunąć dane. Trwałe i nieodwracalne usunięcie danych zostanie potwierdzone stosownym protokołem przedstawionym przez Wykonawcę. Nie usunięcie danych w terminie i nieprzedstawienie stosownego protokołu w ciągu 7 dni skutkować będzie naliczeniem kary przez Zamawiającego w wysokości 100% opłaty kwartalnej brutto określonej w umowie oraz 7 dniowym okresem (od dnia w którym naliczona została kara) na usunięcie nieprawidłowości. |  |

2.2. Wymagania licencyjne

Zamawiający wymaga:

|  |  |
| --- | --- |
| Wymagania | Spełnia (TAK/NIE) |
| Wykonawca w ramach Umowy zapewni dla środowiska wszystkie wymagane licencje zarówno serwerowe na instalowane systemy operacyjne we wskazanej przez Zamawiającego wersji. |  |
| Łączna liczba instancji wykorzystujących system operacyjny Microsoft Windows Server: 2. |  |
| Pozostałe instancje będą wykorzystywały systemy operacyjne w wersji community np. Centos, Ubuntu Server, Debian |  |

2.3. Wymagania techniczne

Zamawiający wymaga:

|  |  |
| --- | --- |
| Wymagania | Spełnia (TAK/NIE) |
| Centra przetwarzania danych, o które opiera się usługa muszą być zlokalizowane na terenie Europejskiego Obszaru Gospodarczego z gwarancją zmiany lokalizacji (w obrębie EOG) przetwarzania danych jedynie za pisemną zgodą Zamawiającego. |  |
| Wymagane jest SLA dla usług na poziomie minimum 99,5% w skali miesiąca. |  |
| Wymagana jest wewnętrzna infrastruktura sieciowa o wydajności minimalnej 100 Mbps (bez limitu danych). Zdefiniowana przepustowość musi uwzględnić wszystkie wymagania funkcjonalne. |  |
| Wymagana jest zewnetrzna infrastruktura sieciowa o wydajności minimalnej 20 Mbps (bez limitu danych). Zdefiniowana przepustowość musi uwzględnić wszystkie wymagania funkcjonalne. |  |
| Zamawiający wymaga przynajmniej 4 zewnętrznych adresów IPv4 |  |
| Infrastruktura sieciowa musi być chroniona przynajmniej za pomocą technologii Firewall, IPS, LB L4-7, WAF, AV realizując wydajność zdefiniowaną powyżej. |  |

**2.3.1 Procesory i pamięć**

Zamawiający wymaga:

|  |  |
| --- | --- |
| Wymagania | Spełnia (TAK/NIE) |
| Minimum 20 fizycznych rdzeni obliczeniowych oraz minimum 32 GB RAM. |  |
| Dostępność kreowania instancji zawierających od 1 do 20 vCPU (nie współdzielonych) oraz od 1 do minimum 32 GB RAM. |  |
| Zamawiający szacuję wykorzystanie 2vCPU per instancja. | |

2.3.2 Storage

Zamawiający wymaga:

|  |  |
| --- | --- |
| Wymagania | Spełnia (TAK/NIE) |
| Usługa musi udostępniać zasoby dyskowe w dwóch klasach wydajności.   * Klasa podstawowa: Klasa podstawowa nie mniej niż 2TB, zasoby z puli będą przydzielane wg. Potrzeb Zamawiającego. Wydajność całości storage na poziomie 10 k IOPS dla wielkości bloku 4k. * Klasa szybka: nie mniej niż 1TB, zasoby z puli będą przydzielane wg. Potrzeb Zamawiającego.. Wydajność całości storage na poziomie 30k IOPS dla wielkości bloku 4k. |  |
| Pamięć masowa (storage) musi uwzględniać mechanizmy redundancji gwarantujące dostępność zasobów w przypadku awarii (np. RAID 6, 10, itp.). |  |
| Usługa musi umożliwiać definiowania co najmniej 128 woluminów logicznych. |  |
| Każdy serwer fizyczny (tworzący chmurę) musi mieć dostęp do zasobów dyskowych po sieci o przepustowości minimalnej 2x 8 Gb/s |  |

2.4 Wymagania finansowe

* Zamawiający przewiduje jednorazową opłatę za pakiet dostarczonych usług.

2.5 Wymagania funkcjonalne

Zamawiający wymaga:

|  |  |
| --- | --- |
| Wymagania | Spełnia (TAK/NIE) |
| System zarządzania usługami chmury będącymi przedmiotem dostawy. |  |
| Mechanizmy kreowania maszyn wirtualnych tj. Microsoft Windows Server i Linux. |  |
| Mechanizmy monitorowania parametrów pracy używanych usług. |  |
| System monitoringu zbierającego informacje o wykorzystaniu zasobów chmury. |  |
| Platforma musi udostępniać usługi auto-skalowania, lokalnego i globalnego load-balancingu. |  |
| Zapewnienie usługi monitoringu obejmującej monitorowanie: dostępności sieciowej, poziomu utylizacji cpu, pamięci RAM, zasobów dyskowych, operacji IOPS, przepływów sieciowych, dostępności serwisów systemowych, odpowiedzi serwerów aplikacyjnych. |  |
| Dostępność logów dotyczących tożsamości jakichkolwiek osób wykonujących działania w obrębie usług i danych Zamawiającego. |  |
| Dostępność logów informujących o wszystkich zdarzeniach uwierzytelnienia do usługi danych Zamawiającego, zakończonych powodzeniem lub niepowodzeniem. |  |
| Mechanizmy samoobsługi użytkowników w zakresie:   * Uruchamiania usług. * Konfiguracji usług. * Uruchamianie maszyn wirtualnych na podstawie gotowych szablonów. * Rekonfiguracji maszyn wirtualnych (np. rozszerzenie pamięci RAM). * Zarządzania systemami operacyjnymi na maszynach wirtualnych. * Monitorowania usług i aplikacji Zamawiającego w trybie 24/7/365. * Monitorowanie SLA. * Przypisywania uprawnień użytkownikom i zarządzanie nimi. |  |

3. Wymagania minimalne dot. DC (centrum danych)

Zamawiający wymaga:

|  |  |
| --- | --- |
| Wymagania | Spełnia (TAK/NIE) |
| Usytuowanie w wydzielonej części (lub osobnym) budynku, chronionej przez system alarmowy, system telewizji przemysłowej oraz firmę wyspecjalizowaną w zakresie ochrony. |  |
| System monitoringu CCTV, kontrola 24/7/365. |  |
| Systemy alarmowe monitorowane 24/7/365. |  |
| Musi posiadać system wykrywania ognia i dymu. |  |
| Musi posiadać system sygnalizacji włamania i napadu. |  |
| Musi być zabezpieczone przez generator prądotwórczy, który zapewnia pracę przez minimum 24 godziny. |  |
| Musi posiadać umowę z zewnętrznym dostawcą z gwarantowanym czasem dostawy paliwa dla generatorów. |  |
| Musi gwarantować czas podtrzymania zasilania przez system zasilaczy awaryjnych UPS, nie mniejszy niż 10 minut, przy pełnym obciążeniu elektrycznym pomieszczenia serwerowego. |  |
| Musi istnieć system gaszenia, bezpieczny dla ludzi i sprzętu komputerowego. |  |
| Musi zapewnić w sposób nieprzerwany odpowiednie parametry otoczenia (temperatura, wilgotność). |  |
| Musi być zabezpieczone przed nieuprawnionym dostępem. |  |
| Musi posiadać procedury gwarantujące poprawne i nieprzerwanie działanie. |  |
| Pomieszczenia muszą być pozbawione zbędnych instalacji stanowiących źródła zagrożeń, brak instalacji wodno-kanalizacyjnych, grzewczych. |  |
| Musi być zapewniona redundancja zasilania (dwie niezależne stacje transformatorowe), systemów chłodzenia ,sieci szkieletowej i telekomunikacyjnej. |  |

4. Wymagania minimalne dot. sieci i bezpieczeństwa sieci

Zamawiający podzielił ochronę realizowaną przed maszynami wirtualnymi na trzy poziomy.

* Pierwszy poziom:
  + Ochrona DoS/DDoS – zaimplementowane rozwiązanie DDoS na warstwie sieci publicznej i mitygacja cyberataków w czasie rzeczywistym (może być realizowane automatycznie).
* Drugi poziom:
  + Network firewall, SSL termination, IP reputation blacklist, SYN floods, ICMP floods.
* Trzeci poziom:
  + OSI 7, WAF, Load Balancing, ochrona-DDoS L7.

Zamawiający wymaga:

|  |  |
| --- | --- |
| Wymagania | Spełnia (TAK/NIE) |
| Dostępu zdalnego. |  |
| Firewall |  |
| Systemu przeciwdziałania włamaniom – IPS. |  |
| Systemu wykrywania włamań - IDS. |  |
| Monitoringu i eliminacji ruchu zanonimizowanego. Ocena reputacji IP użytkownika czy hosta. W tym dodatkowe usługi zapewniające, informacje o lokalizacji, znanych źródłach ataków anonimowych proxy czy też sieciach Botnet. System powinien zawierać funkcjonalności rozwiązania Anti-Bot (reputacja adresów IP, analiza zachowania, sygnatury narzędzi typu bot). |  |
| Monitorowania łącz na podstawie przepływów (flow). |  |
| Blokowania dostępu z adresów lub podsieci. |  |
| Wykorzystywanie mechanizmów rate limit dla zdefiniowanego ruchu, adresów, sieci. |  |
| Możliwości kombinacji funkcjonalności blacklist i whitelist. |  |
| Wdrożenie reguł na podstawie, których można odrzucać niepożądany ruch sieciowy. |  |
| Wykrywania i blokowania próby skanowania portów. |  |
| Możliwość skonfigurowania wielu podsieci opartych o warstwę 2 lub mechanizm SDN i sterowanie ruchem pomiędzy nimi. |  |
| Możliwość definiowania VLAN i definiowania ich na wirtualnym przełączniku. |  |
| Możliwość samodzielnego definiowania adresów z zakresu adresów prywatnych (RFC 1918). |  |

4.1. Dostęp zdalny

Usługa musi umożliwiać zestawienie bezpiecznego połączenia VPN.

Poniżej wymagania funkcjonalne wymagane przez Zamawiającego:

|  |  |
| --- | --- |
| Wymagania | Spełnia (TAK/NIE) |
| Możliwość zestawienia bezpiecznej komunikacji VPN: L2TP, SSL, IPSec (25 Mbps, 10 jednoczesnych użytkowników). |  |
| Obsługa trybów: tunelowanie aplikacji, pełny dostęp. |  |
| Uwierzytelnienie użytkowników przy wykorzystaniu certyfikatów, hasła, loginu. |  |
| Wsparcie dla platform klientów VPN: Windows, Linux. |  |
| Definiowanie reguł dostępu użytkownika bazując na listach uwzględniających parametry warstwy 4 oraz 7 modelu ISO OSI. |  |
| Funkcja raportowania, uwzględniająca błędne uwierzytelnienie, nazwę użytkownika, przydzielone zasoby, lokalizację geograficzną. |  |
| Obsługa funkcji site-to-site IPSec VPN |  |
| Zapewnienie konfiguracji VPN chmury do infrastruktury Zamawiającego. Część aplikacji Zamawiającego zlokalizowanych w siedzibę Szpitala będzie stale wymieniać dane z środowiskiem chmury. |  |

4.2 Firewall oraz IPS/IDS

Wykonawca zobowiązany jest do ochrony przed wszelkimi atakami osób trzecich, których celem jest zaburzenie normalnej pracy serwisów i aplikacji. Wymaganym jest zapewnienie takiego poziomu bezpieczeństwa, który zminimalizuje możliwości dokonania włamania lub uzyskania jakiegokolwiek nieautoryzowanego dostępu bądź przerwania pracy.

Firewall powinien posiadać minimum następujące funkcjonalności:

|  |  |
| --- | --- |
| Wymagania | Spełnia (TAK/NIE) |
| Normalizację protokołów na poziomie warstwy 7. |  |
| Brama bezpieczeństwa, która realizuje funkcje Firewall’a z możliwością zarządzania pasmem QoS. |  |
| Rozwiązanie musi realizować pełną inspekcję stosu na poziomie aplikacji i precyzyjną kontrolę przy użyciu zdefiniowanych zasad. |  |
| Identyfikacja nieznanego ruchu oraz zarządzanie nim. |  |
| Identyfikowanie aplikacji niezależnie od portu, protokołu, metody obchodzenia zabezpieczeń lub deszyfrowania. |  |
| Ochrona w czasie rzeczywistym przed znanymi, nieznanym zagrożeniami związanymi z aplikacjami. |  |
| Systematyczne zarządzanie nieznanym ruchem. |  |
| Kontrolowanie ruchu SSH (np. wykrywanie przekierowania portów). |  |
| Rozpoznanie klasyfikacja i kontrola indywidualnych funkcji aplikacji. |  |
| Zdolność identyfikowania aplikacji na wszystkich portach, niezależnie od stosowanych protokołów, szyfrowania SSL czy sposobów terminacji mających na celu uniknięcie wykrycia. |  |
| Zapewnianie ochrony w czasie rzeczywistym przed atakami oraz złośliwym oprogramowaniem osadzonym w ruchu sieciowym związanym z użytkowaniem aplikacji. |  |
| Rozwiązanie musi zapewniać funkcjonalność stanowej zapory sieciowej umożliwiającej kontrolę ruchu sieciowego oraz ochronę przed atakami typu DoS w warstwie 3 i 4 ISO/OSI. |  |
| Pełnienie punktu kontroli dostępu na podstawie zasad (akceptowanie/odrzucanie) dla całego ruchu sieciowego. |  |
| Eliminowanie zagrożeń przy użyciu pozytywnego modelu kontroli, czyli zezwalać na określony ruch sieciowy i blokować pozostały. |  |
| Musi zapewnić ochronę w zakresie Firewall opartą na technologii StateFull Inspection. |  |
| W przypadku kontroli ruchu musi uwzględniać kierunek przepływu pakietów, protokoły i usługi sieciowe, stan połączenia oraz dane aplikacyjne (m.in. obsługa fragmentacji IP, ochrona systemu operacyjnego przed atakami, exploitami oraz DoS). |  |
| Musi umożliwiać dynamiczną i statyczną translację adresów NAT, reguły NAT generowane automatycznie lub definiowane ręcznie. |  |
| Musi pełnić rolę ściany ogniowej śledzącej stan połączeń z funkcją weryfikacji informacji charakterystycznych dla warstwy aplikacji. |  |
| Analiza protokołów i aplikacji na zgodność z RFC. |  |
| Analiza sygnatur ataków. |  |
| Analiza ruchu w sieci. |  |
| Wykrywanie i blokowanie zagrożeń typu nadużycie protokołu, próby tunelowania, oprogramowania typu exploit, kontrola aplikacji, ataki ogólnego typu bez predefiniowanych sygnatur, ruchu generowanego przez szkodliwe oprogramowanie, podatności serwera i klienta wraz z możliwością definiowania własnych sygnatur. |  |
| Musi umożliwić prace w trybie IPS (In-line). |  |
| Musi wykrywać ataki w oparciu o sygnatury oraz o wykrywanie anomalii. |  |
| Możliwość definicji reakcji z dokładnością do jednej sygnatury. |  |
| Możliwość grupowania sygnatur ataków. |  |
| Musi umożliwić obsługę co najmniej 20 VLAN. |  |
| Rozpoznawanie, monitorowanie i blokowanie aplikacji na podstawie zdefiniowanych sygnatur przez producenta. |  |

4.3 Ochrona DDOS

W zakresie wykrywania ataków Zamawiający wymaga:

|  |  |
| --- | --- |
| Wymagania | Spełnia (TAK/NIE) |
| Usługa, monitoruje ruch do i od chronionej podsieci w czasie rzeczywistym. |  |
| Usługa, zapewnia wykrywanie anomalii polegających na przekroczeniu wartości uważanych za normalne w ruchu Internetowym w szczególności pakietów TCP SYN, TCP RST, TCP Null, ICMP, IP Null, IP Fragmented, DNS. |  |
| System realizujący usługę na podstawie danych historycznych wyznacza oczekiwaną wartość ruchu do i od chronionej podsieci o danej porze dnia w danym dniu tygodnia. |  |
| Usługa zapewnia wykrywanie anomalii polegających na znaczącym przekroczeniu wolumenu ruchu w stosunku do wcześniej wyznaczonych wartości oczekiwanych ruchu. |  |

W zakresie mitygacji (filtrowania) ataków Zamawiający wymaga:

|  |  |
| --- | --- |
| Wymagania | Spełnia (TAK/NIE) |
| Usługa zapewnia filtrowanie ruchu z błędnymi nagłówkami IP/TCP/UDP. |  |
| Usługa zapewnia odrzucanie lub przepuszczanie na bazie zdefiniowanych filtrów operujących na informacjach w nagłówka warstwy 3-ciej i 4-tej modelu OSI. |  |
| Usługa zapewnia filtrowanie ruchu na określonych portach TCP/UDP na podstawie zawartości pola danych w oparciu o wyrażenia regularne. |  |
| Usługa chroni przed atakami ze „spoofowanymi” (udawanymi) adresami źródłowymi IP |  |
| Usługa zapewnia filtrowanie nieprawidłowych zapytań HTTP. |  |
| Usługa zapewnia blokowanie ruchu od stacji końcowych przekraczających progi dla operacji HTTP na sekundę per serwer lub per URL. |  |
| Usługa zapewnia filtrowanie ruchu w oparciu o wyrażenia regularne dotyczące nagłówków HTTP. |  |
| Usługa zapewnia ochronę przez atakami typu „slow lories” |  |
| Usługa zapewnia wykrywanie i filtrowanie pakietów z nieprawidłowymi nagłówkami SSL/TLS lub nagłówkami SSL/TLS które są poza sekwencją. |  |
| Usługa zapewnia blokowane sesji jeżeli podczas negocjacji SSL/TLS klient zażąda nadmiernej ilości metod kryptograficznych lub rozszerzeń użytkownika. |  |
| Usługa zapewnia wykrywanie i rozłączanie sesji jeżeli negocjacja SSL/TLS nie zakończy się w zadanym czasie. |  |
| Usługa zapewnia blokowanie ruchu z hostów dla których występuje nadmierna liczba nieprawidłowych, nadmiarowych lub niekompletnych sesji SSL. |  |
| Usługa monitoruje negocjację SSL dla wszystkich portów na których mogą być stosowane aplikacje zabezpieczone protokołem TLS: HTTPS. |  |
| Usługa chroni przed atakami pochodzącymi od sieci botnetowych (komputerów zainfekowanych w sposób umożliwiające zdalne sterowanie przez hackerów) poprzez filtrowanie na podstawie na bieżąco aktualizowanych sygnatur zawierających listę adresów IP. |  |
| Usługa chroni przed atakami pochodzącymi z sieci botnetowych poprzez wykrywanie źródeł ataku o wolumenie przekraczającym zadane wartości. Wartości progowe są definiowalne zarówno dla całości ruchu jak i do części ruchu zdefiniowanego za pomocą filtru. |  |