Załącznik nr 2. Opis Przedmiotu Zamówienia (OPZ)

1. Zamawiający wymaga dostarczenia usług hostingowych w oparciu o chmurę

1.1. Wymagania szczegółowe infrastruktury udostępnionej jako chmura :

1.1.1. Dwa niezależne Centra Przetwarzania Danych (CPD) – jedno podstawowe (PCPD)oraz drugie zapasowe (ZCPD) w innej lokalizacji.

1.1.2. Pomiędzy  oboma CPD

1.1.2.1. połączenie redundantne

1.1.2.2. minimum 1Gb/s

1.1.2.3. z opóźnieniem nie większym niż 2ms.

1.1.2.4. Ruch pomiędzy CPD musi być szyfrowany minimum za pomocą algorytmu AES128.

1.1.3. W CPD routing do sieci Internet z wykorzystaniem protokołu BGP4, przynajmniej dwa łącza do operatorów.

1.1.4. Łącza do operatorów muszą być o przepływności minimum 1Gb/s każde.

1.1.5. Realizacja BGP musi się odbywać w ramach własnego numeru autonomicznego AS oraz własnej adresacji PI lub PA usługodawcy.

1.1.6. Routing do największych krajowych sieci Internetowych (np. Orange, Netia) musi odbywać się z opóźnieniami nie większymi niż 10ms (całkowite RTT).

1.1.7. PCPD (główne) musi spełniać normę Rated 3 (dawna Tier 3) zgodnie z TIA-942, chyba, że Zamawiajacy dopuścił niższe wymagania. Zamawiajacy nie wymaga certyfikacji,

1.1.8. PCPD musi być wyposażone w redundancję zasilania oraz generator prądotwórczy.

1.1.9. PCPD musi być zabezpieczone przed pożarem za pomocą gaszenia gazowego.

1.1.9.1. W przypadku planowanych testów systemu przeciwpożarowego Wykonawca poinformuje o tym zamawiajacego z 7 dniowym wyprzedzeniem i dołoży starań, by nie odbiło się to negatywnie na elementach infrastruktury.

1.1.10. CPD musi posiadać środki ochrony fizycznej – zabezpieczenia fizyczne, system kontroli dostępu,  monitoring 24h oraz procedury dostępowe.

1.2. Wszystkie maszyny wirtualne muszą być chronione przez dwa  (jeden na każde CPD) firewalle  typu Next Generation Firewall (NGN-FW).

1.2.1. NGN-FW musi chronić infrastrukturę przed atakami z wykorzystaniem znanych podatności

1.2.2. oraz zapewniać inspekcję na poziomie aplikacyjnym (warstwa L7 ISO/OSI).

1.2.2.1. Identyfikacja aplikacji nie może wymagać podania w konfiguracji urządzenia numeru lub zakresu portów na których dokonywana jest identyfikacja aplikacji.

1.2.2.2. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach.

1.2.2.3. Wydajność kontroli firewall i kontroli aplikacji musi być taka sama i wynosić w ruchu full-duplex nie mniej niż 1 Gbit/s.

1.2.2.4. NGN-FW musi posiadać możliwość pracy w formie routera, transparentego firewall (L2) oraz TAP.

1.2.2.5. System musi mieć możliwość kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników.

1.2.2.6. System musi mieć możliwość kształtowania ruchu sieciowego (QoS) per sesja na podstawie znaczników DSCP.

1.2.2.7. Musi istnieć możliwość przydzielania takiej samej klasy QoS dla ruchu wychodzącego i przychodzącego.

1.2.2.8. System musi mieć możliwość poddania  ruchu właściwej inspekcji, nie mniej niż:

1.2.2.8.1. wykrywanie i kontrola aplikacji,

1.2.2.8.2. wykrywanie i blokowanie ataków typu exploit (ochrona Intrusion Prevention),

1.2.2.8.3. wirusy i inny złośliwy kod (ochrona anty-wirus i any-spyware),

1.2.2.8.4. filtracja plików, danych i URL.

1.2.2.9. Firewall musi pozwalać na analizę i blokowanie plików przesyłanych w zidentyfikowanych aplikacjach.

1.2.2.10. W przypadku gdy kilka aplikacji pracuje na tym samym porcie UDP/TCP (np. tcp/80) musi istnieć możliwość przydzielania innych, osobnych profili analizujących i blokujących dla każdej aplikacji.

2. Serwery fizyczne tworzące chmurę obliczeniową mogą być współdzielone przez innych klientów.

2.1. CPU musi być w architekturze amd64 wspierając 64-bitowe systemy operacyjne

2.1.1. oraz musi wspierać sprzętową akcelerację dla szyfrowania AES.

2.2. Zasoby dyskowe maszyn VM muszą być udostępniane z macierzy dyskowych.

2.2.1. Każde CPD (główne i DRC) muszą posiadać autonomiczne macierze dyskowe.

2.2.2. Macierz musi posiadać połączenie do serwerów fizycznych poprzez redundantną sieć SAN lub bezpośrednie o wydajności minimum 8Gbps w technologii FC lub TenGigabitEthernet.

2.2.3. Pamięć masowa na macierzach (tzw. Datastore) wykorzystywana przez maszyny wirtualne VM Zamawiającego musi być replikowana do ośrodka ZCPD w sposób ciągły (on-line).

2.2.4. Zasoby vCPU oraz vMEM muszą posiadać tzw. rezerwację zasobów. Nie jest dopuszczalne sytuacja, gdzie maszyna fizyczna posiada mniej pamięci RAM niż jest przypisanych do maszyn wirtualnych.

2.2.5. Ponadto klaster HyperVisorów musi posiadać odpowiednie zasoby gwarantujące redundancję w przypadku awarii pojedynczych serwerów fizycznych.

2.2.6. Oprogramowanie wirtualizacyjne (Hypervisor) musi być skonfigurowany w funkcji wysokiej dostępności

2.2.6.1. oraz wspierać możliwość migracji maszyn VM pomiędzy fizycznymi serwerami a także PCPD a ZCPD automatycznie lub za sprawą ręcznej interwencji administratora.

2.2.6.2. Ponadto Hypervisor musi wspierać funkcję Fault-Tolerance (FT) dla wybranych maszyn VM – to znaczy taka maszyna VM musi działać jednocześnie w obrębie dwóch fizycznych serwerów z pełną synchronizacją pamięci vRAM oraz zasobów dyskowych vHDD, gdzie awaria pojedynczego fizycznego serwera czy macierzy dyskowej nie powoduje awarii VM z funkcją FT.

2.2.7. W przypadku poważnej awarii (lub wyłączenia) PCPD ZCPD  powinno automatycznie i w sposób możliwie bezprzerwowy przejąć funkcję PCPD

2.2.8. Świadczona Usługa musi zapewniać centralną konsolę umożliwiającą zarządzanie dostępnymi zasobami.

2.2.9. W ramach rozwiązania istniała będzie możliwość dodawania pamięci RAM, vCPU oraz vHDD do maszyn wirtualnych bez przerywania ich pracy “na gorąco”.

2.2.10. Platforma musi umożliwiać konfigurację dynamicznego (automatycznego) dodawania pamięci vRAM jeśli na danej VM ilość wolnej pamięci osiągnie skonfigurowaną ilość.

2.2.11. Konfiguracja tego parametru musi odbywać się per VM.

2.3. Oprogramowanie wirtualizacje (HyperVisor) musi wspierać systemy operacyjne:

2.3.1. Ubuntu  16.04LTS, 17,18 i późniejsze

2.3.2. Debian  7,8,9 i późniejsze

3. Zamawiający oczekuje świadczenia usług doradczych, konfiguracyjnych

i administracyjnych dla potrzeb niniejszego środowiska oraz własnych maszyn wirtualnych.

3.1. Usługi doradcze to m.in.

3.1.1. dostarczenie niezbędnej wiedzy zamawiającemu przed uruchomieniem rozwiązania

3.1.1.1. Przekazanie dokumentacji, najlepszych praktyk

3.1.1.2. opiniowanie projektu, ewentualnie przedstawienie własnego

3.1.2. pełne wsparcie przy tworzeniu maszyn wirtualnych,  zgodnie z wymaganiem Zamawiającego.

3.1.3. planowanie/konfiguracja NGN-FW.

3.1.4. troubleshooting problemów.

3.1.5. Forma kontaktu powinna być najbardziej dogodna zarówno dla zamawiajacego jak i wykonawcy, oraz gwaratnować efektywne przekazanie wiedzy

3.2. Usługi konfiguracyjne to m.in:

3.2.1. Przygotowanie środowiska i stworzenie kont dla zamawiającego

3.2.2. wstępna konfiguracja NGN-FW

3.2.3. Usługodawca zapewni stały, szyfrowany kanał VPN typu Site-to-Site IPSEC do Zamawiającego w celach administracji oraz monitoringu maszyn wirtualnych.

3.2.4. Usługodawca zapewni dostęp do logów serwera oraz logów z błędami.

3.2.5. Usługodawca zapewni dostęp do konsoli zarządzania dla każdej maszyny wirtualnej.

3.3. Usługi administracyjne to m.in:

3.3.1. Przegląd logów systemu pod kątem nieprawidłowości.

3.3.2. Reagowanie na zdarzenia wstępujące na serwerach (np. nieprawidłowości, alarmy).

3.3.2.1. monitoring przez dyżurującego Administratora 24h/dobę.

3.3.3. Usługodawca zobowiązuje się do niezwłocznego likwidowania awarii powstałych po swojej stronie.

3.3.3.1. Czas reakcji na zgłoszenie wynosi 120 minut i oznacza maksymalny okres czasu, który może upłynąć:

3.3.3.1.1. od momentu zauważenia przez dyżurującego administratora lub otrzymania zgłoszenia awarii od Zamawiającego do całkowitego usunięcia awarii.

3.3.4. Usługodawca poinformuje  Zamawiającego o terminach planowanych przerw technicznych w świadczeniu usługi hostingowej z co najmniej 24 godzinnym wyprzedzeniem.

3.3.4.1. Usługodawca zagwarantuje, że wszystkie przerwy techniczne będą miały miejsce w godzinach nocnych: pomiędzy godziną 23.00 a godziną 6.00 rano i nie będą jednorazowo dłuższe niż 6 godzin.

4. Usługodawca zapewni bezwarunkowe bezpieczeństwo danych Zamawiającego przechowywanych na serwerach Usługodawcy.

4.1. Co 24 godz. jest automatycznie wykonywana pełna kopia zapasowa (ang. backup) danych z wszystkich serwerów (dyski wirtualne) i baz danych SQL w sposób nieutrudniający korzystania z serwisu internetowego.

4.1.1. Prawidłowy przebieg procesu jest monitorowany przez Administratora Usługodawcy.

4.1.2. Usługodawca zapewni Zamawiającemu bezpośredni dostęp do kopii bezpieczeństwa z ostatnich 7 dni oraz do kopii bezpieczeństwa z końca każdego tygodnia w okresie poprzednich 30 dni.

4.1.3. Dodatkowo należy zapewnić drugą kopię zapasową utrzymaną w ZCPD – kopia ta musi być wykonywana niezależnie od głównej kopii zapasowej (nie może być dokonywana za pomocą replikacji).

4.1.4. Kopie zapasowe muszą być trzymane poza macierzami dyskowymi, gdzie znajdują się dyski wirtualne maszyn VM.

4.2. Usługodawca jest zobowiązany do niezwłocznego informowania Zamawiającego o wszelkich stwierdzonych incydentach bezpieczeństwa, w szczególności o przypadkach nieautoryzowanego dostępu do  danych za pośrednictwem infrastruktury zapewnianej przez Usługodawcę, atakach typu DoS, DDos itp. a także wszystkich wykrytych problemach i incydentach mogących mieć wpływ na działanie usługi.

4.3. Usługodawca jest zobowiązany do rejestrowania  każdego wykorzystania uprawnień administracyjnych na infrastrukturze objętej umową.

5. Usługodawca zagwarantuje :

5.1. nadzór i monitoring w systemie 24 godziny / 7 dni w tygodniu / 365 dni w roku,

5.2. dostęp telefoniczny i za pomocą poczty elektronicznej do Biura Obsługi Klienta,

5.3. w przypadku awarii dostęp telefoniczny i za pomocą poczty elektronicznej do dyżurnego administratora - 24h/dobę.

5.3.1. dyżurny administrator powinien być dostępny i udzielić aktualnych informacji niezależnie od skali awarii i zaabsorbowania w jej naprawę

5.3.1.1. Zakres minimalnej informacji - to aktualna diagnoza, oraz prognoza co do przywrócenia usług.

5.4. możliwość zgłaszania awarii i nieprawidłowości w działaniu usług telefonicznie oraz pocztą elektroniczną w systemie 24 godziny /7 dnia w tygodniu/365 dni w roku kalendarzowym.

5.5. Możliwość konsultacji z administratorem dyżurnym 24h/dobę oraz z administratorami II linii w ich ramowych godzinach pracy, z wyjątkiem zaangażowania ich w usuwanie awarii

5.5.1. W momencie awarii i jej usuwania - konsultacje są możliwe o ile są niezbędne do ponownego uruchomienia usługi.

5.5.2. W przypadku urlopu któregoś z administratorów II linii wykonawca informuje kiedy pracownik będzie ponownie dostępny oraz zapewnia kontkat z osobą zastępującą danego administratora

5.6. Usługodawca zagwarantuje dostępność usługi na poziomie nie mniejszym niż 99,9% czasu w roku kalendarzowym.

5.6.1. Dopuszczalny czas niedostępności 24h  w roku kalendarzowym.

6. W celu realizacji przedmiotu Umowy  zapewni w gwarantowanej, **podstawowej części zamówienia**, następujące zasoby infrastruktury dostępne dla Zamawiającego:

6.1. vCPU (ilość rdzeni fizycznych do dyspozycji bez HT)– nie mniej niż 8 sztuk (z możliwością rozszerzenia)

6.2. Częstotliwość taktowania vCPU/fizycznego rdzenia CPU – nie mniej niż 2.0 GHz

6.3. vRAM – 8GB (z możliwością rozszerzenia)

6.4. Przestrzeń dyskowa – 0,4 TB (400 GB) z możliwością rozszerzenia

6.5. Przestrzeń na backup – 0,8 TB (800 GB) z możliwością rozszerzenia

6.6. Łącze symetryczne do każdej wirtualnej maszyny o przepustowości – min. 1Gbit/s

6.7. Ilości maszyn wirtualnych – nie mniej niż 4

6.8. Ilość stałych publicznych adresów IP v4 – 4 sztuk z możliwością rozszerzenia

6.9. 2xFirewall NGFW

6.10. Opłaty związane ze świadczeniem usługi będą naliczane od momentu uruchomienia maszyn wirtualnych

1. W ramach rozszerzenia realizacji przedmiotu Umowy zapewni następujące zasoby infrastruktury dostępne dla Zamawiającego:

7.1. Opłaty związane ze świadczeniem usługi będą obliczane i naliczane na podstawie rzeczywistego wykorzystania zasobów dostępnych dla Zamawiającego z dokładnością do jednej godziny wykorzystania zasobów. Stawka godziny będzie obliczana jako 1/720 stawki miesięczne podanej w Załączniku nr A do formularza ofertowego.

7.2. Zamawiający zastrzega, że nie wszystkie zdeklarowane, rozszerzone zasoby będą wykorzystane od początku umowy, w szczególności żadne zasoby rozszerzone mogą nie być wykorzystywane.

7.3. W przypadku braku wykorzystania zasobów rozszerzonych Usługodawca nie obciąży Zamawiający jakąkolwiek opłatą.

7.3. Czas trwania usług rozszerzonych – periodycznie w okresie realizacji umowy.

8. Zamawiający Wymaga aby Usługodawca wykazał się odpowiednią wiedzą – musi posiadać zespół techniczny do realizacji wymaganych usług konfiguracyjnych i administracyjnych dla urządzeń wykorzystywanych do świadczenia usługi, w tym minimum:

8.1. I linia wsparcia:

8.1.1. Administrator dyżurny - zespół osób 24h/dobę

8.1.2. Wykonawca zapewnia kontakt 24h/na dobę do wymienionej osoby

8.2. II llinia wsparcia:

8.2.1. Administrator systemów operacyjnych (znajomość Linux + ewentualnie systemu operacyjnego hosta) - 1 osoba

8.2.2. Administrator rozwiązań wirtualizacyjnych  – 1 osoba

8.2.3. Administrator rozwiązań HA  – 1 osoba

8.2.4. Administrator rozwiązań NGN-FW – 1 osoba

8.2.5. Administrator rozwiązań sieci SAN – 1 osoba

8.2.6  Jedna osoba może pełnić więcej niż 1 funkcję

8.4. Wszystkie osoby muszą biegle porozumiewać się językiem polskim – w mowie i piśmie.

8.5. Wykonawca poda numery kontaktowe do wymienionych osób

8.6. Zamawiający poda listę osób uprawnionych do kontaktu z I i II linii wsparcia

8.6.1. Osoby spoza listy uprawnione są wyłącznie do kontaktu z Biurem Obsługi Klienta