Załącznik nr 1

Opis Przedmiotu Zamówienia Oraz Warunków Realizacji Usługi

I. Wstęp

Przedmiotem zamówienia jest świadczenie usługi ochrony i przyśpieszania aplikacji (CDN – Content Delivery Network) spełniających poniższe wymagania ogólne:

- Dostarczenie i przyspieszenie aplikacji za pośrednictwem rozproszonej platformy serwerów CDN;
- Rozłożenie ruchu pomiędzy różne data center na poziomie chmury;
- Ochrona aplikacji przy użyciu Web Application Firewall;
- Pełnego wsparcia w zakresie wdrożenia powyższych produktów i obsługi powdrożeniowej (wsparcie 24h/7 dni w tygodniu);
- Bieżąca ekspertyza dotycząca działających rozwiązań.

II. Szczegółowe wymagania techniczne

II.1 Platforma CDN

Ochrona i przyspieszenie aplikacji muszą polegać na użyciu rozwiązania klasy CDN posiadającego serwery na terenie Unii Europejskiej.

Dostępność oferowanej platformy CDN musi być na poziomie100%.

Wykonawca składając ofertę deklaruje, że oferowana platforma CDN nie miała żadnych przerw w dostępności w okresie 12 miesięcy licząc od dnia publikacji zamówienia.

Oferowana platforma CDN musi mieć możliwość limitowania obsługi aplikacji jedynie do serwerów CDN znajdujących się na terenie Unii Europejskiej.

Oferowana platforma CDN musi posiadać protokół umożliwiający dostarczenie contentu alternatywną ścieżką w stosunku do tej proponowanej przez zewnętrzny protokół routingu (BGP), co ma przełożyć się na dodatkowe przyspieszanie działania aplikacji.

Oferowana platforma CDN musi być gotowa do rozbudowy w przyszłości pod kątem rozwiązań umożliwiających:

- Zastosowanie zaawansowanego firewalla aplikacyjnego (z możliwością ustawienia oddzielnych konfiguracji dla poszczególnych hostów, manualnego doboru reguł i dostępu do security operations center);

- Zastosowanie rozwiązania typu Real User Monitoring – monitoring zachowań użytkowników w czasie rzeczywistym;
- Zastosowanie rozwiązania umożliwiającego optymalizację grafiki na poziomie chmury;
- Zastosowanie rozwiązania umożliwiającego optymalizację stron pod kątem różnego typu urządzeń, jakości sieci czy zarządzania skryptami stron trzecich;
- Zastosowanie rozwiązania typu Customer Identity Access Management (CIAM), tj. zarządzania tożsamością i kontami użytkowników, w tym ich zabezpieczenia.

II.2 Firewall Aplikacyjny (Web Application Firewall, WAF)

Ochrona aplikacji przeciwko atakom DDoS, a także atakom na warstwę aplikacyjną typu SQL Injection, UDP Flood, XSS i innym wymienianym w OWASP TOP10.

W pełni konfigurowalna ochrona przed atakami na warstwę 3 i 4. Ochrona przed atakami na warstwę 7 wraz z automatyczną aktualizacją dla najnowszych reguł i wektorów ataków. Poziom 100% SLA dla dostępności platformy odpowiedzialnej za dostarczanie i ochronę aplikacji webowej klienta. Rozwiązanie ma być automatyczne i po poprawnym skonfigurowaniu nie wymagać dodatkowej obsługi ze strony użytkownika.

II.3 Monitoring

Platforma ma udostępniać funkcjonalność monitorowania ruchu użytkowników oraz warstwy bezpieczeństwa pod kątem:

- Ruchu webowego na aplikacji Zamawiającego (w podziale na wywołania brzegowe, wolumen – GB, URL, odpowiedzi ze źródła, pochodzenie użytkowników i typy systemów operacyjnych, przeglądarek, pochodzenia geograficznego);
- Poziomu offload-u (redukcja obciążenia infrastruktury, ilość ruchu przejętego przez platformę względem tego który dotarł do źródła);
- Typów ataków w podziale na ich pochodzenie (IP, region), składnię (możliwość sprawdzenia jakie zapytanie zostało wykorzystane w trakcie ataku), typ ataku (m.in. SQL Injection, Local File Inclusion, Cross Site Scripting, Web Protocol Attack oraz inne);
- Sprawdzenia która warstwa ochrony została wykorzystana DDoS/Rate Controls/WAF/IP.

Zamawiający wymaga posiadania możliwości sprawdzenia powyższych danych w okresie do 90 dni wstecz.

II.4 Application Load Balancing

Funkcjonalność Load Balancing na poziomie chmury umożliwiająca ustawianie zaawansowanych reguł routingu oraz kontrolowanie zachowań w poszczególnych sesjach (w tym Cookie Based Session Stickiness).

II.5 Ochrona DNS

Dostępność 24 godziny przez 7 dni w tygodniu wraz z gwarancją 100% SLA na działanie platformy odpowiedzialnej za dostarczenie DNS.

II.6 Biała Lista

Oferowana platforma musi umożliwiać generowanie listy IP serwerów, które będą obsługiwały aplikację, w celu ich umieszczenia ich na „białej liście" na poziomie serwerów źródłowych po stronie klienta.

II.7 Wielkość ruchu

Zamawiający wymaga - gwarancjii obsługi ruchu na poziomie minimum 10 TB miesięcznie (estymowany próg ruchu) oraz minimalne pasmo przeznaczone do obsługi CDN to 10 Gb/s.

II.8 SLA na dostępność

SLA na dostępność platformy wyniesie 100%.

II.9 Obsługa ataków

W przypadku ataku na usługę świadczoną za pomocą platformy, obsługa tego ataku przez dostawcę nie będzie limitowana ani nie będzie generowała dodatkowych kosztów.

II.10 Wsparcie

Zamawiający wymaga dostępności wsparcia w języku polskim w zakresie 24 godziny przez 7 dni, z możliwością dokonywania zgłoszeń zarówno elektronicznie jak i telefonicznie. Maksymalny czas reakcji na zgłoszenie od Zamawiającego to 2 godziny.