Zapytania wraz z odpowiedziami oraz zmiana SIWZ

Dotyczy postępowania o udzielenie zamówienia publicznego w trybie przetargu nieograniczonego na **dostawę i wdrożenie systemu do inwentaryzacji sprzętu komputerowego w ramach projektu „Opracowanie i wdrożenie zintegrowanego systemu informatycznego dla jednostek oświatowych miasta Lublin"**

Prezydent Miasta Lublin informuje, iż w przedmiotowym postępowaniu wpłynęły następujące zapytania:

1) Zwracam się do Państwa z uprzejmą prośba o przesłanie plików SIWZ wraz ze wszystkimi załącznikami w wersji edytowalnej.

ODPOWIEDŹ:

Zamawiający informuje, iż udostępnił wszystkie niezbędne załączniki w formie edytowalnej.

2) W załączniku nr 1 do SIWZ – Szczegółowy opis przedmiotu zamówienia, art I ust. 5 pkt. b), Zamawiający wymaga:

„Zgłoszenia w ramach asysty technicznej dokonywane będą w systemie zgłoszeń Wykonawcy lub za pośrednictwem poczty e-mail z potwierdzeniem otrzymania zgłoszenia, z terminem realizacji do ..... dni roboczych dla błędów krytycznych oraz z terminem realizacji 5 dni roboczych dla usterek ..."

a) Zwracam się prośbą do Zamawiającego o wskazanie terminu realizacji zgłoszenia dla błędów krytycznych.

ODPOWIEDŹ:

Zamawiający informuje, iż termin realizacji zgłoszenia dla błędów krytycznych jest kryterium oceny ofert określonym w pkt. 13.2. SIWZ. Zgodnie z pkt. 13.2.1. SIWZ z maksymalny czas realizacji dla błędów krytycznych wynosi 5 dni roboczych.

b) Czy Zamawiający dopuści możliwość wydłużenia terminu realizacji dla usterek do 10 dni roboczych?

ODPOWIEDŹ:

Zamawiający działając zgodnie z art. 38 ust. 4 ustawy z dn. 29 stycznia 2004 r. Prawo zamówień publicznych (tj. Dz. U. Z 2017 poz. 1579 z późn. zm.) zmienia treść Specyfikacji Istotnych Warunków Zamówienia.

Załącznik nr 1 do SIWZ – Szczegółowy opis przedmiotu zamówienia, art I ust. 5 pkt. b) otrzymuje brzmienie:

„b)wszelkie zmiany w systemie skutkujące niedostępnością lub wpływające na jego stabilność lub wydajność wymagają uprzedniej zgody Zamawiającego.

Zgłoszenia w ramach asysty technicznej dokonywane będą w systemie zgłoszeń Wykonawcy lub za pośrednictwem poczty e-mail z potwierdzeniem otrzymania zgłoszenia, z terminem realizacji do ..... dni roboczych dla błędów krytycznych oraz z terminem realizacji 10 dni roboczych dla usterek, gdzie błąd krytyczny to sytuacja polegająca na nieprawidłowym, funkcjonowaniu systemu, w tym niezgodnie z dokumentacją, skutkująca:
- niedostępnością systemu,
- niespójnością danych
- zawieszaniem się systemu,
- niedostępnością funkcjonalności określonych w dokumentacji;
a usterka to sytuacja inna niż błąd krytyczny, polegająca na nieprawidłowym funkcjonowaniu systemu, nieograniczająca zakresu funkcjonalnego, lecz utrudniająca pracę użytkownikom lub administratorom."

c) Czy Zamawiający dopuści możliwość wstrzymania biegu terminu realizacji w przypadku, gdy usunięcie błędu krytycznego bądź usterki będzie wymagało wypuszczenia łatki/patcha oprogramowania przez jej producenta?

ODPOWIEDŹ:
Zamawiający nie przewiduje możliwości wstrzymania biegu terminu realizacji usunięcia błędu krytycznego ze względu na jego potencjalna wagę dla bezpieczeństwa systemu, a także bezpieczeństwa danych przechowywanych na stacjach roboczych, w szczególności w świetle obowiązujących przepisów odnoszących się do RODO.

3) W załączniku nr 1 do SIWZ – Szczegółowy opis przedmiotu zamówienia, art I ust. 5 pkt. b), jako usterkę Zamawiający wskazuje:

Sytuacja inna niż błąd krytyczny, polegająca na nieprawidłowym funkcjonowaniu systemu, nieograniczająca zakresu funkcjonalnego, lecz utrudniająca pracę użytkownikom lub administratorom.

d) Czy Zamawiający zgodni się na rozszerzenie definicji usterki objętej SLA, jako:

Sytuację inną niż błąd krytyczny, polegającą na nieprawidłowym funkcjonowaniu systemu, nieograniczającą zakresu funkcjonalnego, lecz utrudniającą pracę co najmniej 20% użytkowników lub administratorów?

ODPOWIEDŹ:

Zamawiający nie przychyla się do propozycji zmiany definicji usterki. Wprowadzenie zmian spowodowałoby powstanie luki w definicjach, a co za tym idzie sytuacji w której system nie działałby prawidłowo, a występujących błędów w jego działaniu nie można byłoby zaklasyfikować do żadnej kategorii które obligowałyby Wykonawcę do ich usunięcia w jakimkolwiek z określonych terminów.

4) W załączniku nr 1 do SIWZ – Szczegółowy opis przedmiotu zamówienia, art. I ust. 4 pkt. 4 ppkt. j), Zamawiający wymaga:

przeprowadzenie testów penetracyjnych obejmujących skanowanie portów, badanie podatności systemu operacyjnego oraz aplikacji na znane luki w bezpieczeństwie, weryfikację poprawności działania firewalla, ocenę poprawności reakcji systemu zabezpieczeń na wykonywane ataki DDOS, w tym co najmniej:
- flooding,
- smurfing,
- IP fragmentation,
- syn flood,
- nuking.

e) Czy Zamawiający oczekuje przeprowadzenia badania podatności systemu operacyjnego oraz aplikacji na znane luki w bezpieczeństwie, jedynie w zakresie maszyny wirtualnej z zainstalowaną aplikacją, konfigurowanej przez oferenta?

ODPOWIEDŹ:

Zamawiający informuje, iż zgodnie z załącznikiem nr 1 do SIWZ – Szczegółowy opis przedmiotu zamówienia, art. I ust. 4 pkt. 4 w szczególności ppkt. J, oczekuje przeprowadzenia testów penetracyjnych dla całości rozwiązania strony serwerowej narażonej na bezpośrednie zagrożenia z Internetu, bez ograniczania się do pojedynczej maszyny wirtualnej. W przypadku, gdy wdrożenie wymagać będzie infrastruktury rozbudowanej np. o dodatkowe serwery proxy, czy autoryzacyjne dostępne z Internetu, również one muszą podlegać wspomnianym testom.

f) Czy Zamawiający oczekuje testów penetracyjnych w modelu black box aplikacji?

ODPOWIEDŹ:

Zamawiający oczekuje przeprowadzenia przez Wykonawcę testów zgodnie z z załącznikiem nr 1 do SIWZ – Szczegółowy opis przedmiotu zamówienia, art. I ust. 4 pkt. 4 w ppkt. J bez wymagań co do modelu przeprowadzanych testów.

g) Czy przez skanowanie portów, Zamawiający rozumie skanowanie adresacji maszyny wirtualnej której dotyczą prace wdrożeniowe?

ODPOWIEDŹ:

Zamawiający informuje, iż zgodnie z załącznikiem nr 1 do SIWZ – Szczegółowy opis przedmiotu zamówienia, art. I ust. 4 pkt. 4 w szczególności ppkt. J, oczekuje przeprowadzenia testów penetracyjnych dla całości rozwiązania strony serwerowej narażonej na bezpośrednie zagrożenia z Internetu, bez ograniczania się do pojedynczej maszyny wirtualnej. W przypadku, gdy wdrożenie wymagać będzie infrastruktury rozbudowanej np. o dodatkowe serwery proxy, czy autoryzacyjne dostępne z Internetu, również one muszą podlegać wspomnianym testom.

h) Co zamawiający rozumie przez atak DDoS typu „nuking"?

ODPOWIEDŹ:

Zamartwiający informuje, iż atak DDoS typu „nuking" polega na wysyłaniu pofragmentowanych lub uszkodzonych pakietów, najczęściej protokołem ICMP, czego efektem jest awaria atakowanego systemu, spowolnienie lub blokada połączeń od uprawnionych użytkowników.

i) Co zamawiający rozumie przez atak DdoS typu „IP fragmentation"

ODPOWIEDŹ:

Zamartwiający informuje, iż atak DdoS typu „IP fragmentation polega na wysyłaniu niepoprawnych pakietów większych od MTU zdefiniowanych dla sieci, których ze względu na błędy nie można ponownie złożyć, co przekłada się na obciążenie atakowanego systemu lub jego niedostępność.

Pozostałe zapisy SIWZ pozostają bez zmian.

W załączeniu ujednolicony zał. nr 1 do SIWZ - szczegółowy opis przedmiotu zamówienia

Z up. PREZYDENTA MIASTA LUBLIN
Elżbieta Daszyńska
DYREKTOR
Biura Zamówień Publicznych