Warszawa, dnia 20.09.2018 r.

L.dz. 4567../2018

Do wszystkich Wykonawców
przetargu nieograniczonego
P/12/AUDYT/2018

Dotyczy: postępowania o udzielenie zamówienia publicznego prowadzonego w trybie przetargu nieograniczonego na **Przeprowadzenie audytu bezpieczeństwa wraz z aktualizacją dokumentów organizacyjnych w ramach projektu „e-Zdrowie "INFLANCKA"** sprawa nr **P/12/AUDYT/2018**

WYJAŚNENIA TREŚCI SIWZ

Szanowni Państwo,

Informuję, iż do Zamawiającego wpłynęły zapytania dotyczące Specyfikacji Istotnych Warunków Zamówienia (dalej SIWZ) dotyczące przedmiotowego postępowania. Na podstawie art. 38 ust 2 ustawy z dnia 29 stycznia 2004 roku – Prawo zamówień publicznych (Dz. U. z 2017 r., poz. 1579 ze zm.), (dalej ustawy Pzp) Zamawiający przekazuje Wykonawcom treść pytań wraz z odpowiedziami. Odpowiedzi na pytania stanowią integralną część SIWZ i są wiążące dla Wykonawców przy opracowaniu ofert. Jednocześnie Zamawiający informuje, że na podstawie art. 38 ust. 4 dokonuje zmiany treści SIWZ poprzez zmianę terminu składania ofert: do dnia **25.09.2018 godz. 10.00** oraz zmianę terminu otwarcia ofert: dnia **25.09.2018 godz.11.00**.

Pytanie nr 1
Pytania dotyczące testów penetracyjnych Aplikacji Webowej / API.
Jaka jest liczba ról w aplikacji np. użytkownik, moderator, administrator
Odp. Występuje niewielka liczba ról: Użytkownicy (Użytkownicy z podziałem na personel lekarz, pielegniarka, technik radiolog, rejestratorka), pacjent, administratorzy danych modułów.

Pytanie nr 2
Jaka jest liczba funkcjonalności. Proszę o krótki opis funkcjonalności / endpointów API np. wysłanie wniosku, wgrywanie zewnętrznych plików, wyszukiwanie danych, edycja danych / 50 endpointów
Odp. Opis funkcjonalności dostępny jest na stronie http://ipzp.pl/display/index.php?id=021B2B26B932CD2 są to funkcjonalności związane z obszarem e-usług oraz wdrożeniem i integracją systemu RIS/PACS. Zamawiający podtrzymuje zapisy SIWZ.

Pytanie nr 3
Czy aplikacja jest dostępna publicznie z możliwością zarejestrowania się/zalogowania (wersja demo) - jeśli tak, prośba o dostarczenie adresu URL i dostępów? <adres URL>

Odp. Nie , nie jest dostępna wersja demo. Zamawiający podtrzymuje zapisy SIWZ.

Pytanie nr 4
Czy konta użytkowników w aplikacji zostaną dostarczone testerom? np. Tak/Nie(testy blackbox)/Samodzielna rejestracja
Odp. Zamawiający dopuszcza różne rozwiązania w tym zakresie. Zamawiający podtrzymuje zapisy SIWZ.

Pytanie nr 5
Czy testerzy otrzymają dokumentacje do aplikacji / API? np. Tak/Nie(testy blackbox, graybox)
Odp. Nie, testerzy nie otrzymają dokumentacji do aplikacji API. Zamawiający podtrzymuje zapisy SIWZ.

Pytanie nr 6
Czy należy wykluczyć pewne typy testów? np. Denial of Service, exploitacja podatności
Odp. Tak, Zamawiający nie przewiduję przeprowadzenia testów typu Denial of Service. Zamawiający podtrzymuje zapisy SIWZ.

Pytanie nr 7
Czy testy mogą zostać przeprowadzone zdalnie? np. Tak/Nie/przez VPN
Odp. Zamawiający dopuszcza różne rozwiązania w tym zakresie. Zamawiający podtrzymuje zapisy SIWZ.

Pytanie nr 8
Czy testy mają być przeprowadzone w określonych oknach czasowych? np. w godzinach pracy, poza godzinami pracy, strefa czasowa, w weekendy/bez weekendów
Odp. Godziny przeprowadzenia testów zostaną ustalone po podpisaniu umowy. Zamawiający podtrzymuje zapisy SIWZ.

Pytanie nr 9
Czy infrastruktura jest chroniona przez systemy WAF/IDS/IPS/Cloudflare? Tak/Nie jesli tak, to jakie
Odp. Informacje tego rodzaju zostanie przekazana wybranemu wykonawcy po podpisaniu umowy. Zamawiający podtrzymuje zapisy SIWZ.

Pytanie nr 10
Czy systemy WAF/IDS/IPS/Cloudflare będą aktywne w trakcie testów? Tak/Nie/IP testerów można dodać do whitelisty
Odp. Patrz odpowiedź na pytanie 9.

Pytanie nr 11
W jakiej technologii została stworzona aplikacja? np. PHP/Python/Java/JavaScript
Odp.: JAVA SCRIPT, FLASH, HTML5, CLARION. Zamawiający podtrzymuje zapisy SIWZ.

Pytanie nr 12
Jakiego typu jest testowane środowisko? np. produkcja, pre-prod, testowe
Odp. Testowane będzie środowisko testowe i/lub produkcyjne w ustalonym zakresie. Zamawiający podtrzymuje zapisy SIWZ.

Pytanie nr 13
Bardzo proszę o udzielenie odpowiedzi na poniższe pytania dotyczące testów penetracyjnych Infrastruktury. Jaka jest liczba adresów IP/hostów lub zakres/podsieć do przetestowania np. 20 lub 192.168.0.0/24
Odp. Patrz odpowiedź na pytanie 9.

Pytanie nr 14
Jaki jest typ sieci np. zewnętrzna/lokalna/bezprzewodowa
Odp. Występują różne rodzaje sieci. Zamawiający podtrzymuje zapisy SIWZ.

Pytanie nr 15
Proszę o ogólny opis przeznaczenia hostów w sieci (w przypadku testów greybox)
np. 192.168.0.1 - serwer WWW
192.168.0.100 - firewall
192.168.0.5 - serwer FTP
192.168.0.6-50 – desktopy
Odp.: Występują serwery aplikacyjne 5 (JBOSS, PACS, MPI, RIS, EDM), serwery bazodanowe 3 (DB2 RIS/PACS, ORACLE MPI, ORACLE HIS), serwer pośredniczący 1, serwer webowy 1. Szczegółowe dane będą udostępnione po podpisaniu umowy. Zamawiający podtrzymuje zapisy SIWZ.

Pytanie nr 16
Czy należy wykluczyć pewne typy testów np. Denial of Service, exploitacja podatności
Odp. Patrz odpowiedź na pytanie 6.

Pytanie nr 17
Czy testy mogą zostać przeprowadzone zdalnie? np. Tak/Nie/przez VPN
Odp. Patrz odpowiedź na pytanie 7.

Pytanie nr 18
Czy testy mają być przeprowadzone w określonych oknach czasowych? np. w godzinach pracy, poza godzinami pracy, strefa czasowa, w weekendy/bez weekendów
Odp. Patrz odpowiedź na pytanie 8.

Pytanie nr 19
Czy infrastruktura jest chroniona przez systemy IDS/IPS? Tak/Nie
Odp. Patrz odpowiedź na pytanie 9.

Pytanie nr 20
Czy systemy IDS/IPS będą aktywne w trakcie testów? Tak/Nie/IP testerów można dodać do whitelisty
Odp. Patrz odpowiedź na pytanie 9.

Pytanie nr 21
Jakiego typu jest testowane środowisko? np. produkcja, pre-prod, testowe
Odp.: Patrz odpowiedź na pytanie 12.

Pytanie nr 22
Prosimy o odpowiedź na poniższe pytania dla każdej aplikacji webowej, która ma być objęta testami.
Nazwa aplikacji, producent, wersja.
Odp.: AMMS WMS RIS WMS PACS; ASSECO GABOS: zawsze aktualizowana do najnowszej. Zamawiający podtrzymuje zapisy SIWZ.

Pytanie nr 23
Krótki opis do czego służy aplikacja oraz kluczowe funkcje (lista główny funkcji).
Odp.: Patrz odpowiedź na pytanie 2.

Pytanie nr 24
Lista metod logowania i uwierzytelniania: (np. ID, hasło, certyfikat, token, kod sms).
Odp. Patrz odpowiedź na pytanie 9.

Pytanie nr 25
Lista metod autoryzacji operacji: (np. certyfikat, token, kod sms, urządzenia HSM (Hardware Security Module)).
Odp. Patrz odpowiedź na pytanie 9.

Pytanie nr 26
Liczba ról, które mają podlegać testom (np. gość, użytkownik zwykły, użytkownik rozszerzony, operator, administrator, itp.).
Odp.: Patrz odpowiedź na pytanie 1

Pytanie nr 27
Lista / Liczba stron / formularzy dynamicznie generowanych.
Odp. Patrz odpowiedź na pytanie 9.

Pytanie nr 28
Liczba pól we wszystkich formularzach.
Odp. Patrz odpowiedź na pytanie 9.

Pytanie nr 29
Jakie są zewnętrzne i wewnętrzne interfejsy poszczególnych aplikacji (np. interfejs webowy, webserwisy, bramki email lub SMS, współdzielone bazy danych lub pliki wsadowe)?
Odp. Interfejs webowy, aplikacja na stacjach końcowych, serwery bazy danych, serwery aplikacyjne, bramki SMS, serwery e-mail, interfejs HL7. Zamawiający podtrzymuje zapisy SIWZ.

Pytanie nr 30
Jaka jest przybliżona liczba bibliotek zewnętrznych (open source lub komercyjnych) używanych przez poszczególne aplikacje?
Odp. Patrz odpowiedź na pytanie 9.

Pytanie nr 31
Jakie są najbardziej wrażliwe typy danych przetwarzanych przez aplikację (np. numery kart płatniczych, dane osobowe, informacje zdrowotne)?
Odp.: Dane osobowe historie choroby. Zamawiający podtrzymuje zapisy SIWZ.

Pytanie nr 32
Użyte technologie po stronie klienta i serwera.
Odp.: ORACLE, DB2, GLASFISH, JBOSS, LINUX DOCKER, TOMCAT, APACHE. Zamawiający podtrzymuje zapisy SIWZ.

Pytanie nr 33
Szacunkowa całkowita liczba argumentów przekazywanych od użytkownika.
Odp. Patrz odpowiedź na pytanie 9.

Pytanie nr 34
Czy aplikacje internetowe będą dostępne za WAF'em? Jeżeli tak to czy istnieje możliwość jego wyłączenia na czas testów?
Odp. Patrz odpowiedź na pytanie 9.

Pytanie nr 35
Czy zakres prac ma obejmować testy infrastruktury na jakiej działa aplikacja? Jeżeli tak to prosimy o informację o:
a) IP adresy, które będą podlegały audytowi (lista IP adresów, klasa IP adresów lub liczba IP adresów).
Odp. Patrz odpowiedź na pytanie 9

b) Liczba serwerów, które mają być objęte testami:
a. aplikacyjne
b. webowe / html
c. bazodanowe
d. proxy
e. inne – jakie
Odp. Patrz odpowiedź na pytanie 15

Pytanie nr 36
Testy infrastruktury:
a) Liczba serwerów, model i producent, które mają podlegać testom
b) Liczba urządzeń aktywnych (routery, switche), model i producent, które mają podlegać testom
c) Liczba baz danych, które mają podlegać testom
d) Liczba komputerów, które mają podlegać testom
e) Liczba innych urządzeń (np. drukarki, skanery), które mają podlegać testom
f) Liczba VLAN.
Odp. Patrz odpowiedź na pytanie 9.

Pytanie 37 - Czy zdaniem Zamawiającego możliwość wprowadzenia kontroli logowania do konta użytkownika (np. blokowanie logowania na konta prywatne) oraz ograniczenia dostępu do konta użytkownika tylko dla wskazanego urządzenia (lub urządzeń) nie powinno być wymagane dla oprogramowania ? Brak takiej możliwości może skutkować wyciekiem danych pacjentów.

Odp. Zamawiający zmienia* w *Załącznik nr 1 do SIWZ - Opis przedmiotu zamówienia.pdf rozdział 3 punkt 3 - Analiza architektury poprzez wprowadzenie

wymagań w podpunkcie n:

liii Możliwość wprowadzenia kontroli możliwości logowania do konta użytkownika (np. blokowanie logowania na konta prywatne) oraz ograniczenia dostępu do konta użytkownika tylko dla wskazanych urządzeń.

Pytanie 38 - Czy Zamawiający uważa za dostateczne zabezpieczenie transmisji danych za pomocą standardowych protokołów tj. SSL/TLS w proponowanej architekturze? Pragniemy stwierdzić, że w ramach zaleceń CSIOZ takie zabezpieczenie zostało uznane za niebezpieczne, a wykorzystywane przez Służbę Zdrowia rozwiązania powinny zapewniać ochronę danych w modelu end-to-end encryption oraz korzystać z mechanizmów uniemożliwiających skuteczne prowadzenie podsłuchu transmisji czy też ataki typu man in the middle.

Odp. Zamawiający wymaga zapewnienia ochrony danych w modelu end to end w podpunkcie o Załącznik nr 1 do SIWZ - Opis przedmiotu zamówienia.pdf rozdział 3 punkt 3. Jednocześnie Zamawiający zmienia Załącznik nr 1 do SIWZ - Opis przedmiotu zamówienia.pdf rozdział 3 punkt 3 - Analiza architektury poprzez wprowadzenie wymagań: podpunkt s: oprogramowanie ma korzystać z mechanizmów uniemożliwiających skuteczne prowadzenie podsłuchu transmisji czy też ataki typu man in the middle.

Pytanie 39 - Czy Zamawiający przewiduje dodanie do *Załącznika nr 2 do SIWZ_07 - Prezentacja_pdf.pdf* do elementów oceny punktacji *(rozdział 3 pkt 3.2 ppkt 4)* za spełnienie wymagań dotyczących architektury opisanej w *Załącznik nr 1 do SIWZ - Opis przedmiotu zamówienia.pdf* rozdział 3 punkt trzeci – Analiza architektury?

Odp. Nie, Zamawiający nie przewiduje zmiany elementów oceny.

Na podstawie art. 38 ust. 4 Zamawiający dokonuje zmiany treści SIWZ w Załączniku nr 1 do SIWZ strona 6 poprzez dodanie zapisu:

W ramach prezentacji – zgodnie z zapisami nr 2 do SIWZ w zakresie: Testów bezpieczeństwa należy przedstawić metodyką realizacji testów a w ramach czasowego użyczenie licencji na oprogramowanie służące do bezpiecznego przesyłania i współdzielenia plików wymagane jest przedstawienie opisu funkcjonalnego systemu jak i załączenia oprogramowania szyfrującego, potwierdzającego te wymagania.

Pytanie 40- Prosimy o dopisanie w dokumencie oferta :
„Ponadto oświadczamy, że:

1) Nasza oferta jest zgodna z wymaganiami opisanymi w załączniku nr 1 do SIWZ Opis Przedmiotu Zamówienia.

2) zapoznaliśmy się z warunkami zamówienia i nie wnosimy do nich żadnych zastrzeżeń oraz zdobyliśmy konieczne informacje potrzebne do właściwego wykonania zamówienia;

3) akceptujemy wzór umowy i zobowiązujemy się, w przypadku wybrania naszej oferty jako najkorzystniejszej, podpisać umowę na proponowanych warunkach i w terminie wyznaczonym przez Zamawiającego;

4) uważamy się związani niniejszą ofertą przez okres 30 dni od dnia upływu terminu składania ofert;

5) osobą/ami upoważnioną/ymi do podpisania umowy w przedmiotowym postępowaniu jest/są: „

Odp. Zamawiający wyraża zgodę na dopisanie do formularza oferty pkt 1 -"Nasza oferta jest zgodna z wymaganiami opisanymi w załączniku nr 1 do SIWZ Opis Przedmiotu Zamówienia"

Pozostałe zapisy pozostają bez zmian.

KIEROWNIK
Biura Administracyjno-Gospodarczego
Krzysztof Silny