CENTRUM USŁUG INFORMATYCZNYCH
W E W R O C Ł A W I U

Centrum Usług Informatycznych we Wrocławiu
ul. Namysłowska 8, 50-304 Wrocław

Wrocław, 03.09.2024

Dotyczy: postępowania o udzielenie zamówienia publicznego pn. **„Audyt bezpieczeństwa systemów informatycznych”** znak postępowania: CUI-ZZ.3200.24.2024

Zamawiający informuje, że do przedmiotowego postępowania wpłynęły wnioski o treści jak poniżej. Zamawiający, na podstawie art. 284 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (t.j. Dz. U. z 2023 r. poz. 1605 ze zm.) – dalej ustawa Pzp, przekazuje odpowiednio: odpowiedzi na wnioski o wyjaśnienie treści SWZ i/lub zmienia treść SWZ:

Pytanie nr 1:

jakie wymogi bezpieczeństwa ma Zamawiający na myśli w sformułowaniu: "Weryfikacja realizacji przez Wykonawcę systemu wymogów bezpieczeństwa"? Czy jest to powszechnie znany standard lub zestaw wymagań, czy jest to dokument wewnętrzny Zamawiającego - w tym drugim przypadku prosimy o podanie informacji, jak szeroki jest zbiór wymagań (ile jest wymagań do sprawdzenia)?

Odpowiedź:

Standard opisany jest w OPZ, pkt. III – Standardowe czynności związane z audytem bezpieczeństwa aplikacji.

Pytanie nr 2:

w "Ogólnych Zasadach" Zamawiający wskazuje, iż "Audytowi bezpieczeństwa podlegać będą wszystkie elementy składające się na całość rozwiązania Systemu tj. serwery aplikacyjne, bazy danych, moduły wewnętrzne aplikacji oraz aplikacje klienckie". Z kolei na str. 2 w ust. 5 pkt. III Zamawiający podaje: "Analizę konfiguracji (serwery, systemy operacyjne, bazy danych, usługi, porty)":

- Czy analizie konfiguracji podlegają również systemy operacyjne (niewymienione w punkcie "Ogólne zasady")? Jeżeli tak - proszę o podanie listy systemów

operacyjnych, mogących podlegać analizie lub, jeśli to nie jest możliwe, liczby różnych systemów operacyjnych.

- Czy pojęcie "serwery" z pkt. III ust. 5 oznacza "serwery aplikacyjne" i "bazy danych" z "Ogólnych zasad", czy oznacza również serwerowe systemy operacyjne?

Odpowiedź:

Hardening systemów operacyjnych wchodzących w skład systemów nie jest objęty audytem.

Pytanie nr 3:

Str. 3, pkt. III ust. 10 - proszę o wyjaśnienie wątpliwości dotyczących testów powtórnych:

1) Czy powtórne testy penetracyjne mają objąć jedynie scenariusze, które doprowadziły do wykrycia błędów w trakcie testów właściwych, czy należy powtórzyć wszystkie scenariusze testów właściwych?

2) Czy w ramach testów powtórnych należy uwzględnić ewentualne nowe scenariusze, wynikające np. ze zmian w stanie wiedzy, jakie zaszły pomiędzy testami właściwymi a testami powtórnymi?

3) Czy możliwe będą zmiany (w szczególności dodanie albo zmiana funkcjonalności) w przedmiocie poszczególnych testów (w poszczególnych aplikacjach) pomiędzy testami właściwymi a testami powtórnymi i czy zmieniona albo nowa funkcjonalność ma również podlegać testom w ramach re-audytu?

Odpowiedź:

1) Retesty obejmują tylko scenariusze, które doprowadziły do wykrycia błędów.

2) Nie.

3) Nie.

Pytanie nr 4:

Str. 3, pkt. III ust. 11 - czy przeprowadzenie prezentacji i omówienia metodyki Audytu wymagane jest w formie fizycznej w lokalizacji Zamawiającego, czy też Zamawiający dopuszcza formę wideokonferencyjną? (Pytanie dotyczy sytuacji, w której forma zdalna nie jest narzucana z zewnątrz np. w wyniku stanu epidemii czy zagrożenia epidemicznego).

Odpowiedź:

Może być zdalnie, Zamawiający nie wymaga fizycznej obecności.

Pytanie nr 5:

czy przeprowadzenie szkoleń w formie warsztatu dla Systemu 2 w ramach Zamówienia Podstawowego wymagane jest w formie fizycznej w lokalizacji Zamawiającego, czy też Zamawiający dopuszcza formę wideokonferencyjną? (Pytanie dotyczy sytuacji, w której forma zdalna nie jest narzucana z zewnątrz np. w wyniku stanu epidemii czy zagrożenia epidemicznego).

Odpowiedź:

Może być zdalnie, Zamawiający nie wymaga fizycznej obecności.

Pytanie nr 6:

Czy liczby baz danych, wymienione w opisach Systemów podlegających badaniu (tabele na str. 3-5), oznaczają różne bazy danych w ramach tego samego, pojedynczego serwera bazy danych, czy liczbę różnych serwerów bazy danych?

Odpowiedź:

Każda baza danych może, ale nie musi być na osobnym serwerze.

Pytanie nr 7:

Zamawiający wskazuje 5 różnych aplikacji Web (Zamówienie Podstawowe: System 1, System 2 oraz Prawo Opcji: Wariant nr 1, Wariant nr 2 i Wariant nr 3). Dla każdego z powyższych prosimy o podanie informacji umożliwiających rzetelne zwymiarowanie audytu bezpieczeństwa, podanych na liście poniżej. Jeśli dany system albo wariant obejmuje więcej niż jeden adres https:// - prosimy o podanie sumarycznych danych dla wszystkich adresów lub odrębnie dla każdego adresu https:// - w zależności od preferencji Zamawiającego

1. Jakie jest ogólne przeznaczenie aplikacji (np. system obiegu dokumentów, portal społecznościowy, serwis informacyjny, itp.)?

2. Lista ról użytkownika podlegających badaniu (np. zwykły użytkownik / redaktor / administrator)

3. Liczba / rząd wielkości liczby podstron aplikacji Web dostępnych dla każdej z ww. ról (w tym - ile podstron jest dostępnych bez uwierzytelnienia)

4. Lista punktów styku Systemu z wewnętrznymi i zewnętrznymi serwisami, bazami danych oraz serwisami centralnymi (np. Węzeł Identyfikacji Elektronicznej, ePUAP lub inne wykorzystane w danym projekcie)

5. Czy aplikacja udostępnia API? Jeżeli tak - jaka jest liczba endpointów/metod i - sumarycznie - parametrów podlegających badaniu?

6. Jaka jest liczba różnych rodzajów serwerów, wymienionych w opisie poszczególnych Systemów podlegających badaniu?

7. Jaka jest liczba różnych rodzajów serwerów baz danych, wymienionych w opisie poszczególnych Systemów podlegających badaniu?

Odpowiedź:

W zamówieniu podstawowym zostały wskazane maksymalne ilości składowych części systemu. Zamawiający nie jest w stanie wskazać szczegółów dla prawa opcji. Jeśli chodzi o ilości adresów https:// w zamówieniu podstawowym słowo maksymalnie określa stan faktyczny.

Pytanie nr 8:

Czy aplikacyjne ataki DoS/DDoS oraz inne testy z definicji wysoce inwazyjne mają być wykonane poza standardowymi godzinami pracy?

Odpowiedź:

Tak, prosimy o wykonanie tych testów po godzinie 16:00.

Pytanie nr 9:

Czy systemy bezpieczeństwa Zamawiającego zostaną skonfigurowane w sposób zapewniający, iż nie nastąpi automatyczne odcięcie ruchu generowanego przez Usługodawcę w trakcie symulowanych ataków (testów penetracyjnych)? Jeśli nie, jaką procedurę przewiduje Zamawiający dla przywrócenia dostępu Usługodawcy do testowanych aplikacji?

Odpowiedź:

Konfiguracja środowisk będzie uwarunkowana tym, czy testy będą przeprowadzane na środowisku testowym, czy produkcyjnym. W przypadku utraty łączności z systemami Zamawiającego Wykonawca będzie kontaktował się z Zespołem Bezpieczeństwa lub Administratorem systemu.

Pytanie nr 11:

Czy Zamawiający zapewni możliwość kontrolowanego, bezpiecznego zdalnego dostępu do Systemów podlegających badaniu również w celu umożliwienia zapoznania się z ich konfiguracją?

Odpowiedź:

Zamawiający zapewni możliwość zdalnego zapoznania się z konfiguracją Systemów.

Pytanie nr 12:

Par. 1 ust. 2 - Zamawiający wskazuje, iż "Wykonanie zamówienia podstawowego obejmuje rozpoczęcie audytu Systemu 1 oraz Systemu 2 w terminie nie dłuższym niż 10 dni od zlecenia wykonania audytu przez Zamawiającego, z zastrzeżeniem, że audyt musi zakończyć się nie później niż do 31 października 2024 r.". Czy Zamawiający zapewni umożliwienie realizacji testów powtórnych Systemów 1 i 2 w takim terminie, aby móc zakończyć je przed dniem 31.10.2024 r., ewentualnie wyłączy te testy z zakresu, który musi być zakończony do tej daty? (W OPZ Zamawiający wskazuje na możliwość realizacji testów powtórnych nawet do 2 miesięcy po przekazaniu i omówieniu wyników i raportów testów właściwych).

Odpowiedź:

Testy mają być wykonane do 31.10.2024, retesty natomiast mogą być wykonane po wprowadzeniu odpowiednich poprawek – do 2 miesięcy.

Pytanie nr 13:

Par. 1 ust. 6 - czy konsultacje, o których mowa, mają mieć formę opracowania pisemnego, dyskusji, czy innej albo dowolnej formy? Czy w przypadku konsultacji realizowanych w formie dyskusji możliwa jest konsultacja zdalna (telekonferencja, rozmowa telefoniczna)?

Odpowiedź:

Możliwa jest konsultacja zdalna, Zamawiający wymaga tylko pisemnej formy raportu z testów wraz z opisem podatności i rekomendacjami w celu ich wyeliminowania.

Pytanie nr 14:

Par. 2 ust. 4 - Zamawiający stanowi w tym miejscu iż "przeprowadzanie audytu nie doprowadzi do zmiany konfiguracji urządzeń Zamawiającego, ani nie wpłynie na ich prawidłowe funkcjonowanie", jednocześnie umieszczając w zakresie prac "Próby aplikacyjnych ataków DoS/ DDoS". Ataki takie z definicji wpływają negatywnie na funkcjonowanie testowanej infrastruktury, choć najczęściej można oczekiwać, że wpływ ten ustanie z końcem testu. To samo, choć z mniejszym prawdopodobieństwem, dotyczy innych rodzajów testów, które również z założenia mogą być złośliwe lub co najmniej niestandardowe - obliczone na wywołanie nieoczekiwanej reakcji obiektu-celu. Należy wskazać, że unikanie testów z definicji agresywnych, choć możliwe, wydłuży czas testu penetracyjnego

i obniży jakość uzyskanych wyników. Czy Zamawiający może zmienić zapis np. w sposób wskazujący, iż chodzi o permanentną zmianę konfiguracji lub stały (tj. wykraczający poza bezpośredni skutek realizowanego testu) wpływ na urządzenia Zamawiającego?

Odpowiedź:

Zapis ten dotyczy przede wszystkim środowisk produkcyjnych, by zapewnić ciągłość działania. Agresywne testy mogą być wykonane na środowisku testowym. W przypadku testów na środowisku produkcyjnym zakres ataków nie może zaburzyć ciągłości działania.

Pytanie nr 15:

Par. 8 ust. 1 lit. e) - "na podstawie § 7 ust. 11 niniejszej umowy" - czy chodzi o § 10 ust. 11 projektu Umowy?

Odpowiedź:

Zamawiający zmienia SWZ w ten sposób, że w załączniku nr 8 do SWZ – projekt umowy, wykreśla dotychczasową treść §8 ust 1 lit. e) i nadaje mu nowe brzmienie: „e. Wykonawca zapłaci Zamawiającemu karę umową z tytułu niewykonania obowiązku dokonania waloryzacji wynagrodzenia podwykonawcy na podstawie § 10 ust. 11 niniejszej umowy w wysokości 10.000zł za każdy przypadek.”

Pytanie nr 16:

W związku ze specyfiką przedmiotu zamówienia w celu umożliwienia dokonania prawidłowej wyceny Wykonawca zwraca się z wnioskiem o podanie dodatkowych informacji, a mianowicie:

• rodzaj i wersje systemów operacyjnych,

• opis każdej aplikacji, technologia wykonania (języki programowania, frameworki, wykorzystane silniki baz danych), lista funkcjonalności/modułów wraz z opisem, liczba i opis ról, architektura aplikacji, np. poprzez udostępnienie dokumentacji technicznej lub funkcjonalnej;

Odpowiedź:

Takie szczegółów informację nie zostaną udzielone ze względu na pkt 1 w OPZ "Przeprowadzenie testów penetracyjnych typu blackbox i greybox." co oznacza ,że osoba wykonująca test posiada częściowe informacje na temat badanego obszaru lub nie posiada informacji o badanym obszarze oraz nie ma uprawnień dostępu do schematów

Pytanie nr 17:

Wykonawca zwraca się z wnioskiem o wskazanie czy Zamawiający udostępni kody źródłowe aplikacji?

Odpowiedź:

Zamawiający nie udostępnimy kodu źródłowego aplikacji. Część aplikacji które będą testowane mogą być rozwiązaniami firm zewnętrznych dostępne w środowisku SaaS.

Dyrektor
Centrum Usług Informatycznych we Wrocławiu
Tymoteusz Przybylski

Dokument podpisano podpisem elektronicznym

Sporządziła: Marta Kozyra