DEPARTAMENT INFORMATYZACJI I REJESTRÓW SĄDOWYCH

Warszawa, 2 października 2020 r.

DIRS-XI-2420.18.2020

WYKONAWCY

Zamawiający – Ministerstwo Sprawiedliwości udziela odpowiedzi na pytania Wykonawców do Rozeznania rynku na „Przeprowadzenie i udokumentowanie audytu bezpieczeństwa systemu informatycznego Krajowego Rejestru Zadłużonych”:

Audyt bezpieczeństwa:

1. Prosimy o informację jaki ma być zakres audyt:
   a. Audyt zgodnie z ISO 27001?

   Ad. 1a Tak

   b. Audyt zgodnie z innymi normami, standardami, przepisami – jakimi?

   Ad. 1b Zgodnie z OPZ – Metodyka prowadzenia testów.

Testy penetracyjne:

1. Krótki opis do czego służy aplikacja oraz kluczowe funkcje (lista głównych funkcji).

   Ad. 1 Szczegółowy opis znajduje się w OPZ.

2. Lista metod logowania i uwierzytelniania: (np. ID, hasło, certyfikat, token, kod sms).

   Ad. 2 Dostępne metody to: token, login, hasło, certyfikat.

3. Lista metod autoryzacji operacji (jeśli występuje): (np. certyfikat, token, kod sms, urządzenia HSM (Hardware Security Module)).

   Ad. 3 Dostępne metody to: certyfikat.

„Projekt współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Społecznego Program Operacyjny Wiedza Edukacja Rozwój”

4. Liczba ról, które mają podlegać testom (np. gość, użytkownik zwykły, użytkownik rozszerzony, operator, administrator, itp.) wraz z krótkim opisem (np. administrator – zarządza prawami dostępu innych użytkowników).

   Ad. 4 Załącznik nr 1 OPZ – 5 głównych ról zawierające pod profile, dodatkowo grupy użytkowników branżowych

5. Lista / Orientacyjna liczba stron / podstron.
6. Lista / Orientacyjna liczba formularzy (podstron, na której użytkownik może wprowadzać dane np. strona logowania, formularz kontaktowy, składanie zamówień itp.) dynamicznie generowanych.
7. Orientacyjna liczba pól we wszystkich formularzach.
8. Szacunkowa (orientacyjna) liczba wszystkich używanych zmiennych (GET, POST, nagłówków - z uwzględnieniem ew. zmiennych przyjmowanych np. przez elementy Flash - jeśli występują) w całym testowanym systemie. Chodzi o sumaryczną / całkowitą liczę parametrów w całej aplikacji, która ma być przedmiotem testów.

   Ad. 5 – 8 System jest w fazie budowy.

Audyt kodu:

1. Technologia aplikacji:

a. Język w jakim napisana jest aplikacja (.net, JavaScript, J2EE, PHP) wraz z informacją o frameworkach.

   Ad. 1a Angular 9 lub nowszy, SpringBoot 2.x, MS VisualStudio Code, mssql server tools, TypeScript, JavaScript, CSS, OpenJDK 1.9 lub wyższa, T-sql, xml

b. Sposób budowy (MVC, MVP, itp).

   Ad. 1b Aplikacja zbudowana jako mikrousługi.

c. Technologia backend (SQL, NoSQL, itp.).

   Ad. 1c IBM DB2 LUW 11.1 lub wyższa, MS SQL Server 2019 wraz z ReportServer 2019

2. Wielkość kodu wraz z bibliotekami zewnętrznymi, ale z pominięciem wszystkich resource'ów (takich jak: pliki graficzne, metadane systemów zarządzania kodem, itp. - chodzi wyłącznie o sam kod badanej aplikacji oraz biblioteki zewnętrzne z których korzysta:
   a. Liczba linii kodu z komentarzami
   b. Liczba linii kodu bez komentarzy
   c. Objętość (MB)

   Ad. 2 a- c System jest w fazie budowy.

„Projekt współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Społecznego Program Operacyjny Wiedza Edukacja Rozwój”

3. Jakie są najistotniejsze moduły aplikacji? Ile linii kodu obejmują te moduły?

Ad. 3 Całość traktujemy równoważnie.

4. Czy zakres audytu ma obejmować cały kod (wszystkie linie kodu), czy też wybrane, najważniejsze fragmenty?

Ad. 4 Cały kod.

Pozostałe:

1. Jakie jest oczekiwane miejsce przeprowadzenia prac oraz sposób dostępu do aplikacji będącej przedmiotem testów? Prosimy o wybór spośród poniższych:

1) Zdalny dostęp do aplikacji w bezpośrednim połączeniu z sieci Internet
2) Zdalny dostęp do aplikacji udostępnionej poprzez tunel VPN zestawiony do Państwa siedziby
3) Zdalny dostęp do aplikacji udostępnionej poprzez tunel VPN zestawiony do zewnętrznego operatora hostingu
4) Lokalny bezpośredni dostęp do aplikacji
5) Lokalny dostęp do aplikacji przez tunel VPN

Prosimy o wskazanie, czy uzyskanie dostępu do aplikacji wymaga korzystania ze stacji przesiadkowej.

Ad. 1 Zamawiający oczekuje iż audyt bezpieczeństwa środowiska produkcyjnego musi odbyć się poprzez lokalny bezpośredni dostęp do aplikacji natomiast dla pozostałych środowisk Zamawiający oprócz lokalnego dostępu do aplikacji może rozważyć tunel VPN do stacji przesiadkowej wraz z monitorowaniem sesji z zachowaniem wszelkich procedur obowiązujących w MS niezbędnych do zestawienia takiego połączenia.

2. Czy zamawiający dopuszcza możliwość negocjowania warunków umowy w dalszym etapie postępowania?

Ad. 2 Usługa zostanie udzielona na zasadach określonych w ustawie Prawo zamówień publicznych w trybie przetargu nieograniczonego.

„Projekt współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Społecznego Program Operacyjny Wiedza Edukacja Rozwój”