Fundusze Europejskie
Polska Cyfrowa

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego

ZZ/41/055/U/20

Opis Przedmiotu Zamówienia na realizację audytu bezpieczeństwa platformy oraz infrastruktury IT w ramach projektu MOST DANYCH

MOST DANYCH

POLITECHNIKA GDAŃSKA

ul. G. Narutowicza 11/12
80-233 Gdańsk

tel. +48 58 347 65 19
fax: +48 58 347 14 90
e-mail: most@pg.gda.pl
http://pg.edu.pl/most

SPIS TREŚCI

POLITECHNIKA GDAŃSKA

ul. G. Narutowicza 11/12
80-233 Gdańsk

tel. +48 58 347 65 19
fax: +48 58 347 14 90
e-mail: most@pg.gda.pl
http://pg.edu.pl/most

A. Wstęp

Przedmiotem zamówienia jest usługa polegająca na przeprowadzeniu audytu oprogramowania oraz infrastruktury IT wytworzonych w ramach projektu *MOST DANYCH – Multidyscyplinarny Otwarty System Transferu Wiedzy – etap II: Open Research Data*, który jest współfinansowanego z Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014–2020. Szczegółowe informacje dotyczące projektu dostępne są na stronie pg.edu.pl/most/danych.

B. Wymagania wstępne przed realizacją audytu

Wykonawca przed przystąpieniem do realizacji audytu jest zobowiązany do podpisania klauzuli poufności i jest zobligowany do zachowania w tajemnicy wszelkich informacji pozyskanych w sposób bezpośredni lub pośredni dotyczących Zamawiającego, a w szczególności danych osobowych, technicznych, ekonomicznych lub organizacyjnych.

Zobowiązanie do zachowania poufności dotyczy wszelkich informacji udzielonych ustnie, pisemnie, drogą elektroniczną lub w inny sposób w odpowiedzi na zapytania Wykonawcy w trakcie realizacji zadań audytowych i jest bezterminowe.

C. Obszary prac audytowych

Przewiduje się realizację następujących obszarów audytowych oprogramowania platformy MOST Wiedzy dostępnej pod adresem mostwiedzy.pl uruchomionej na prywatnej chmurze obliczeniowej (składającej się z 30 maszyn).

D. Harmonogram realizacji audytów

Harmonogram realizacji audytu:

1. Rozpoczęcie prac: 01.02.2021 r.
2. Czas realizacji: nie później niz do 01.03.2021 r.

POLITECHNIKA GDAŃSKA

ul. G. Narutowicza 11/12
80-233 Gdańsk

tel. +48 58 347 65 19
fax: +48 58 347 14 90
e-mail: most@pg.gda.pl
http://pg.edu.pl/most

Dodatkowo zakłada się, że w przypadku przedstawienia Zamawiającemu rekomendacji wdrożenia zmian, które zostaną wprowadzone w środowisku produkcyjnym Wykonawca wykona testy regresyjne po uzgodnieniu z Zamawiającym terminu ich wykonania. Termin ich zakończenia nie może być jednak dłuższy niż 30 dni po zgłoszeniu do Wykonawcy wprowadzenia poprawki wykrytych błędów w środowisku produkcyjnym.

E. Szczegółowy zakres audytu oprogramowania

Zakres merytoryczny musi objąć następujące zadania:

Zakres prac.
Zadanie I. Przeprowadzenie testów penetracyjnych aplikacji.
Zadanie II. Przegląd konfiguracji środowiska aplikacji.
Zadanie III. Przegląd infrastruktury IT
Zadanie IV. Opracowanie raportu końcowego.
Zadanie V. Przeprowadzenie testów regresyjnych w przypadku wykrycia istotnych błędów pod względem istotności i prawdopodobieństwa ich wystąpienia.

Tabela 1. Zakres prac audytowych do wykonania w ramach obszaru I.

Szczegółowe wymagania zawarte w tabeli 1 zostały przedstawione poniżej.

Zadanie I. Przeprowadzenie testów penetracyjnych aplikacji.

Testy Penetracyjne będą realizowane przez Wykonawcę w następujący sposób:

a. Analiza systemu, konfiguracji dostępnych usług oraz dokumentacji systemu (techniczna dokumentacja architektury systemu, ok. 30 stron A4) pod kątem identyfikacji potencjalnych zagrożeń i opracowanie wykazu obszarów tych zagrożeń.
b. Przygotowanie metodologii planowanych testów penetracyjnych (rodzaj testu, narzędzie, harmonogram) wraz z ich uzasadnieniem. Metodyka musi pokrywać zagrożenia potencjalne, jak i zagrożenia zidentyfikowane na podstawie inwentaryzacji rzeczywistego systemu. Przy projektowaniu zakresu testów należy uwzględnić najnowsze opracowania (zawierające listy

POLITECHNIKA GDAŃSKA
ul. G. Narutowicza 11/12
80-233 Gdańsk
tel. +48 58 347 65 19
fax: +48 58 347 14 90
e-mail: most@pg.gda.pl
http://pg.edu.pl/most

krytycznych aspektów bezpieczeństwa systemów, listy najczęściej występujących podatności, kategoryzacji typów ataków, itp.) organizacji zajmujących się bezpieczeństwem teleinformatycznym (SANS, OISSG, OWASP, NIST, CERT, NASK).

c. Sporządzenie raportu z wykonanych testów, analiza wyników oraz przedstawienie rekomendacji minimalizujących zagrożenia, o ile takie zostały wykryte (*wymaganie szerzej opisane w pkt. Zadanie IV. Opracowanie raportu zaleceń audytowych*).

Testy penetracyjne (minimalnie na poziomie 1 standardu: OWASP ASVS 3.0.1) powinny odbyć się dla szeregu scenariuszy testowych:

- Użytkownik nieposiadający konta w aplikacji.
- Użytkownik posiadający w aplikacji konto o standardowych (obniżonych) uprawnieniach.
- Użytkownik posiadający w aplikacji konto redaktora/moderatora.
- Użytkownik posiadający w aplikacji konto administratora, ale nieposiadający uprawnień do serwera, na którym jest hostowana aplikacja.

System MOST Wiedzy dostępny jest w sieci Internet według podziału:

- publicznie odczyt 75%

- prywatnie/po zalogowaniu odczyt 25%

- publicznie zapis 0%

- prywatnie/po zalogowaniu zapis 100% – edycja danych przez zalogowanego użytkownika jest to około 70 formularzy do edycji danych

Dodatkowo, Wykonawca w ramach umowy, po wprowadzeniu przez Zamawiającego poprawek do wykrytych błędów podczas testów, przeprowadzi jedną iterację ponownych testów wskazanych przypadków testowych w zakresie zaraportowanych błędów oraz zweryfikuje, czy wykryte przez niego błędy zostały wyeliminowane i czy w związku z ich wprowadzeniem nie pojawiły się nowe problemy, widoczne bezpośrednio w trakcie powtarzania zgłoszonego przypadku testowego.

Zadanie II. Przegląd konfiguracji środowiska aplikacji.

POLITECHNIKA GDAŃSKA

ul. G. Narutowicza 11/12
80-233 Gdańsk

tel. +48 58 347 65 19
fax: +48 58 347 14 90
e-mail: most@pg.gda.pl
http://pg.edu.pl/most

Wykonawca zobowiązany będzie do przeprowadzenia przeglądu platformy, o ile aplikacja powiązana z usługą jest na niej osadzona oraz do konfiguracji środowiska aplikacji, w szczególności do:

- Konfiguracji serwerów baz danych wykorzystywanych w ramach platformy MOST Wiedzy – 4 serwery bazy danych (klaster 3 maszyn + 1 serwer)
- Konfiguracji serwerów WWW wykorzystywanych w ramach platformy MOST Wiedzy – 2 serwery:
    - wejściowy 4 usługi
    - wewnętrzny 3 usługi
- Konfiguracja serwerów aplikacji wykorzystywanych w ramach platformy MOST Wiedzy - 1 serwer: 4 usługi
- Konfiguracja serwerów PHP/Python wykorzystywanych w ramach platformy MOST Wiedzy – 3 serwery: 5 usług
- Konfiguracja serwerów składowania danych ORD wykorzystywanych w ramach platformy MOST Wiedzy – 1 serwer
- Ustawień systemów zabezpieczeń (w tym konfiguracji szyfrowanej transmisji danych) wykorzystywanych w ramach platformy MOST Wiedzy.

Konfiguracja środowiska ma zostać przebadana pod kątem zgodności z aktualnym stanem wiedzy zakresie bezpieczeństwa IT dla zastosowanych rozwiązań. Dodatkowo, tam gdzie jest to możliwe, Wykonawca odniesie się do opublikowanych zaleceń dotyczących konfiguracji aplikacji lub systemów w przyszłości, tak aby projektowane nowe rozwiązania informatyczne uwzględniały przedstawione rekomendacje w zakresie bezpieczeństwa.

Zadanie III. Przegląd infrastruktury IT

W ramach niniejszego zadania należy przeprowadzić audyt systemów wykorzystywanych w ramach platformy MOST Wiedzy dostępnych z sieci Internet.

Zakres audytu infrastruktury informatycznej:

Testy penetracyjne urządzeń (wykonane przy pomocy narzędzi analizujących sieć) będą obejmować m.in.:

POLITECHNIKA GDAŃSKA
ul. G. Narutowicza 11/12
80-233 Gdańsk
tel. +48 58 347 65 19
fax: +48 58 347 14 90
e-mail: most@pg.gda.pl
http://pg.edu.pl/most

- Badanie portów sieciowych celem wykrycia potencjalnych luk bezpieczeństwa w dostępnych usługach.
- Analizę odporności na ataki typu „denial of service”.
- Użycie przez Wykonawcę narzędzi eksploatujących wykryte luki bezpieczeństwa.
- Analizę środowiska sieciowego (skanowanie, dekodowanie, analiza protokołów i pakietów w sieci, statystyki ruchu sieciowego, przykładowa ewidencja zdarzeń sieciowych, przegląd topologii sieci, systemów operacyjnych pod kątem sieciowym).
- Analizę aktualności oprogramowania urządzeń (firmware), wygenerowanie listy wszystkich koniecznych uaktualnień oprogramowania.
- Audyt polegający na wykryciu oprogramowania typu Spyware.
- Audyt serwerów (parametry sprzętowe, parametry programowe, konfiguracja, administracja zasobami, bezpieczeństwo danych i stosowanych zasad archiwizacji w tym tworzenia kopii zapasowych).

Dodatkowo Wykonawca opracuje wytyczne w zakresie modernizacji i rozbudowy infrastruktury IT do poziomu spełniającego wymagania bezpieczeństwa wynikające z aktualnych przepisów prawa, dobrych praktyk branżowych i normy PN-ISO/IEC 27001:2014-12 (wytyczne do modernizacji: sieci teleinformatycznej, sprzętu komputerowego, serwerów, zarządzania i oprogramowania użytkowego) oraz wskaże obszary zmian dotyczące stosowanej lub brakującej dokumentacji (procedury, instrukcje), samej organizacji Centrum Usług Informatycznych i innych elementów, które mają lub mogą mieć wpływ na poziom bezpieczeństwa.

Zadanie IV. Opracowanie raportu końcowego.

Wykonawca zobowiązany będzie do przedstawienia szczegółowego raportu z wykonanych prac. Raport zawierać musi informacje o przebiegu badania, znalezionych błędach oraz zalecenia poaudytowe. Raporty końcowe zawierające podsumowanie wykonanych prac. Raporty obejmować muszą przynajmniej informacje wymienione poniżej:

- poziom krytyczności błędu według zaproponowanej przez Wykonawcą i uzgodnionej z Zamawiającym klasyfikacją,
- prawdopodobieństwo znalezienia/wykorzystania podatności przez atakującego – tzw. Likehood,*probability*,

POLITECHNIKA GDAŃSKA

ul. G. Narutowicza 11/12
80-233 Gdańsk

tel. +48 58 347 65 19
fax: +48 58 347 14 90
e-mail: most@pg.gda.pl
http://pg.edu.pl/most

- wpływ na system (lub inne systemy) – tzw. *impact*,
- szczegółowy sposób wykrycia i charakterystyka ataku (z uwzględnieniem zasad powtarzalności dla każdego przypadku). Informacje powinny być na tyle szczegółowe, aby była możliwa reprodukcja danego błędu,
- możliwości zabezpieczenia się przed podatnością i uwagi prowadzące do uniknięcia tego typu problemów w przyszłości,
- załączniki dokumentujące wystąpienie błędu (np. zrzuty ekranu, przykładowe pakiety atakujące lub świadczące o podatności, pliki zawierające zapis ruchu sieciowego w formacie *libpcap* itp.).

Wykonawca jest zobligowany do opracowania następujących definicji:

- kryterium wpływu na systemu (impact),
- prawdopodobieństwo wykorzystania podatności przez atakującego (likelihood),
- poziom krytyczności

oraz przedstawienia Zamawiającemu do akceptacji sposobu prezentacji wyników audytu. Zamawiający oczekuje, że dla wykrytych błędów o wpływie na system: średni lub krytyczny i równoczesnym prawdopodobieństwie: średni lub wysoki zostaną opracowane przez Wykonawcę szczegółowe rekomendacje zmian.

Struktura raportu powinna odpowiadać merytorycznemu podziałowi prac na obszary i aplikacje. Dodatkowo należy uwzględnić podział logiczny struktury aplikacji na następujące warstwy:

- baza danych,
- warstwa dostępu do bazy,
- warstwa biznesowa,
- warstwa prezentacji,
- warstwa bezpieczeństwa.

Ponadto Wykonawca może dodatkowo zaoferować Zamawiającemu prezentację wyników w formie 8-godzinnego szkolenia dla programistów systemu i administratorów środowiska, pozwalającego na zapoznanie się z wykrytymi błędami

POLITECHNIKA GDAŃSKA

ul. G. Narutowicza 11/12
80-233 Gdańsk

tel. +48 58 347 65 19
fax: +48 58 347 14 90
e-mail: most@pg.gda.pl
http://pg.edu.pl/most

oraz na uzyskanie wiedzy w zakresie ich unikania. Za przeprowadzenie prezentacji wyników Wykonawca może otrzymać 10 punktów w kryterium oceny ofert.

Wykonawca, z dniem podpisania protokołu odbioru raportu, przenosi na Zamawiającego autorskie prawa majątkowe do raportu na polach eksploatacji, obejmujących:

- odtwarzanie,
- utrwalanie i trwałe zwielokrotnianie całości lub części utworu, wszystkimi znanymi w chwili zawierania Umowy technikami, w tym techniką drukarską, reprograficzną, zapisu magnetycznego oraz techniką cyfrową,
- przekazywanie,
- przechowywanie,
- wyświetlanie,
- wprowadzanie do pamięci komputera wraz z prawem do dokonywania modyfikacji,
- tłumaczenie,
- przystosowywanie,
- zmiany układu lub jakiekolwiek inne zmiany.

POLITECHNIKA GDAŃSKA

ul. G. Narutowicza 11/12
80-233 Gdańsk

tel. +48 58 347 65 19
fax: +48 58 347 14 90
e-mail: most@pg.gda.pl
http://pg.edu.pl/most