Załącznik nr 1 do Ogłoszenia o planowanym zamówieniu

Opis przedmiotu zamówienia

1. Wstęp

Niniejszy dokument precyzuje wymagania dotyczące przedmiotu zamówienia poprzez określenie:

a) celu przedmiotu zamówienia.
b) wymagań w zakresie usług realizowanych w ramach przedmiotu zamówienia,
c) wymagań w zakresie produktów, które mają być wytworzone w związku z realizacją przedmiotu zamówienia,
d) wymagań w zakresie formuły realizacyjnej,
e) systemu teleinformatycznego objętego usługą,
f) miejsca realizacji zamówienia.

2. Cel audytu

Usługa audytu bezpieczeństwa zostanie zrealizowana w celu weryfikacji spełnienia obowiązków nałożonych na Zamawiającego przez obowiązujące przepisy prawa w zakresie stosowanego w projekcie systemu zarządzania bezpieczeństwem informacji. Główne cele audytu to:

a) Pozyskanie informacji na temat istniejących podatności i słabości w obszarze bezpieczeństwa audytowanych systemów teleinformatycznych.
b) Wiarygodna ocena bezpieczeństwa zasobów systemów teleinformatycznych.
c) Rekomendacja rozwiązań w zakresie utrzymania wysokiego poziomu bezpieczeństwa systemów teleinformatycznych.

3. Przedmiot zamówienia

Usługa audytu bezpieczeństwa systemów teleinformatycznych wskazanych w rozdziale 4 niniejszego opisu przedmiotu zamówienia powinna obejmować działania, podzielone na etapy testów zewnętrznych i wewnętrznych (ze względu na umiejscowienie opisanych systemów informatycznych), określone w następujący sposób:

A. Testy systemu (etap I)

W ramach audytu bezpieczeństwa Wykonawca powinien wykonać:

Testy penetracyjne, w ramach których powinna zostać wykonana symulacja włamań do systemów oraz sieci i zidentyfikowane słabe punkty systemu zabezpieczeń prowadzony metodą blackbox (bez znajomości kodów źródłowych ani konfiguracji aplikacji)

Usługa powinna obejmować następujący zakres zadań:

- wykorzystanie manualnych oraz automatycznych metod prowadzenia audytu,
- detekcja błędów aplikacyjnych (kilka testów na każdą z poniższych klas):
  - Security Misconfiguration (błędy w konfiguracji zabezpieczeń, umożliwiające nieuprawnione działanie)
  - Sensitive Data Exposure (potencjalna możliwość nieuprawnionego dostępu do wrażliwych danych)
  - Missing Function Level Access Control
  - Using Components with Known Vulnerabilities (użycie komponentów posiadających znane podatności – np. dana wersja komponentu itp)
  - Unvalidated Redirects and Forwards
  - Insecure Direct Object References
  - Injection (SQL injection, XML injection etc.)
  - Clickjacking (tzw. porywanie kliknięć)
  - XXE (XML eXternal Entity).
  - XSS (Cross Site Scripting) – błędy typu reflected oraz stored.
  - Detekcja zabezpieczeń na podatność CSRF (Cross Site Request Forgery).
  - Broken Authentication and Session Management (badanie losowości ID sesji, próba detekcji składni nazywania cookie sesyjnego, sprawdzenie bezpieczeństwa budowy formularza logowania).
  - Authorization Bypass (próby dostępu do zasobów bez uwierzytelnienia użytkownika).
  - Code Execution (próby wykonania wrogiego kodu na serwerze).
  - Information Leakage (próby detekcji wycieku istotnych informacji – technicznych i biznesowych – z serwera).
  - Insecure Communications (np. dostęp do istotnych danych – np. konta administracyjnego bez szyfrowania).
  - Source Disclosure (próby prowadzące do ujawnienia kodów źródłowych wykorzystanego oprogramowania).
  - Path Traversal.
  - Open Redirection.
  - Denial of Service (DoS).
  - File Inclusion.
  - Response Splitting.
  - Deserialization of untrusted data.
  - Testy web serwera obejmujące m.in.:
    - Bezpieczeństwo skonfigurowanego mechanizmu SSL
    - Dostępność komunikatów o błędach
    - Analiza podatności występujących w zainstalowanej wersji serwera
    - Dostępność nadmiarowych metod HTTP
  - analiza metod uwierzytelniania, w ramach którego wykonane zostaną w szczególności następujące czynności:
    - weryfikacja certyfikatów SSL,
    - weryfikacja kanałów komunikacyjnych.

- oraz innych ataków zdefiniowanych na najnowszej dostępnej liście podatności OWASP

- analizę urządzeń zewnętrznych.
- Raport z wykonanych czynności audytowych w ramach etapu I zgodny z zakresem określonym w pkt 5 lit. a) i b).

B. Etap testów kontrolnych (etap II)

Testy kontrolne, w ramach których należy sprawdzić poprawność instalacji i konfiguracji systemów teleinformatycznych, analiza systemowa stosowanych zabezpieczeń systemów teleinformatycznych wykazująca, w szczególności czy zastosowane w ich produkcji technologie są odpowiednie, czy systemy nie są narażone na podatności, czy istnieją nowsze bezpieczniejsze narzędzia w tym zakresie, kontekście najnowszych rozwiązań teleinformatycznych wykorzystywanych w utrzymaniu wysokiego poziomu bezpieczeństwa systemów teleinformatycznych, w szczególności chroniących przed zagrożeniami wynikającymi z cyberataków.

Usługa w ramach etapu testów kontrolnych musi obejmować następujący zakres zadań:

a) audyt warstwy bazodanowej, w ramach którego wykonane zostaną w szczególności następujące czynności:
   a. wykonanie ataku Sniffing, Scanning (skanowanie portów usług bazodanowych i próba pozyskania haseł metodą brute force), Spoofing, Hijacking, Dos, Buffer Overflow,
   b. możliwość realizacji kodu po stronie serwera lub klienta,
   c. sprawdzenie metod szyfrowania danych,
   d. weryfikacja procedur przechowywania haseł dostępowych,
   e. badanie bazy automatycznym analizatorem,
   f. wskazanie metod zmniejszających ryzyko wycieku danych z bazy danych,
   g. sprawdzenie wdrożenia podstawowych zasad hardeningowych bazy (np.: dostępność domyślnych użytkowników guest, partycjonowanie bazy, składowanie logów, logowanie nietypowych zdarzeń, dostępność wybranych niebezpiecznych procedur /funkcji składowanych),
   h. sprawdzenie komunikacji z klientem bazodanowym - wykorzystanie mechanizmów kryptograficznych (logowanie się klienta oraz transfer danych),
   i. ogólna recenzja architektury bazy (wykorzystane mechanizmy autoryzacji oraz uwierzytelniania; segmentacja uprawnień, wykorzystanie widoków; wykorzystanie procedur składowanych),
   j. weryfikacja sposobu wykonywania kopii zapasowych,
   k. analiza sposobu udostępnienia RDBMS na poziomie sieciowym.
b) testy penetracyjne wewnątrz mające na celu zidentyfikowanie możliwości przeprowadzenia włamania wewnątrz siedziby Zamawiającego, w obrębie wskazanych usług w pkt. 4
   a. skanowanie podatności w udostępnionych usługach sieciowych,
   b. lokalizacja podatności w udostępnionych aplikacjach webowych (np. próby ominięcia ekranów logowania, kradzież danych z aplikacji).
   c. po przejęciu kontroli nad co najmniej jednym z systemów – próba eskalacji ataku na pozostałe maszyny, systemy w LAN,
c) dokonanie próby przejęcia kontroli nad kontami użytkowników,
d) dokonanie próby wykonania nieautoryzowanych operacji bezpośrednio na bazie danych,
e) proces identyfikacji podatności systemów i sieci na ataki typu: DoS, DDos, SQL Injection, Sniffing, Spoffing, XSS, Hijacking, Backdoor, Flooding, Password (próba pozyskania haseł metodą brute force) i inne,
f) raport z wykonanych czynności audytowych w ramach etapu II zgodny z zakresem określonym w pkt 5 lit. a) i b).

4. Usługi i produkty techniczne objęte przedmiotem zamówienia

Usługi i produkty techniczne powstałe w wyniku budowy Portalu Rad-on - zintegrowanej platformy informacyjnej w obszarze szkolnictwa wyższego i nauki w Polsce, która powstaje w ramach projektu "Zintegrowany system usług dla nauki — etap II":

a) Model wymiany danych – wewnętrzny system integracji systemów oparty na Apache Kafka (stan na 2019-09-04)

- szacunkowa liczba unikalnych podstron / formularzy: brak formularzy
- technologia wykonania systemu: Apache Kafka, Java, Spring
- liczba różnych grup użytkowników (o różnych uprawnieniach): brak użytkowników, integracja pomiędzy systemami, zabezpieczenie SSL
- liczba linii kodu źródłowego: około 5 584 bez kodu Open Source Apache Kafka

b) Moduł centralnego logowania (MCL) oparty o system KeyCloak – https://mcl.opi.org.pl (stan na 2019-09-04):

- szacunkowa liczba unikalnych podstron / formularzy: 5
- technologia wykonania systemu: KeyCloak Java, Spring Security, LDAP, MySQL
- liczba różnych grup użytkowników (o różnych uprawnieniach): MLC zajmuje się wyłącznie identyfikacją i uwierzytelnianiem, natomiast autoryzacja przeprowadzana jest w systemach dziedzinowych.
- liczba linii kodu źródłowego: około 5 000 bez kodu Open Source

c) Portal obywatelski wraz z własnym CMS (stan na 2019-09-04)

- szacunkowa liczba unikalnych podstron / formularzy: 45
- technologia wykonania systemu: Angular, TypeScript, Java, Lucene, ElasticSearch, Oracle
- liczba różnych grup użytkowników (o różnych uprawnieniach):tylko użytkownicy anonimowi
- liczba linii kodu źródłowego: 39 300

d) Hurtowania i BI w technologii Oracle (stan na 2019-09-04)

- szacunkowa liczba unikalnych podstron / formularzy: bez ograniczeń – odpowiada liczbie utworzonych raportów
- technologia wykonania systemu: Oracle, Oracle Business Intelligence EE, Oracle Data Integrator, Hadoop danych
- liczba różnych grup użytkowników (o różnych uprawnieniach): 50 imiennych użytkowników Oracle Business Intelligence, liczba uprawnień nie jest możliwa do oszacowania będą tworzone w zależności od potrzeb
- liczba linii kodu źródłowego: około 30 000

e) Usługi udostępniania danych (REST) - https://radon.nauka.gov.pl/pl/api/katalog-udostepniania-danych/uslugi-udostepniania-danych (stan na 2019-09-04)

- szacunkowa liczba unikalnych podstron / formularzy: 13 metod REST (+80 metod słownikowych)
- technologia wykonania systemu: Java, Spring Boot, Oracle, Elasticsearch, Apache Kafka
- liczba różnych grup użytkowników (o różnych uprawnieniach): tylko użytkownicy anonimowi
- liczba linii kodu źródłowego: 27 900

f) Usługi edycji danych (REST) - https://polon.nauka.gov.pl/opi-ws (stan na 2019-09-04)

- szacunkowa liczba unikalnych podstron / formularzy: około 150 metod REST i SOAP
- technologia wykonania systemu: Java, Spring, Apache Cxf
- liczba różnych grup użytkowników (o różnych uprawnieniach): 134 (te same co w systemie POL-on)
- liczba linii kodu źródłowego: 33 000

g) Dedykowane zestawienia publiczne - (stan na 2019-09-04)

- szacunkowa liczba unikalnych podstron / formularzy: 1
- technologia wykonania systemu: Java, Angular, TypeScript, ElasticSearch, Oracle
- liczba różnych grup użytkowników (o różnych uprawnieniach): tylko użytkownicy anonimowi
- liczba linii kodu źródłowego: 500

h) Dostęp do danych obywatela – wdrożenie na przełomie września i października

- szacunkowa liczba unikalnych podstron / formularzy: nie więcej niż 14
- technologia wykonania systemu: Java, Angular 2+, Oracle, Kubernetes
- liczba różnych grup użytkowników (o różnych uprawnieniach): 1 (użytkownicy, którzy będą mieli dostęp do usługi, będą mieli takie same uprawnienia, brak podziału na role)
- liczba linii kodu źródłowego: około 8000

i) Udostępnianie metadanych (REST / API) - https://radon.nauka.gov.pl/pl/api/katalog-udostepniania-danych/uslugi-udostepniania-danych/Meta (stan na 2019-09-04)

- szacunkowa liczba unikalnych podstron / formularzy: 4 usługi REST
- technologia wykonania systemu: Java, Spring Boot, Oracle, Elasticsearch
- liczba różnych grup użytkowników (o różnych uprawnieniach): tylko użytkownicy anonimowi
- liczba linii kodu źródłowego: 100

Docelowe adresy URL zostaną podane po podpisaniu umowy.

5. Wymagania w zakresie dokumentów dostarczonych w związku z wykonanymi usługami

W wyniku realizacji prac, opisanych w punkcie 3 Wykonawca dostarczy, następujące produkty:

a) raport po każdym zrealizowany etapie z przeprowadzonego audytu bezpieczeństwa systemów, który zawierać będzie:

- zakres, metodykę i szczegółowy opis przeprowadzonych prac,
- opis przyjętego modelu oceny luk i podatności,
- listę wykrytych podatności i zagrożeń bezpieczeństwa, w poszczególnych warstwach wskazanych w pkt 1 części opisującej przedmiot zamówienia, w tym
  - szczegółowy opis wykrytych luk i podatności,
  - klasyfikację poziomu wykrytych luk i podatności,
  - szczegółowe zalecenia, dotyczące usunięcia zidentyfikowanych zagrożeń,
  - analizę wykrytych ryzyk pod kątem bezpieczeństwa informacji,
  - opis sposobu weryfikacji istnienia wykrytych luk i podatności;

ze wskazaniem źródła z opisem podatności

- listę dodatkowych zaleceń wynikających z możliwych do zastosowania mechanizmów bezpieczeństwa.

b) informację na temat narzędzi audytowych potrzebnych do realizacji wewnętrznych audytów bezpieczeństwa

6. Miejsce realizacji zamówienia

Czynności audytu będą wykonywane w siedzibie Zamawiającego lub w miejscach przez niego wskazanych. Zadania Wykonawcy w zakresie opracowania niezbędnej dokumentacji będą realizowane w siedzibie Wykonawcy.