zał. nr 1 do zapytania ofertowego nr ST.0140.73.2019

Opis przedmiotu zamówienia

I. Przedmiotem zamówienia jest usługa polegająca na:

1. Przeprowadzeniu audytu:

a) spełnienia wymogów Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 w sprawie KRI - Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych w POSiR (zwane KRI);

b) spełnienia wymogów Rozporządzenia Parlamentu Europejskiego i Rady 2016/679 z dnia 27 kwietnia 2016 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych zwane RODO);

c) bezpieczeństwa systemu informatycznego Zamawiającego;

d) spełnienia wymagań obowiązującej w POSiR Polityki bezpieczeństwa oraz procesów i dokumentów dot. ochrony danych.

2. Przeprowadzenia testów penetracyjnych, które pozwolą ocenić aktualny stan bezpieczeństwa systemów Zamawiającego i określić obecność znanych podatności i odporności na próby przełamania stosowanych zabezpieczeń.

3. Przedstawienie rekomendacji dotyczących zmian w treści Polityki bezpieczeństwa, procedur, instrukcji, procesów i dokumentacji Zamawiającego.

II. Cel audytu

1. Audyt w POSiR we wszystkich jego oddziałach (8 lokalizacji na terenie miasta Poznania) i działach (9 działów w Dyrekcji POSiR) którego celem jest:

a) Weryfikacja poziomu spełnienia wymagań Rozporządzenia Parlamentu Europejskiego i Rady 2016/679 z dnia 27 kwietnia 2016 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE zwanego dalej RODO,

b) Weryfikacja poziomu spełnienia wymagań Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych w POSiR, zwanego dalej KRI,

c) Weryfikacja bezpieczeństwa systemu informatycznego Zamawiającego,

d) Weryfikacja poziomu spełnienia wymagań obowiązującej w POSiR Polityki bezpieczeństwa oraz procesów i dokumentów dot. ochrony danych.

III. Zakres audytu

1. Audyt spełnienia wymogów RODO, KRI oraz obowiązującej w POSiR Polityki bezpieczeństwa

Zakres prac podczas audytu spełnienia wymogów RODO, KRI oraz obowiązującej w POSiR Polityki bezpieczeństwa pod kątem charakterystyki organizacji, jej modelu biznesowego, zasobów oraz aktywów (dla wszystkich oddziałów i działów POSiR) będzie obejmował w szczególności:

a) Zapoznanie się ze strukturą organizacyjną Zamawiającego;

b) Analizę i ocenę dokumentacji w zakresie:

- bezpieczeństwa informacji,
- ochrony danych osobowych,
- zarządzania ryzykiem,

w tym polityk, procedur, zarządzeń, instrukcji, regulaminów wewnętrznych, umów powierzenia danych osobowych zawieranych przez Zamawiającego, dokumentacji dotyczącej zarządzania ryzykiem, rejestrów czynności przetwarzania oraz innych dokumentów;

c) Analizę procesów przetwarzania danych osobowych w szczególności w takich obszarach jak:

- pozyskiwanie danych w tym m.in. analiza podstawy prawnej pozyskiwania danych osobowych, przegląd formularzy służących do zbierania danych i klauzul informacyjnych;
- rozliczalność systemów informatycznych służących do przetwarzania danych osobowych w następujących oddziałach i działach POSiR: oddział ZS i GO (systemy Plaza i Gastro), oddział KA (system Fitnet), oddział RA (system Reservise), dział DO (systemy płacowo-kadrowe), dział DI (system zapisów na imprezy biegowe), dział FE (systemy księgowe);
- przechowywanie i usuwanie danych/analiza retencji danych z uwzględnieniem ograniczenia czasowego przechowywania danych oraz ich usuwania w formie papierowej (wszystkie oddziały i działy POSiR) oraz w systemach informatycznych w następujących oddziałach i działach POSiR: oddział ZS i GO (systemy Plaza i Gastro), oddział KA (system Fitnet), oddział RA (system Reservise), dział DO (systemy płacowo-kadrowe), dział DI (system zapisów na imprezy biegowe), dział FE (systemy księgowe) oraz poczta elektroniczna we wszystkich oddziałach i działach Zamawiającego;

d) zapewnienie ochrony danych osobowych w fazie projektowania i domyślnej ochrony danych (privacy by design, privacy by default);

d) stan bezpieczeństwa fizycznego siedziby dyrekcji POSiR oraz wszystkich oddziałów POSiR (budynki oraz pomieszczenia) na podstawie wizji lokalnej miejsc przetwarzania danych osobowych.

2. Audyt bezpieczeństwa systemu informatycznego

Zakres prac podczas audytu bezpieczeństwa systemu informatycznego będzie obejmował rozwiązania sieciowe, serwerowe, stanowiska robocze oraz punkty styku z siecią publiczną w szczególności:

a) Audyt bezpieczeństwa infrastruktury sieciowej:

- dokładna inwentaryzacja urządzeń sieciowych (adresy IP, konfiguracja urządzeń, konfiguracja zapory ogniowej, podział na sieci logiczne i fizyczne) w siedzibie Dyrekcji Zamawiającego i wszystkich jego oddziałach oraz przedstawienie logicznej i fizycznej struktury sieci w formie zobrazowania graficznego przedstawiającego wszystkie urządzenia sieciowe oraz powiązania pomiędzy nimi,
- analiza urządzeń i ich parametrów technicznych zapewniających stronie Zamawiającej dostęp do sieci Internet - w tym serwera brzegowego, urządzeń UTM, Firewall, routerów,
- analiza konfiguracji sieci lokalnej,
- analiza oprogramowania wykorzystywanego przez Zamawiającego w zakresie zabezpieczenia informatycznego,
- analiza sposobu połączenia segmentów pomiędzy sobą,
- analiza metody komunikacji pomiędzy segmentami sieci,

b) Audyt bezpieczeństwa infrastruktury serwerowej:

- analiza bezpieczeństwa zainstalowanych usług (czy zainstalowane oprogramowanie jest aktualne, czy zainstalowane oprogramowanie posiada znane luki w bezpieczeństwie, kto ma dostęp do udostępnionych usług),
- analiza bezpieczeństwa serwerów pod kątem dostępu użytkowników (czy jedynie uprawnieni użytkownicy mają dostęp do usług, czy udostępnione usługi zawierają jedynie te dane które są wymagane),
- analiza bezpieczeństwa uprawnień poszczególnych użytkowników oraz grup użytkowników,
- analiza bezpieczeństwa fizycznego infrastruktury serwerowej.

c) Audyt bezpieczeństwa poczty, domeny, stron internetowych zamawiającego oraz systemów teleinformatycznych, ze szczególnym uwzględnieniem systemów w których przetwarzane są dane osobowe w szczególności w systemach informatycznych w następujących oddziałach i działach POSiR: oddział ZS i GO (systemy Plaza i Gastro), oddział KA (system Fitnet), oddział RA (system

Reservise) dział DO (systemy płacowo-kadrowe), dział DI (system zapisów na imprezy biegowe), dział FE (systemy księgowe), wszystkie oddziały i działy (system obiegu umów Redmine) w tym analizę szyfrowania danych dla danych przesyłanych przez sieci publiczne.

d) Audyt bezpieczeństwa stacji roboczych:

- analiza kontroli dostępu do stacji roboczych,
- analiza zainstalowanego oprogramowania znajdującego się na stacjach roboczych,
- analiza bezpieczeństwa stacji roboczych pod kątem zainstalowanych usług, dostępów zdalnych do stacji roboczych, bezpieczeństwa ochrony antywirusowej.

e) Audyt kopii zapasowych i ciągłości działania:

- analizę poprawności wykonywanych kopii zapasowych,
- analiza częstotliwości wykonywania kopii zapasowych,
- analiza bezpieczeństwa wykonywanych kopii zapasowych,
- analiza systemu ciągłości działania.

3. Testy penetracyjne

Zakres prac podczas testów penetracyjnych.

3.1 Wymagane jest przeprowadzenie dwóch wariantów testów penetracyjnych dla wszystkich oddziałów i działów Zamawiającego:

- testów penetracyjnych wykonanych ze stacji roboczej podłączonej do systemu informatycznego z zewnątrz mających na celu zidentyfikowanie podatności na włamanie,
- testów penetracyjnych wykonanych ze stacji roboczej podłączonej do wewnętrznego systemu informatycznego w celu zidentyfikowania możliwości przeprowadzenia włamania z wewnątrz sieci Zamawiającego.

3.2 Podczas testów penetracyjnych powinny zostać wykonane m.in. następujące czynności:

a) skanowanie publicznych baz danych dostępnych w Internecie w celu pozyskania informacji o przedmiocie testów,
b) rozpoznanie dostępnych z obszaru Internetu komputerów i urządzeń sieciowych, rodzaju i wersji systemów operacyjnych oraz oprogramowania użytkowego pod kątem wykrywania znanych luk bezpieczeństwa,
c) analiza topologii sieci komputerowej widzianej z Internetu,
d) analiza otrzymanych wyników pod kątem przygotowania symulacji włamań,
e) symulacja włamań,

f) wstępna penetracja systemu za pomocą skanerów portów TCP i UDP oraz skanerów zabezpieczeń powszechnie stosowanych przez hakerów, dostępnych w zasobach sieci Internet,
g) wykrywanie ścieżek dostępowych do testowanej sieci (routing przez Internet),
h) skanowanie wszystkich adresów IP dostępnych z internetu w poszukiwaniu otwartych portów,
i) identyfikacja usług dostępnych przez otwarte porty,
j) weryfikacja poprawności zastosowanych protokołów szyfrujących (m.in. IKE oraz SSL),
k) testy zabezpieczeń systemu za pomocą profesjonalnych skanerów zabezpieczeń,
l) identyfikacja podatności pozwalających na uzyskanie nieuprawnionego dostępu do systemów oraz danych (m.in. Buffer Overflow, Format String, Default Credentials and Configuration),
m) weryfikacja siły haseł za pomocą ataków typu brute-force,
n) analiza możliwości wykonania ataków Denial of Service (DoS).
o) ocena odporności zabezpieczeń systemu na ataki destrukcyjne za pomocą narzędzi dostępnych w sieci Internet,
p) ocena poprawności reakcji systemu zabezpieczeń na wykonywane ataki,
q) analiza bezpieczeństwa systemu zaporowego Firewall,
r) analiza wyników testów pod kątem oceny zagrożenia integralności systemu oraz możliwości dostępu do danych przez osoby upoważnione.

3.3 Podczas testów penetracyjnych aplikacji oraz serwisów www (stron/wordpressów oraz systemu Redmine) zakres zadań obejmuje:

a) testy bezpieczeństwa aplikacji pod kątem:
    - ataków semantycznych na adres URL,
    - ataków związanych z ładowaniem plików,
    - ataków typu Cross-Site Scripting,
    - ataków typu Cross-Site Request Forgery,
    - ataków typu MITM (Man in the Middle),
    - podrabiania zarządzania formularza,
    - sfałszowania żądania http,
    - ujawnienia danych przechowywanych w bazie,
    - trawersowania katalogów,
    - ujawniania kodu źródłowego,

- przepełnienia bufora lub stosu,
- wstrzykiwania kodu wykonywalnego innych języków programowania.

b) badanie enumeracji i wykorzystania znanych podatności w celu uzyskania nieautoryzowanego dostępu,
c) badanie możliwości podszywania się pod użytkowników i uzyskania nieautoryzowanego dostępu do systemu
d) badanie możliwości podszywania się pod użytkowników uprzywilejowanych i uzyskanie dostępu do systemu
e) badanie możliwości blokowania/umożliwienia dostępu do systemu wszystkim lub wybranym jej użytkownikom,
f) badanie możliwości modyfikacji/usunięcia danych z systemu.

3.4 Podczas testów penetracyjnych poczty elektronicznej zakres zadań obejmuje:

a) testy poprawności konfiguracji serwera IMAP, SMTP,
b) testy pod kątem przesyłania poczty niechcianej (SPAM),
c) testy pod kątem przesyłania oprogramowani typu malware,
d) testy pod kątem podszywania się pod nadawców poczty,
e) testy bezpieczeństwa protokołów pocztowych,
f) testy pod katem odporności na awarie.

4. Raport poaudytowy

Wynikiem przeprowadzonych audytów i testów powinien być raport poaudytowy zawierający:

a) raport dla kierownictwa obejmujące ocenę poziomu spełnienia wymogów RODO, KRI, Polityki bezpieczeństwa Zamawiającego oraz ocenę bezpieczeństwa systemu informatycznego w tym podsumowanie zidentyfikowanych podatności wraz z opisem zagrożenia, a także główne rekomendacje dotyczące poprawy bezpieczeństwa informacji, danych i systemu informatycznego.
b) raport techniczny zawierający szczegóły techniczne zidentyfikowanych podatności następującej zawartości:
    - wskazujący dokładne miejsca, w których występują realne bądź potencjalne problemy z bezpieczeństwem informacji;
    - zawierający zapis przeprowadzonych testów oraz informacje umożliwiające przeprowadzenie retestów wykazanych podatności;

- zawierający rekomendacje w zakresie eliminacji zidentyfikowanych podatności oraz poprawy poziomu bezpieczeństwa;
- zawierający zrzuty ekranu, ewentualny kod źródłowy wszystkich skryptów oraz
- programów stworzonych na potrzeby testów bezpieczeństwa oraz inne załączniki ułatwiające reprodukcję zidentyfikowanych podatności.

c) propozycje zmian w treści Polityki bezpieczeństwa, procedur, instrukcji, procesów i dokumentacji Zamawiającego wraz z proponowaną treścią nowych (zmienionych lub dodanych) zapisów.