Załącznik nr 1 do Zapytania ofertowego

Szczegółowy Opis Przedmiotu Zamówienia

Na wykonanie Diagnozy Cyberbezpieczeństwa wg Konkursu Grantowego Cyfrowa Gmina Oś V. Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia - REACT-EU
Działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia

Spis treści

1. Wymagania

Wymagania wobec Wykonawcy

Wykonawca musi posiadać wiedzę i doświadczenie poparte odpowiednimi referencjami w zakresie audytu bezpieczeństwa oraz dołączyć:

Wykonawca w ciągu ostatnich trzech lat, a jeżeli okres prowadzenia działalności jest krótszy wykonał, na potwierdzenie którego powinien przedstawić:

- co najmniej pięć referencji, protokołów odbioru lub umów poświadczających przeprowadzenie audytu bezpieczeństwa w jednostkach administracji publicznej z należytą starannością w zakresie spełnienia wymagań wynikających ISO 27001 albo KRI o wartości brutto 4 000,00 każdy,
- co najmniej pięć referencji, protokołów odbioru lub umów poświadczających przeprowadzenie audytu bezpieczeństwa w jednostkach administracji publicznej z należytą starannością w zakresie wynikającym projektu Cyfrowa Gmina,
- co najmniej trzy referencje, protokoły odbioru lub umowy poświadczające przeprowadzenie testów penetracyjnych aplikacji webowych w jednostkach administracji publicznej z należytą starannością o wartości 20 000,00 zł brutto każda,
- co najmniej jedna referencja, protokół odbioru lub umowa poświadczająca przeprowadzenie testów socjotechnicznych w sektorze publicznym albo w podmiotach prowadzących działalność komercyjną z należytą starannością o wartości 17 000,00 brutto,

Wymagania wobec osób realizujących przedmiot zamówienia

- osobami posiadającymi wiedzę i doświadczenie w zakresie bezpieczeństwa informacji zgodnie z zakresem opisanym poniżej:
    - przynajmniej jedna osoba musi posiadać:
        - co najmniej 3 letnie doświadczenie w zakresie pełnienia funkcji testera bezpieczeństwa (pentestera) *,
        - certyfikat OCSP (Offensive Security Certified Professional),
        - certyfikat uprawniający do przeprowadzenia audytu zgodnie z rozporządzeniem Ministra Cyfryzacji 1 z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu,
        - co najmniej 3 letnie doświadczenie w zakresie prowadzenia audytów bezpieczeństwa uwzględniających założenia wynikające z normy ISO 27001,
    - przynajmniej jedna osoba musi posiadać:
        - co najmniej 3 letnie doświadczenie w zakresie prowadzenia audytów bezpieczeństwa uwzględniających założenia wynikające z normy ISO 27001 i/lub KRI,
        - certyfikat uprawniający do przeprowadzenia audytu zgodnie z rozporządzeniem Ministra Cyfryzacji 1 z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu,
    - przynajmniej jedna osoba musi posiadać:
        - co najmniej 3 letnie doświadczenie w zakresie pełnienia funkcji testera bezpieczeństwa (pentestera) *,
        - certyfikat OCSP (Offensive Security Certified Professional),
        - posiadać wiedzę i doświadczenie w zakresie przygotowywania oraz wykonywania testów socjotechnicznych.

* - przez testy penetracyjne należy rozumieć przeprowadzenie testów mających na celu wykrycie nieznanych podatności. Skanowanie pod kątem znanych podatności narzędziami typu Nessus, OpenVAS (Greenbone), BurpSuite, Acunetix i inne podobne nie spełnia wymagania testów penetracyjnych.

Niepotwierdzenie powyższych wymagań skutkować będzie odrzuceniem oferty.

Wynikiem prac Wykonawcy ma być audyt na podstawie załącznika nr 8 oraz dokumenty audytowe dedykowane pozostałym obszarom objętym zamówieniem. Dokumenty audytowe, o których mowa muszą odzwierciedlać pełny obszar prac objętych zamówieniem. W ramach dokumentacji Wykonawca opisze każde zidentyfikowane ryzyko wraz z precyzyjnym opisem proponowanej metody usunięcia tego ryzyka oraz oceni ryzyka techniczne zgodnie z klasyfikacją CVSS. Prócz tego ryzyka, o których mowa muszą zostać wprowadzone do rejestru ryzyk.

2. Zestawienie ilościowe.

Przedmiot zamówienia obejmuje przeprowadzenie diagnozy cyberbezpieczeństwa

Lp.	Nazwa	Ilość
1	Przeprowadzenie diagnozy cyberbezpieczeństwa	1
2	Przeprowadzenie testów penetracyjnych aplikacji/stron www	1
3	Przeprowadzenie testów penetracyjnych infrastruktury	1
4	Przeprowadzenie skanów na występowanie znanych podatności	1
5	Liczba fizycznych lokalizacji podlegających testom	1
6	Liczba serwerów	2
7	Liczba urządzeń sieciowych	2
8	Liczba łącz do Internetu	2
9	Liczba stacji roboczych użytkowników	46
10	Liczba urządzeń mobilnych	4
11	Liczba użytkowników	46
12	Liczba użytkowników bezpiecznej poczty elektronicznej	46

3. Opis przedmiotu zamówienia

3.1. Przeprowadzenie diagnozy cyberbezpieczeństwa.

1. Diagnoza musi być przeprowadzona lokalnie w siedzibie Zamawiającego.
2. Diagnoza musi być przeprowadzona w zakresie określonym w „Formularzu informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa" stanowiącym załącznik nr 8 do Regulaminu Konkursu Grantowego Cyfrowa Gmina.
3. Diagnoza musi być przeprowadzona przez osobę posiadającą certyfikat uprawniający do przeprowadzenia audytu, o którym mowa w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu.
4. Wykonawca przekaże wynik przeprowadzonej diagnozy w postaci pliku wypełnionego arkusza kalkulacyjnego formularza, o którym mowa w pkt. 2, podpisanego podpisem cyfrowym

(weryfikowanym certyfikatem kwalifikowanym lub przy wykorzystaniu profilu zaufanego) przez osobę posiadającą uprawnienia, o których mowa w pkt. 3.

5. Wykonawca w przypadku stwierdzonych nieprawidłowości przekaże zamawiającemu szczegółowe wytyczne w jaki sposób należy je zniwelować oraz przeprowadzi bezpośrednie konsultacje na ten temat z przedstawicielem zamawiającego.

3.2. Przeprowadzenie testów penetracyjnych aplikacji

Wykonawca powinien przeprowadzić testy penetracyjne zgodnie z zestawieniem kategorii określonych na stronie https://owasp.org/www-project-top-ten/ „Top 10 Web Application Security Risks". Należy przez to rozumieć, że Wykonawca w ramach testów wykona czynności sprawdzające każdy obszar podatności wskazanych w Top 10.

Testom będzie podlegała strona główna Urzędu oraz strona Biuletynu Informacji Publicznej oraz pozostałe strony wskazane przez zamawiającego w ilości określonej w zestawieniu.

Przez testy penetracyjne należy rozumieć ręczne poszukiwanie podatności:

- w konfiguracji serwerów baz danych oraz www, które pozostają w dyspozycji Zamawiającego,
- w kodzie źródłowym aplikacji podlegających testom,
- przeprowadzenie testu odporności na atak typu DDoS,
- w sposobie wykonywania się aplikacji.

3.3. Przeprowadzenie testów penetracyjnych infrastruktury

Wykonawca powinien przeprowadzić testy penetracyjne infrastruktury, których celem jest odnalezienie podatności wynikających z błędnej konfiguracji urządzeń sieciowych, urządzeń podłączonych do sieci przewodowej oraz bezprzewodowej oraz konfiguracji tych sieci. Testy penetracyjne infrastruktury mają być przeprowadzone lokalnie, w siedzibie Zamawiającego..

3.3.1. Testy bezpieczeństwa sieci LAN

- Próby oszukania działania przełącznika;
- Ataki Man-in-the-Middle: podsłuchiwanie, przechwytywanie sesji;
- Określenie producenta urządzeń sieciowych;
- Próba ominięcia kontroli dostępu rozwiązań typu NAC;
- Próba uzyskania dostępu do wydzielonych VLAN-ów;
- Uzyskanie informacji z protokołów routingu;
- Próba zaburzenia działania protokołów routingu;
- Test zabezpieczeń protokołu SNMP na urządzeniach sieciowych: próba odczytu informacji, próba zmiany ustawień;
- Uzyskiwanie informacji z usług: DNS, SMTP, SNMP, SMB;
- Weryfikacja stosowanych kluczy SSL;
- Sprawdzenie restrykcji i ich skuteczności w komunikacji do sieci Internet;
- Analiza architektury pod względem optymalnego działania.

3.3.2. Testy bezpieczeństwa sieci bezprzewodowych

- Atak na Access Point – DoS;
- Łamanie siłowe haseł sieci WPA/WPA2-PSK;
- Łamanie siłowe haseł sieci WPA/WPA2-Enterprise: atak na protokół PEAP, atak na protokół EAP-TLS;
- Podstawienie fałszywego Access Pointa;
- Powiązanie wybranego komputera siecią Wi-Fi;

- Utworzenie mapy zasięgu sieci bezprzewodowych;
- Wykrycie ukrytych sieci Wi-Fi;
- Omijanie filtracji adresów MAC;
- Ataki Man-in-the-Middle przy sieciach bezprzewodowych: podsłuchiwanie w sieciach bezprzewodowych, przechwytywanie sesji w sieciach bezprzewodowych
- Określenie producenta Access Point-a;
- Analiza architektury pod względem optymalnego dział.

3.3.3. Testy styku sieci firmowej z Internetem

- Skanowanie urządzenia w celu określenia działających usług;
- Identyfikacja wersji uruchomionych usług;
- Pogrupowanie odnalezionych usług do poszczególnych systemów, które je udostępniają;
- Próba wykonania nadużyć działających usług;
- Weryfikacja czy znalezione usługi i systemy posiadają znane błędy i podatności;
- Próba wyszukania nowych podatności: ze znajomością kodu źródłowego, bez znajomości kodu źródłowego;
- Test wykrywalności ataków przez urządzenie brzegowe;
- Analiza architektury pod względem optymalnego działania;
- Określenie nazwy producenta;
- Weryfikacja stosowanych kluczy SSL;
- Próba przeforsowania mechanizmów uwierzytelnienia wystawionych usług;
- Weryfikacja odporności urządzenia i wystawionych usług na nietypowy ruch.

3.3.4. Testy urządzeń służących do filtrowania ruchu sieciowego

- Generowanie złośliwego ruchu: w warstwie sieci, w warstwie aplikacji, na aplikacje webowe, ataki wychodzące;
- Przesyłanie malware'u poprzez użycie próbki przynajmniej 30 złośliwych programów;
- Generowanie ruchu o nietypowych godzinach;
- Próba wejścia na serwisy www zablokowane przez urządzenia;
- Próba nawiązania połączenia z podejrzanymi domenami;
- Nawiązanie połączenia do sieci Tor;
- Zweryfikowanie działania komunikatorów, torrentów;
- Przeprowadzanie skanowania portów różnymi technikami, łącznie z obniżającymi wykrycie;
- Generowanie błędnego ruchu.

3.4. Testy oprogramowania antywirusowego

Wykonawca będzie zobowiązany do przeprowadzenia testu skuteczności działania oprogramowania antywirusowego w zakresie zatrzymywania złośliwego oprogramowania przez posiadane przez Zamawiającego oprogramowanie antywirusowe. W tym celu Zamawiający przekaże Wykonawcy jedną licencję na stację roboczą a Wykonawca na środowisku wirtualny przez siebie przygotowanym przeprowadzi testy przy użyciu próbki przynajmniej 30 złośliwych programów. Próbka powinna być uzgodniona z Zamawiającym i zawierać co najmniej oprogramowanie typu adware, trojan, ransomware, worm.

3.5. Testy socjotechniczne

3.5.1. Szczegółowy opis testów

Wykonawca będzie zobowiązany do przeprowadzenia testów socjotechnicznym w zakresie opisanym poniżej. Wszelkie elementy infrastruktury w tym oprogramowania leżą po stronie Wykonawcy.

3.5.2. Stworzenie fałszywych stron

Wykonawca w ramach wykonywanych działań utworzy 3 fałszywe strony i zamieści je w Internecie w kontrolowanym przez siebie środowisku (lokalizację środowiska Wykonawca uzgodni z Zamawiającym). Na tym środowisku Wykonawca zainstaluje oraz skonfiguruje wymagane komponenty do prawidłowego przeprowadzenia testów socjotechnicznych z wykorzystaniem fałszywych stron.

Opisywany sposób testu winien być powiązany z innymi formami ataków, które mają na celu skłonienie do odwiedzenia spreparowanej strony. W tym celu Wykonawca użyje metod: spoofing wiadomości e-mail.

Wykonawca otrzyma listę adresów e-mail, które będą poddane testom.

Wykonawca w uzgodnieniu z Zamawiającym zarejestruje 3 domeny, które poprzez zastosowanie techniki typosquatting posłużą do uruchomienia stron wyłudzających informacje.

3.5.3. Wysłanie wyłudzających informację wiadomości e-mail (spoofing)

Wykonawca przygotuje scenariusze testu, które przedstawi Zamawiającemu do akceptacji a następnie na ich podstawie przygotuje i uzgodni z Zamawiającym treść 3 wiadomości e-mail, które posłużą do nakłonienia odbiorcy do wykonania czynności określonych w wiadomości.

Przynajmniej jedna z wiadomości musi zawierać specjalnie przygotowany plik, którego wykonanie przez odbiorcę wiadomości będzie powodowało automatyczne przekazanie danych świadczących o podjęciu takiej czynności.

3.5.4. Zakres zbieranych informacji

W ramach testów Wykonawca będzie zbierał wyłącznie minimalny zakres informacji stanowiący potwierdzenie dla wykonania przez odbiorcę czynności przekazanych w wiadomości. Zakres minimalny to:

- Nazwa użytkownika
- Data i godzina wykonania czynności

Wykonawcy nie wolno zbierać jakichkolwiek haseł albo informacji poufnych.

W celu uzyskania najlepszych wyników prowadzonych testów Wykonawca uzgodni z Zamawiającym wykonanie w odpowiednich przerwach oraz o określonych godzinach. Pod uwagę zostaną wzięte również lokalizacje fizyczne w celu rozproszenia informacji przekazywanych pomiędzy osobami znającymi się na określonym środowisku.

3.6. Rejestr ryzyka

Wykonawca w ramach Zamówienia będzie prowadził rejestr ryzyka, w którym dokona oceny oraz analizy każdego zidentyfikowanego ryzyka przypisanego do ww. obszarów dotyczących testów penetracyjnych, testów socjotechnicznych oraz wynikające z obserwacji. Rejestr ma posłużyć Zamawiającemu jako wyznacznik dla określenia elementów stwarzających największe zagrożenie dla:

- zagrożenia organizacji w zakresie wycieku danych,
- zagrożenia w zakresie braku ciągłości działania,
- zagrożenia w zakresie zwiększenia kosztów funkcjonowania organizacji,
- estymacji możliwości rozwoju (rozbudowy, utrzymania) elementów stanowiących przedmiot audytu w okresie co najmniej 3 lat od dnia zakończenia audytu przez Wykonawcę,

Rejestr ryzyka przedstawiono poniżej w postaci spisu pól posiadających wartości liczbowe oraz informacyjne, wpływające na ostateczny kształt oceny każdego zidentyfikowanego ryzyka.

Wskaźnik stanu	ID Ryzyka	Data identyfikacji ryzyka	Narażony zasób	Opis ryzyka	Wstępna ocena ryzyka					Wynik oceny ryzyka	Status ryzyka	Właściciel ryzyka	Reakcja na ryzyko	Plan minimalizacji ryzyka	Ocena ryzyka po minimalizacji					Wynik oceny ryzyka po minimalizacji	Status ryzyka po minimalizacji	Ocena ryzyka	Data kolejnego przeglądu
					Poufność	Integralność	Dostępność	Prawdopodobieństwo	Wpyw						Poufność	Integralność	Dostępność	Prawdopodobieństwo	Wpływ				
y	I D	10.06. 2022	Dane osobowe	Przykład	T	T	T	1	3	3	Niskie	Jan Kowalski	Kontroluj	Uszczelnić	T	T	T	4	3	12	Średnie	Poważne	10.10. 2022