ROZDZIAŁ II - OPIS PRZEDMIOTU ZAMÓWIENIA

Świadczenie usługi testów bezpieczeństwa w okresie 18 miesięcy.

CPV:
79212000-3 – usługi audytu
72800000-8 – usługi audytu komputerowego

Przedmiotem zamówienia jest świadczenie usługi testów bezpieczeństwa w okresie 18 miesięcy, w wymiarze średnim od 2 do 20 dni roboczych miesięcznie, w każdym kwartale.
Przedmiotowe usługi podzielone są na cztery części:

1. Część 1 - Dekompozycja oprogramowania lub/i firmware'u urządzeń;
2. Część 2 - Testy bezpieczeństwa obszaru aplikacji;
3. Część 3 - Testy bezpieczeństwa obszaru infrastruktury;
4. Część 4 - Testy bezpieczeństwa kodu źródłowego.

Świadczenie usługi testów bezpieczeństwa w poszczególnych częściach będzie realizowane w okresie 18 miesięcy od dnia podpisania umowy lub do wyczerpania limitu kwotowego umowy, w zależności od tego które ze zdarzeń nastąpi wcześniej.

A. Przedmiot usługi

1. Zakres testów bezpieczeństwa w poszczególnych częściach

1.1. **Część 1** - Dekompozycja oprogramowania lub/i firmware'u urządzeń, a w tym:
- 1.1.1. identyfikacja stosowanych komponentów firm trzecich,
- 1.1.2. określenie wersji wykorzystywanych bibliotek,
- 1.1.3. analiza podatności zidentyfikowanych komponentów,
- 1.1.4. analiza podatności metodą inżynierii wstecznej.

1.2. **Część 2** - Testy bezpieczeństwa obszaru aplikacji wykonywane zgodnie z jednym ze standardów:
- 1.2.1. Open Web Application Security Project (OWASP),
- 1.2.2. The Open Source Security Testing Methodology Manual (OSSTMM),
- 1.2.3. The penetration testing execution standard (PTES).

1.3. **Część 3** - Testy bezpieczeństwa obszaru infrastruktury wykonywane zgodnie z jednym ze standardów:
- 1.3.1. Open Web Application Security Project (OWASP),
- 1.3.2. The Open Source Security Testing Methodology Manual (OSSTMM),
- 1.3.3. The penetration testing execution standard (PTES).

1.4. **Część 4** - Testy bezpieczeństwa kodu źródłowego, a w tym:
- 1.4.1. Konfiguracja środowiska testowego na serwerach Zamawiającego, w oparciu o licencje Zamawiającego,

1.4.2. Analiza statyczna kodu źródłowego,
1.4.3. Analiza oparta o najlepsze praktyki w obszarze bezpiecznego wytwarzania oprogramowania:
1.4.3.1. zalecenia Software Engineering Institute CERT Oracle Coding Standard for Java,
1.4.3.2. zalecenia organizacji OWASP (między innymi standard ASVS oraz dokument OWASP Code Review Guide).

2. Usługi dla wszystkich części realizowane będą z uwzględnieniem poniższych warunków:

2.1. Testy i analizy odbywać się będą w zależności od możliwości technicznych: w środowisku Zamawiającego, bądź zdalnie – poza lokalizacją Zamawiającego.
2.2. Niedopuszczalne jest stosowanie rozwiązań chmurowych, SaaS, itp.
2.3. Zamawiający na potrzeby wykonania usługi może zapewnić:
2.3.1. stację roboczą,
2.3.2. maszynę wirtualną,
2.3.3. przestrzeń dyskową,
2.3.4. Oprogramowanie i licencje na narzędzia zainstalowane na stacji roboczej Zamawiającego.
2.4. Wykonawca na potrzeby wykonania usługi musi zapewnić:
2.4.1. stację roboczą do realizacji prac zdalnych,
2.4.2. możliwość wykonania prac w siedzibie Zamawiającego,
2.4.3. niezbędne narzędzia, oprogramowanie, licencje.
2.5. W ramach testów i analiz Wykonawca zapewni wsparcie w interpretacji wyników.
2.6. Wykonawca będzie zobowiązany do zachowania trwałości zespołu realizującego prace zlecane przez Zamawiającego. Wszelkie zmiany będą wymagały akceptacji Zamawiającego oraz weryfikacji dokumentów potwierdzających kompetencje, doświadczenie i certyfikaty wskazane w części C (poniżej). Wykonawca będzie informował Zamawiającego o wszelkich zmianach w zespole Wykonawcy realizującym prace objęte przedmiotem umowy z 10-dniowym wyprzedzeniem.
2.7. Roboczodzień oznacza dzień roboczy w godzinach od 9:00 do 17:00.
2.8. Podstawą obliczenia wynagrodzenia będzie stawka za jeden roboczodzień realizacji zlecenia przemnożona przez liczbę roboczodni określoną w Zamówieniu.
2.9. Cena brutto określona w stawce za roboczodzień obejmuje wszystkie koszty Wykonawcy, w tym podatek VAT oraz wynagrodzenie za przeniesienie praw autorskich majątkowych oraz prawa do wykonywania praw zależnych do utworów i wyrażania zgody na wykonywanie tych praw do wszystkich utworów wytworzonych w związku z realizacją umowy wykonawczej.
2.10. Umowa zobowiązująca Wykonawcę do realizacji zlecanych prac w łącznym wymiarze:
a) 25 roboczodni dla części 1 - Dekompozycja oprogramowania lub/i firmware'u urządzeń;
b) 124 roboczodni dla części 2 - Testy bezpieczeństwa obszaru aplikacji;
c) 40 roboczodni dla części 3 - Testy bezpieczeństwa obszaru infrastruktury;
d) 60 roboczodni dla części 4 - Testy bezpieczeństwa kodu źródłowego;
zawarta zostanie na okres 18 miesięcy. W całym okresie obowiązywania Umowy, prace będą zlecane wg potrzeb Zamawiającego, gdzie minimalna liczba roboczodni zleconych

przez Zamawiającego wyniesie odpowiednio dla punktu 2.10. ppkt a) 10 roboczodni, b) 62 roboczodni, c) 20 roboczodni, d) 30 roboczodni.

2.11. Wykonawca rozpocznie realizację zleconych prac w terminie nie dłuższym niż 5[1] dni roboczych od przekazania zamówienia przez Zamawiającego.

2.12. Podstawą wystawienia faktury za dane Zamówienie będzie dokonanie odbioru zleconych prac i podpisanie protokołu zdawczo-odbiorczego do Zamówienia.

B. Wymagania dotyczące produktów

1. W ramach każdego Zamówienia Wykonawca zobowiązany jest do przedstawienia Zamawiającemu raportu (w formacie docx), zgodnego z szablonem dostarczonym przez Zamawiającego, zawierającego co najmniej:

1.1. Podsumowanie dla kierownictwa (streszczenie ogólne), a w nim informacje opisujące jakościowo wyniki usługi, przy czym podsumowanie nie może zawierać informacji, które w przypadku ujawnienia zmniejszają bezpieczeństwo badanego obszaru lub systemu.

1.2. Opracowanie szczegółowe, które będzie zawierać:

1.2.1. W części ogólnej:

a) Streszczenie, w tym w zależności od zakresu Zamówienia szczegółowego ogólną opinię nt. bezpieczeństwa, przeciwskazań do produkcyjnego wdrożenia, zgodności z określonymi standardami i regulacjami wewnętrznymi i zewnętrznymi, zakres analizy lub koncepcji;

b) Główne ustalenia, zalecenia lub założenia – odpowiednio do zakresu Zamówienia szczegółowego;

1.2.2. W części szczegółowej:

a) Opis konfiguracji, nr wersji i stanu testowanego obszaru;

b) Szczegółowy opis dat przeprowadzenia testów, użytych narzędzi, konfiguracji środowiska testowego;

c) Zakres przeprowadzonych testów i sposób ich przeprowadzenia;

d) Obserwacje audytowe;

e) Wyniki testów i ich interpretację;

f) Listę wykrytych luk (w tym podatności) opatrzonych komentarzem audytora wraz z ich kwalifikacją w znaczeniu dla bezpieczeństwa (krytyczność);

g) Wnioski z audytu;

h) Zalecenia i rekomendacje;

i) Zakres czynności niezbędnych do weryfikacji i potwierdzenia luk (podatności) – o ile przedmiot audytu tego dotyczy;

j) Zakres czynności niezbędnych do zaimplementowania rekomendacji poaudytowych;

k) W przypadku konieczności wykonania zmian konfiguracyjnych lub instalacji uaktualnień/poprawek, Wykonawca przedstawi opis konfiguracji lub instalacji.

[1] Termin stanowi kryterium wyboru oferty

2. Oczekiwany zakres prac wykonywanych w ramach testów bezpieczeństwa:

Dla części I, II, III, IV

2.1. Zapoznanie się z zakresem i przedmiotem testów.

2.2. Skonfigurowanie narzędzi, w celu przeprowadzenia testów.

2.3. Przeprowadzenie testów i analiz, zgodnie ze specyfikacją zakresu umieszczoną w pkt 1 Zakres testów bezpieczeństwa w poszczególnych częściach, mających na celu wskazanie zagrożeń i ryzyk wynikających z:

2.3.1. Zastosowanych technologii i standardów zabezpieczeń,

2.3.2. Błędów oprogramowania,

2.3.3. Poprawnej konfiguracji komponentów systemowych, aplikacyjnych i sieciowych,

2.3.4. Istniejących / Wykrytych styków sieci o różnym charakterze (np. styku z siecią Internet, styku sieci systemów utrzymywanych / budowanych w COI z innymi sieciami,

2.3.5. Potencjalnych zagrożeń ze strony sieci wewnętrznej (LAN/WAN/WLAN) i zewnętrznej (Internet),

2.3.6. Zastosowanych rozwiązań na poziomie architektury i ich wpływu na wydajność systemu,

2.3.7. Prawidłowości wyboru rozwiązania sprzętowego dla aplikacji pod kątem bezpieczeństwa i wydajności.

2.4. Sporządzenie i dostarczenie Zamawiającemu raportu z przeprowadzonych prac, zgodnie z wymaganiami zdefiniowanymi powyżej w pkt 1.

2.5. Zamawiający zastrzega sobie prawo, że na jego zgłoszenie Wykonawca, bez dodatkowych opłat, usunie zidentyfikowane nieprawidłowości, wyjaśni nieścisłości i/lub przeprowadzi warsztaty celem omówienia i wyjaśnienia informacji przedstawionych w produktach prac na zasadach zawartych w umowie.

Dla części IV

2.6. Przeprowadzone w ramach realizacji części IV testy i analizy jakości kodu źródłowego powinny uwzględniać specyfikę testowanego rozwiązania, a w szczególności:

2.6.1. Podatności systemów (wynikające z błędów w aplikacji i oprogramowania, z którymi aplikacja się komunikuje np. bazy danych, serwery proxy, etc.) na znane ataki,

2.6.2. Jakości kodu źródłowego z punktu widzenia bezpieczeństwa aplikacji – weryfikacja, czy kod spełnia dobre wzorce projektowe oraz dobre praktyki przyjęte u Zamawiającego oraz w analogicznych systemach informatycznych,

2.6.3. Jakości kodu źródłowego z punktu widzenia wydajności aplikacji – zbadanie czy ilość przesyłanych/przetwarzanych danych jest optymalna przy przyjętym rozwiązaniu,

2.6.4. Podatności kodu źródłowego co najmniej w obszarach:

2.6.4.1. Walidacji danych wejściowych,

2.6.4.2. Autentykacji i autoryzacji,

2.6.4.3. Podatności na ataki odmowy usługi,

2.6.4.4. Nieautoryzowanego dostępu, umożliwiającego naruszenie bezpieczeństwa danych.

C. Wymagania dotyczące zespołu audytowego

1. Wymaga się, aby Wykonawca dysponował jednocześnie dla:

1.1. **Część I** – zespołem składającym się z 2 osób, z których każda posiada poniższe kompetencje:

1.1.1. doświadczenie w przeprowadzaniu analizy firmware'u urządzeń z wykorzystaniem technik inżynierii wstecznej, potwierdzone zgłoszeniem w okresie ostatniego roku co najmniej jednej podatności (CVE, PSV lub ICS-VU) dla rynkowych produktów.

1.2. **Część II** – zespołem składającym się z 6 osób, przy czym każda z nich musi posiadać co najmniej jeden z poniższych certyfikatów, z zastrzeżeniem, że zespół musi posiadać dwa różne certyfikaty spośród niżej wymienionych:

1.2.1. aktualny certyfikat Offensive Security Certified Professional (OSCP) lub równoważny, który pokrywa obszary:

1.2.1.1. Bezpieczeństwo ofensywne,

1.2.1.2. Techniki przełamywania zabezpieczeń sieciowych, systemów operacyjnych oraz oprogramowania,

1.2.1.3. Narzędzia bezpieczeństwa,

1.2.1.4. Techniki wykrywania błędów oprogramowania,

1.2.2. Aktualny certyfikat eLearnSecurity Mobile Application Penetration Tester (eMAPT) lub równoważny, który pokrywa obszary:

1.2.2.1. Zbieranie informacji,

1.2.2.2. Inżynieria wsteczna dla aplikacji Android,

1.2.2.3. Wykorzystanie podatności w systemie Android,

1.2.2.4. Stosowanie zasad bezpieczeństwa,

1.2.2.5. Wady logiczne,

1.2.2.6. Szyfrowanie i kryptografia,

1.2.2.7. Identyfikacja podatnych implementacji,

1.2.3. Aktualny certyfikat eLearnSecurity Web application Penetration Tester (EWPT) lub równoważny, który pokrywa obszary:

1.2.3.1. Procesy i metodologie testów penetracyjnych,

1.2.3.2. Analiza i inspekcja aplikacji WEB,

1.2.3.3. Gromadzenie informacji,

1.2.3.4. Zarządzanie podatnościami WEB aplikacji,

1.2.3.5. OWASP Testing Guide / OWASP Top 10,

1.2.3.6. Manualne potwierdzenie podatności XSS, SQLi itd.,

1.2.3.7. Zaawansowana raportowanie i remediacja,

1.2.4. Aktualny certyfikat eLearn Security Web application Penetration Tester eXtreme (EWPTX) lub równoważny, który pokrywa obszary:

1.2.4.1. Procesy i metodologie testów penetracyjnych,

1.2.4.2. Analiza i kontrola aplikacji WEB,

1.2.4.3. Zaawansowane umiejętności raportowania i działań naprawczych,

1.2.4.4. Zaawansowana wiedza i umiejętności omijania podstawowych oraz zaawansowanych filtrów XSS, SQLi itd.,

1.2.4.5. Zaawansowana znajomość różnych systemów zarządzania bazami danych,

1.2.4.6. Umiejętność przygotowania własnego exploita, gdy gotowe narzędzia zawodzą,

1.2.5. Aktualny certyfikat Offensive Security Certified Expert (OSCE) lub równoważny, który pokrywa obszary:
1.2.5.1. Ataki na aplikacje webowe (min. XSS/LFI),
1.2.5.2. Analiza i wstrzykiwanie kodu złośliwego w pliki wykonywalne PE,
1.2.5.3. Omijanie systemów antywirusowych,
1.2.5.4. Omijanie mechanizmów zabezpieczenia pamięci,
1.2.5.5. Fuzzing, konstruowanie exploitów 0-day,
1.2.5.6. Obchodzenie zabezpieczeń,
1.2.5.7. Atakowanie infrastruktury sieciowej,
1.2.6. Aktualny certyfikat Certified Ethical Hacker (CEH) lub równoważny, który pokrywa obszary:
1.2.6.1. Analiza oraz ocena ryzyka danych oraz systemów,
1.2.6.2. Kontrola bezpieczeństwa, wykrywanie oraz zapobieganie atakom,
1.2.6.3. Znajomość narzędzia, systemów, programów,
1.2.6.4. Znajomość procedur oraz metodologii,
1.2.6.5. Znajomość Regulacji i polityk.

1.3. **Część III** – zespołem składającym się z 4 osób, przy czym każda z nich musi posiadać co najmniej jeden z poniższych certyfikatów, z zastrzeżeniem, że zespół musi posiadać dwa różne certyfikaty spośród niżej wymienionych:
1.3.1. aktualny certyfikat Offensive Security Certified Professional (OSCP) lub równoważny, który pokrywa obszary:
1.3.1.1. Bezpieczeństwo ofensywne,
1.3.1.2. Techniki przełamywania zabezpieczeń sieciowych, systemów operacyjnych oraz oprogramowania,
1.3.1.3. Narzędzia bezpieczeństwa,
1.3.1.4. Techniki wykrywania błędów oprogramowania,
1.3.2. Aktualny certyfikat eLearnSecurity Mobile Application Penetration Tester (eMAPT) lub równoważny, który pokrywa obszary:
1.3.2.1. Zbieranie informacji,
1.3.2.2. Inżynieria wsteczna dla aplikacji Android,
1.3.2.3. Wykorzystanie podatności w systemie Android,
1.3.2.4. Stosowanie zasad bezpieczeństwa,
1.3.2.5. Wady logiczne,
1.3.2.6. Szyfrowanie i kryptografia,
1.3.2.7. Identyfikacja podatnych implementacji,
1.3.3. Aktualny certyfikat eLearnSecurity Web application Penetration Tester (EWPT) lub równoważny, który pokrywa obszary:
1.3.3.1. Procesy i metodologie testów penetracyjnych,
1.3.3.2. Analiza i inspekcja aplikacji WEB,
1.3.3.3. Gromadzenie informacji,
1.3.3.4. Zarządzanie podatnościami WEB aplikacji,
1.3.3.5. OWASP Testing Guide / OWASP Top 10,
1.3.3.6. Manualne potwierdzenie podatności XSS, SQLi itd.,
1.3.3.7. Zaawansowane raportowanie i remediacja,

1.3.4. Aktualny certyfikat eLearn Security Web application Penetration Tester eXtreme (EWPTX) lub równoważny, który pokrywa obszary:
1.3.4.1. Procesy i metodologie testów penetracyjnych,
1.3.4.2. Analiza i kontrola aplikacji WEB,
1.3.4.3. Zaawansowane umiejętności raportowania i działań naprawczych,
1.3.4.4. Zaawansowana wiedza i umiejętności omijania podstawowych oraz zaawansowanych filtrów XSS, SQLi itd.,
1.3.4.5. Zaawansowana znajomość różnych systemów zarządzania bazami danych,
1.3.4.6. Umiejętność przygotowania własnego exploita, gdy gotowe narzędzia zawodzą,
1.3.5. Aktualny certyfikat Offensive Security Certified Expert (OSCE) lub równoważny, który pokrywa obszary:
1.3.5.1. Ataki na aplikacje webowe (min. XSS/LFI),
1.3.5.2. Analiza i wstrzykiwanie kodu złośliwego w pliki wykonywalne PE,
1.3.5.3. Omijanie systemów antywirusowych,
1.3.5.4. Omijanie mechanizmów zabezpieczenia pamięci,
1.3.5.5. Fuzzing, konstruowanie exploitów 0-day,
1.3.5.6. Obchodzenie zabezpieczeń,
1.3.5.7. Atakowanie infrastruktury sieciowej,
1.3.6. Aktualny certyfikat Certified Ethical Hacker (CEH) lub równoważny, który pokrywa obszary:
1.3.6.1. Analiza oraz ocena ryzyka danych oraz systemów,
1.3.6.2. Kontrola bezpieczeństwa, wykrywanie oraz zapobieganie atakom,
1.3.6.3. Znajomość narzędzia, systemów, programów,
1.3.6.4. Znajomość procedur oraz metodologii,
1.3.6.5. Znajomość Regulacji i polityk.

1.4. **Część IV** – zespołem składającym się z 3 osób, w tym co najmniej 1 osoba posiadająca łącznie poniższe kompetencje i certyfikaty:
1.4.1. Aktualny certyfikat Certified Information Security Professional (CISSP) wydany przez ISC2 lub równoważny, który pokrywa obszary:
1.4.1.1. Bezpieczeństwo i zarządzanie ryzykiem,
1.4.1.2. Bezpieczeństwo telekomunikacji i sieci,
1.4.1.3. Obsługa incydentów,
1.4.1.4. Testy bezpieczeństwa,
1.4.1.5. Bezpieczeństwo oprogramowania,
1.4.1.6. Zarządzanie tożsamością i dostępami,
1.4.2. Aktualny certyfikat CSSLP lub równoważny, który pokrywa obszary:
1.4.2.1. Wymagania bezpieczeństwa,
1.4.2.2. Projektowanie bezpiecznego oprogramowania,
1.4.2.3. Wytwarzanie bezpiecznego kodu źródłowego,
1.4.2.4. Testowanie bezpieczeństwa oprogramowania,
1.4.2.5. Wdrażanie i utrzymanie bezpiecznego oprogramowania.

2. Osoby wchodzące w skład zespołu audytowego dla części I, II, III, IV:

2.1. Będą bezstronne i niezależne, w zakresie wykonywanych prac, od:

2.1.1. Ministerstwa Cyfryzacji,

2.1.2. Ministerstwa Spraw Wewnętrznych i Administracji,

2.1.3. NASK PIB,

2.1.4. NASK S.A.,

2.1.5. Comarch S.A.,

2.1.6. Pentacomp S.A.,

2.1.7. PWPW S.A.

2.2. Za bezstronne i niezależne od wyżej wymienionych podmiotów Zamawiający rozumie osoby, które na dzień składania ofert, w czasie trwania postępowania o udzielenie zamówienia publicznego oraz przez cały okres obowiązywania umowy nie będą zatrudnione na umowę o pracę z w/w podmiotami oraz podmiotami powiązanymi (dot. podmiotów wskazanych w pkt. 2.1.3., 2.1.4., 2.1.5) należącymi do tej samej grupy kapitałowej, w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2015 r. poz. 184, 1618 i 1634) oraz nie brały udziału w pracach wytwórczych lub utrzymaniowych systemów utrzymywanych przez Centralny Ośrodek Informatyki, w szczególności:

2.2.1. CEPiK,

2.2.2. CEPiK 2.0,

2.2.3. SRP,

2.2.4. EPUAP,

2.2.5. CEWiUDP,

2.2.6. pl.ID,

2.2.7. ESOM,

2.2.8. PZP,

2.2.9. SPOC,

na dowód czego złożą, przed podpisaniem umowy, stosowne oświadczenia. Przyjmuje się, że pracami wytwórczymi i/lub utrzymaniowymi nie są testy bezpieczeństwa.

Zamawiający zastrzega sobie prawo do weryfikacji i zmian składu osobowego zespołu audytowego na zasadach określonych w Umowie.