**ZAPYTANIE OFERTOWE**

1. **ZAMAWIAJĄCY**

Ministerstwo Spraw Zagranicznych,

Biuro Informatyki i Telekomunikacji

Al. J.Ch. Szucha 23, 00-580 Warszawa

1. **FORMA POSTĘPOWANIA: ZAPYTANIE OFERTOWE**
2. **OPIS PRZEDMIOTU ZAMÓWIENIA**

Testy bezpieczeństwa aplikacji webowych

**Cześć Pierwsza Zamówienia (waga 60%) :**

1. Przeprowadzenie testów bezpieczeństwa, pentesty dla portali oraz aplikacji webowych - 25 roboczodni. Zamawiający zakłada możliwość na etapie planowania testów skrócenia bądź wydłużenia czasu przeznaczonego na testy dla danej aplikacji (np. aplikacja składająca się z pojedynczego formularza, a skomplikowany portal będą wiązały się z inną pracochłonnością i w takiej sytuacji Zamawiający w porozumieniu z Wykonawcą określi mniejszą ilość roboczodni dla małego serwisu, więcej dla dużego, przy zachowaniu maksymalnej łącznej czasochłonności na zlecone aplikacje jako 25 roboczodni. Czas wykorzystany na przygotowanie do testu, ustalanie harmonogramu z Zamawiającym nie pomniejsza roboczodni przeznaczonych na testy. Zamawiający zakłada że maksymalny czas trwania umowy to 12 miesięcy.
2. Przedstawienie raportów z przeprowadzonych testów. Wykonawca w ramach telekonferencji (np. z wykorzystaniem MS Teams) omówi z Zamawiającym wyniki testów i rekomendacje. Raporty i ich omówienie będą również realizowane dla dodatkowych roboczodni, z części drugiej zamówienia.

**Część druga Zamówienia (waga 34%):**

Dodatkowe (opcjonalne) 25 roboczodni do wykorzystania w ciągu 12 miesięcy od podpisania umowy. Dodatkowe roboczodni mogą, ale nie muszą zostać wykorzystane przez Zamawiającego. Zamawiający zapłaci tylko za wykorzystane roboczodni. Dodatkowe roboczodni mogą zostać wykorzystane na ponowne testy aplikacji z podstawowej części umowy (np. w celu weryfikacji usunięcia wykrytych podatności/błędów), lub innych/nowych aplikacji webowych.

Przykładowe strony internetowe MSZ, które mogą być przedmiotem testów :

|  |  |
| --- | --- |
| Twinning | <https://twinning.msz.gov.pl> |
| Traktaty | <https://traktaty.msz.gov.pl> |
| Instytutposki | <https://intytutpolski.pl> |
| Egranty | <https://egranty.msz.gov.pl> |
| Archiwum | <https://archiwum.msz.gov.pl> |
| Poland.pl | <https://poland.pl> |
| Oda | <https://oda.msz.gov.pl> |
| Oda dane | <https://oda-dane.msz.gov.pl> |

**Cel**: identyfikacja podatności, błędów aplikacji i portali webowych MSZ - w celu ich usunięcia, minimalizacji ich negatywnego wpływu na systemy MSZ, bezpieczeństwo przetwarzanych danych.

**Opis uzupełniający:**

* Testy zostaną przeprowadzone zdalnie, w przypadku zapewnienia konieczności bezpośredniego dostępu do aplikacji wykorzystany będzie VPN (OpenVPN)
* Testy zostaną przeprowadzone w oparciu o zasadę grey box gdzie atakujący będzie miał cześć informacji o testowanym systemie.
* Testy nie mogą być przeprowadzone jedynie w trybie automatycznym. Każda wykryta podatność musi być manualnie zweryfikowana. Ponadto Zamawiający oczekuje wykonanie testów manualnych mających na celu wykrycie nieznanych błędów.
* Testy nie zakładają weryfikacji podatności na ataki DoS/DDoS.
* Przeprowadzenie testów nie może wymagać od Zamawiającego zakupu żadnych dodatkowych licencji lub wyposażenia.
* Testy będą wykonywane we wcześniej określonych oknach serwisowych (w razie potrzeby kilkudniowych) przy czym wsparcie Zamawiającego będzie realizowane tylko w dni robocze w godzinach 8-16.
* Testy będą wykonywane z pominięciem WAF. Po zakończeniu testów bez WAF, wykryte podatności Wykonawca na żądanie Zamawiającego zweryfikuje na środowisku z włączonym WAF w celu oceny czy zastosowane środki ochrony uniemożliwiają wykorzystanie wykrytej podatności/luki/błędu.
* Testy z założenia będą prowadzone na środowisku testowym tak aby zniwelować negatywny wpływ na dostępność usług Zamawiającego.
* Testy muszą uwzględniać zarówno próby przełamania zabezpieczeń przez niezalogowanych użytkowników jak i z uwierzytelnionego użytkownika.
* Testy penetracyjne muszą również objąć badanie czy możliwa jest eskalacja dostępu na poziomie innych komponentów powiązanych z aplikacją np. baz danych, systemów plików itd.
* Zakres testów powinien uwzględniać wytyczne w tym zakresie zdefiniowane w metodyce OWASP, z uwzględnieniem OWASP Top 10 i OWASP AVS - w przypadku gdy dany test nie będzie miał zastosowania należy zaznaczyć to w raporcie z testu. W tym w szczególności: badanie mechanizmów autoryzacji, kontroli dostępu, zarządzania sesjami, walidacji danych wejściowych, obsługi błędów, ochrony danych, konfiguracji bezpieczeństwa http, ochrony przed wprowadzaniem złośliwego kodu, ochrony zasobów plikowych, itd.
* Informacje uzyskane w wyniku wykonywanych testów są informacjami do użytku Zamawiającego, a ich wyniki nie mogą być przekazywane osobom/podmiotom trzecim, nie będą publikowane (nawet w zakresie statycznym).

Raporty z przeprowadzonych testów muszą zawierać co najmniej :

* 1. Podsumowanie zidentyfikowanych podatności wraz z rekomendacjami.
  2. Opis założeń przyjętych dla testów, metodyk, technik, ewentualnych wykluczeń.
  3. Informacje o wykonanych testach, adresach IP.
  4. Pozyskane informacje o testowanych systemach.
  5. Zestawienie zidentyfikowanych podatności zawierających identyfikator podatności, nazwę, opis, opis wpływu, narzędzie użyte do wykrycia i wykorzystania podatności, typ podatności prawdopodobieństwo wykorzystania, rekomendacje oraz sposoby wyeliminowania ( tam gdzie zasadne zrzuty ekranu), polecenia umożliwiające odtworzenie podatności.

**Opis środowiska:**

Systemy i aplikacje posadowione są w chmurze.

**Wykorzystana technologia miedzy innymi :** Windows Server, Centos, MSSQL, Mysql, MariaDB, PosgreSQL, Tomcat, Apache, IIS, Wildfly, ASP.NET , PHP, Java, NodeJS, Python, Wordpress, Django, Umbraco.

**Warunki udziału**

O udzielenie zamówienia ubiegać się mogą Oferenci spełniający następujące warunki:

1. posiadają niezbędne doświadczenie oraz uprawnienia do wykonywania prac będących przedmiotem Zamówienia.
2. Zamawiający wymaga, aby Wykonawca przedstawił potwierdzenie wykonania należycie w okresie ostatnich trzech lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie co najmniej 3 usług polegających na wykonaniu usługi testu bezpieczeństwa aplikacji webowej, w ramach których wykonane zostały m. in. testy penetracyjne. Na etapie składania ofert Zamawiającemu wystarczy oświadczenie Oferenta.

**Doświadczenie zespołu**

Zamawiający wymaga, aby Wykonawca dysponował zespołem osób, które będą uczestniczyć w wykonywaniu zamówienia, które posiadają n/w doświadczenie:

Co najmniej dwie osoby ds. bezpieczeństwa IT, które w okresie ostatnich 3 lat przed upływem terminu składania ofert przeprowadziły co najmniej 3 audyty bezpieczeństwa systemów informatycznych, w tym pentestów. Posiadające przynajmniej 3 - letnie doświadczenie w zakresie testowania bezpieczeństwa systemów informatycznych i posiadające certyfikat OSCP (Offensive Security Certified Professional). Na etapie składanie ofert Zamawiającemu wystarczy oświadczenie o posiadaniu wymaganego doświadczenia, certyfikatów bez konieczności przedkładania ich do Oferty. Po wybraniu Oferenta, przed podpisaniem Umowy Zamawiający może zwrócić się do Wykonawcy o doręczenie stosownych dokumentów potwierdzających doświadczenie, certyfikaty zespołu. W trakcie trwania umowy Wykonawca może zgłosić zmiany w zakresie zespołu Wykonawcy. Jednakże nowi pracownicy Wykonawcy muszą spełniać opisane wyżej wymagania, i zmiana będzie wymagała potwierdzenia przez Zamawiającego.

Wykonawca może skierować do realizacji zamówienia większą liczbę osób spełniających wskazane wymagania.

Dodatkowe punkty można zdobyć po przedstawieniu oświadczenia o posiadaniu przez pracowników Wykonawcy biorących udział w realizacji – wykonanie, analiza wyników testów penetracyjnych certyfikatu Security Web Expert (OSWE). Przed podpisaniem umowy należy wskazać, który pracownik posiada certyfikat i przedstawić go do wglądu.

Dodatkowe Punkty ( waga 6% - maksymalnie 6 punktów) .

* + Zamawiający za każdego wskazanego pracownika posiadającego certyfikat (OSWE) przyzna dodatkowe 2 punkty (DP - waga 4%, maksymalnie 4 punkty). Oferta, w której nie zadeklarowano personelu ze wskazanym certyfikatem, otrzyma 0 pkt.
  + Kryterium społeczne (Ks - waga 2%, maksymalnie 2 punkty)

Ks -  liczba punktów uzyskanych w kryterium społecznym „zatrudnienie”.

**W kryterium społeczne „zatrudnienie” Wykonawcy zostaną przyznane punkty za zatrudnienie osób niepełnosprawnych, tj. osób spełniających przesłanki statusu niepełnosprawności, określone ustawą z dnia 27 sierpnia 1997 r. o rehabilitacji zawodowej i społecznej oraz zatrudnieniu osób niepełnosprawnych (Dz. U. z 2021 r., poz. 573 z późn. zm.)  - waga 2 %**

Kryterium będzie oceniane w następujący sposób: co najmniej jedna osoba niepełnosprawna zatrudniana przez Wykonawcę przy wykonywaniu zadań w ramach realizacji przedmiotu zamówienia osoby niepełnosprawnej = 2 pkt.

Zatrudnienie osób niepełnosprawnych na ww. warunkach może dotyczyć zarówno osób nowo zatrudnionych, jak również wcześniej zatrudnionych przez Wykonawców, skierowanych do wykonywania zadań w ramach realizacji przedmiotu zamówienia.

Oferta, w której nie zadeklarowano zatrudnienia osób niepełnosprawnych, otrzyma 0 pkt.

W przypadku złożenia deklaracji dotyczącej zatrudnienia przy wykonywaniu zadań w ramach realizacji przedmiotu zamówienia osoby niepełnosprawnej, Wykonawca będzie zobowiązany przestrzegać tego obowiązku w toku realizacji zamówienia pod rygorem zastosowania przez Zamawiającego kar umownych przewidzianych z tytułu nienależytego wykonania umowy. W przypadku wygaśnięcia lub rozwiązania stosunku pracy przed zakończeniem okresu realizacji zamówienia, Wykonawca zobowiązany będzie do przedłużenia umowy o pracę (w przypadku jej wygaśnięcia) lub zatrudnienie w to miejsce innej osoby niepełnosprawnej na czas realizacji zadań dla Zamawiającego opisanych w umowie.

Jeżeli Wykonawca zadeklaruje zatrudnienie przy wykonywaniu zadań w ramach realizacji przedmiotu zamówienia osoby niepełnosprawnej, będzie zobowiązany do:

1. przedstawienia Zamawiającemu w ciągu trzech dni od dnia podpisania umowy poświadczonego za zgodność z oryginałem przez Wykonawcę zaświadczenia o skierowaniu do realizacji zamówienia osoby niepełnosprawnej,
2. wywiązania się z deklarowanego zatrudniania 1 osoby przez cały okres obowiązywania umowy, pod rygorem zastosowania przez Zamawiającego kary umownej,
3. w przypadku zmiany osoby niepełnosprawnej skierowanej wykonywania zadań w ramach realizacji przedmiotu zamówienia, Wykonawca zobowiązany będzie do przedstawienia Zamawiającemu zaświadczenia o zatrudnieniu nowej osoby, w ciągu trzech dni od dnia zgłoszenia zmiany.

W trakcie realizacji zamówienia Zamawiający uprawniony jest do wykonywania czynności kontrolnych wobec Wykonawcy odnośnie spełniania przez Wykonawcę wymogu zatrudnienia osoby niepełnosprawnej w tym w szczególności:

1. żądania oświadczeń i dokumentów w zakresie potwierdzania spełniania ww. wymogu  
   i dokonywania jego oceny,
2. żądania wyjaśnień w przypadku wątpliwości w zakresie potwierdzenia spełniania ww. wymogu,
3. przeprowadzenia kontroli.

W trakcie realizacji zamówienia na każde wezwanie Zamawiającego w wyznaczonym terminie Wykonawca przedłoży Zamawiającemu poświadczoną za zgodność z oryginałem przez Wykonawcę kopię umowy o pracę osoby skierowanej do realizacji zamówienia. Kopia umowy powinna zostać zanonimizowana w sposób zapewniający ochronę danych osobowych pracownika (tj. w szczególności bez adresu oraz nr PESEL). Imię i nazwisko pracownika nie podlega animizacji. Informacje takie jak: data zawarcia umowy, rodzaj umowy o pracę i wymiar etatu powinny być możliwe do zidentyfikowania.

**Kary umowne**

1. W wypadku niewykonania bądź nienależytego wykonania niniejszej umowy, z przyczyn za które Wykonawca ponosi odpowiedzialność, Wykonawca zapłaci Zamawiającemu kary umowne:
2. za rozwiązanie umowy z przyczyn leżących po stronie Wykonawcy – w wysokości 5 000 (słownie: pięć tysięcy) złotych.
3. 500 (słownie: pięćset) złotych kary za każdy stwierdzony przypadek naruszenia obowiązku zatrudnienia **w kryterium społeczne „zatrudnienie** (w przypadku gdy Wykonawca otrzymał punkty z tego tytułu).
4. Wykonawca wyraża zgodę na potrącenie kary umownej z należnego mu wynagrodzenia. W przypadku gdy takie potrącenie nie będzie możliwe, Wykonawca zobowiązuje się zapłacić karę umowną w terminie 7 dni od otrzymania pisemnego wezwania do zapłaty.
5. Zamawiający zastrzega sobie prawo dochodzenia odszkodowania przewyższającego wysokość zastrzeżonych kar umownych na zasadach ogólnych.
6. **MIEJSCE ORAZ TERMIN SKŁADANIA OFERT**

Oferta powinna być przesłana drogą elektroniczną z opisem w temacie: „*Oferta na testy bezpieczeństwa.*” na adres [**kontakt\_oferta@msz.gov.pl**](mailto:kontakt_oferta@msz.gov.pl) do dnia 20 sierpnia 2021 r.

1. **OPIS KRYTERIÓW OCENY**

Zamawiający będzie rozpatrywał i oceniał oferty na podstawie prezentowanego wzoru:

Punkty dodatkowe PD:

Wykonawca który nie wykaże pracownika przeznaczonego do realizacji Zamówienia posiadającego certyfikat (OSWE) otrzyma 0 punktów dodatkowych (PD1).

Wykonawca który wykaże 1 pracownika przeznaczonego do realizacji Zamówienia posiadającego certyfikat (OSWE) otrzyma 2 punkty dodatkowe (PD1).

Wykonawca który wykaże 2 pracowników przeznaczonego do realizacji Zamówienia posiadających certyfikat (OSWE) otrzyma 4 punkty dodatkowe (PD1).

Wykonawca który nie wykaże w kryterium społecznym „zatrudnienie”, zatrudnienia przynajmniej jednej osoby niepełnosprawnej otrzyma 0 punktów dodatkowych (PD2).

Wykonawca który wykaże w kryterium społecznym „zatrudnienie”, zatrudnienia przynajmniej jednej osoby niepełnosprawnej otrzyma 2 punkty dodatkowe (PD2).

pkt = W + W2 + PD1+PD2

1. **SPOSÓB OBLICZENIA CENY OFERTY**

Podstawą do określenia ceny jest zakres opisany w punkcie **III** dokumentu.

1. **TERMIN WYKONANIA ZAMÓWIENIA**

Do 12 miesięcy od podpisania umowy.

1. **OPIS SPOSOBU PRZYGOTOWANIA OFERTY**
2. Oferta musi mieć formę pliku w formacie pdf w języku polskim.
3. Oferta musi zawierać:
4. imię, nazwisko, firmę i dokładny adres wykonawcy, datę sporządzenia oferty oraz imię i nazwisko osoby uprawnionej do reprezentowania Wykonawcy;
5. cenę za którą wykonawca zobowiązuje się do wykonania pracy z części 1 ( netto i brutto);
6. cenę za którą wykonawca zobowiązuje się do wykonania pracy z części 2 ( netto i brutto);
7. Oświadczenie o doświadczeniu i kompetencjach zespołu opisane w części III niezbędne do realizacji Usługi.
8. Oświadczenie o liczbie pracowników posiadających certyfikat OSWE, skierowanych do realizacji Zamówienia.
9. Oświadczenie o zatrudnieniu osoby niepełnosprawnej, zgodnie z opisem w części III.
10. **UDZIELENIE ZAMÓWIENIA**

Zamawiający udzieli zamówienia Wykonawcy, którego oferta będzie najwyżej punktowana na podstawie obliczeń wg wzoru w pkt. V.

1. **DODATKOWE INFORMACJE**

Termin ważności oferty winien obejmować 90 dni.

Dodatkowych informacji udzielają pracownicy MSZ drogą elektroniczną pod adresem email: [**kontakt\_oferta@msz.gov.pl**](mailto:kontakt_oferta@msz.gov.pl)

**Ministerstwo Spraw Zagranicznych zastrzega sobie prawo do negocjacji warunków zawartych w ofertach oraz do nie wybrania żadnej z wpływających ofert.**