Rozeznanie rynku na usługę audytu bezpieczeństwa teleinformatycznego w biurze PFRON

1. Nazwa i adres zamawiającego:
Państwowy Fundusz Rehabilitacji Osób Niepełnosprawnych
00-828 Warszawa
Al. Jana Pawła II 13

Postępowanie prowadzone będzie na podstawie art. 4 pkt 8 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych — (Dz. U. z 2015 r. poz. 2164 z późn. zm.), zgodnie z którym ustawy nie stosuje się do zamówień, których wartość nie przekracza wyrażonej w złotych równowartości kwoty 30 tyś. euro. Postępowanie prowadzone zgodnie z zasadą konkurencyjności.

1. Opis Przedmiotu Zamówienia

Przedmiotem Zamówienia jest przeprowadzenie testów bezpieczeństwa systemów informatycznych Zamawiającego. Wymaga się aby przedmiot Zamówienia został zrealizowany przez odpowiednie testy aplikacji i oprogramowania systemowego, wywiady z pracownikami, weryfikacje konfiguracji systemów informatycznych, wizje lokalne oraz analizę procedur i dostarczonej dokumentacji. W ramach realizacji Przedmiotu Zamówienia Wykonawca dokona weryfikacji procedur dotyczących bezpieczeństwa teleinformatycznego. Zakres audytu jest zawarty w Istotnych Postanowieniach Umowy.

Prace będą nadzorowane przez pracowników Zamawiającego w dni robocze w godzinach 9:00 - 16:00. Pracę będą odbywać się Biurze Funduszu oraz w zewnętrznych lokalizacjach hostingodawców.

### Systemy i warstwy poddane testowaniu i audytowi

* systemy CMS/aplikacje www,
* sieciowe urządzenia brzegowe,
* systemy firewall,
* usługi VPN,
* serwery aplikacji, serwery bazodanowe, systemy operacyjne.
* warstwy dostępowe do usług bankowości elektronicznej,
* usługi udostępniane dla użytkowników systemów wspierających realizowanie statutowych zadań PFRON.

Dostęp do dokumentacji systemów Zamawiającego zostanie udzielony podczas wizji lokalnej przeprowadzone w siedzibie Zamawiającego. Celem umówienia terminu wizji prosimy o wysłanie zgłoszenia na adres osoby podanej do kontaktów w ramach realizacji niniejszego zapytania, czyli na adres: jrydlakowski@pfron.org.pl

Dla każdego z testowanych systemów Zamawiający oczekuje przeprowadzenia testów zmierzających do:

* podniesienia poziomu uprawnień uwierzytelnionego lub anonimowego użytkownika,
* przejęcia danych uwierzytelniania lub sesji kont innych użytkowników,
* uzyskania nieautoryzowanego dostępu do danych lub nieuprawnionej zmiany danych,
* przejęcia kontroli na sposobem działania usług,
* zablokowania działania usług,
* wykazania braku możliwości redundantnego działania zdublowanych podsystemów,
* uruchomienia własnych usług nie ujętych w dokumentacji systemów,
* wykrycia wszelkich podatności mających wpływ na dostępność, poufność oraz integralność danych.

Wymaga się by wymienione powyżej testy zostały wykonane kluczowe testy przewidziane
w podręczniku OWASP Testing Guide v4. Testy te muszą przewidywać próby dokonania ataków za pośrednictwem sieci WAN(Internet), sieci LAN/WLAN Zamawiającego, usługi Active Directory Zamawiającego. Testy powinny obejmować swoim zakresem wszelkie podatności ujawnione
w publicznie dostępnych bazach(m.in. www.exploit-db.com, www.rapid7.com, wuldb.com)

Wymaga się przeprowadzenia audytu warstwy zabezpieczeń systemów i danych w Biurze Funduszu. W szczególności audytowi poddane zostaną:

* warstwa fizycznych zabezpieczeń dostępu do danych,
* warstwa wymiany danych z systemami zewnętrznymi,
* warstwa uprawnień określonych użytkowników oraz grup użytkowników do określonych zbiorów danych.

Audyt warstw, o których mowa powyżej, powinien być przeprowadzony przy założeniu, że pożądanym stanem rzeczy jest: zachowanie zasady minimalnego koniecznego dostępu do danych oraz zasad zabezpieczeń danych przed wyciekiem oraz próbami uzyskania nieautoryzowanego dostępu. Oczekuje się, że Wykonawca przeprowadzi co najmniej trzy próby uzyskania nieuprawnionego, fizycznego dostępu do infrastruktury teleinformatycznej Zamawiającego
w obszarze stacji roboczych posiadających dostęp do kluczowych systemów Zamawiającego, infrastruktury sieciowej oraz serwerowej.

### 2.2. Wymagane produkty

Produktem dla każdego testowanego i audytowanego obszaru, systemu lub warstwy powinny być raporty zawierające

* streszczenie dla kierownictwa,
* szczegółowy zakres czynności wykonanych podczas przeprowadzania testów bezpieczeństwa i audytu,
* rekomendacje usprawnień natury organizacyjnej, fizycznej lub technicznej pozwalających na wyeliminowanie lub ograniczenie wykrytych zagrożeń. Rekomendacje mogą dzielić się na rekomendację tymczasowe pozwalające na doraźne obejście problemu oraz rekomendacje docelowe stanowiące opis stanu oczekiwanego, którego osiągnięci pozwala na całkowite wyeliminowanie podatności.

W przypadku stwierdzenia podatności krytycznej Wykonawca powiadomi o nich niezwłocznie Zamawiającego. Zakłada się, ze w wyniku analizy ryzyka przeprowadzonej w ramach audytu warstwy fizycznej zostaną wydzielone co najmniej dwa poziomy/strefy bezpieczeństwa do których będą miały zastosowanie odmienne rekomendowane poziomy stosowania środków bezpieczeństwa.

## 3. Termin realizacji Zamówienia

Oczekuje się, ze zamówienie zostanie zrealizowane w ciągu 60 dni kalendarzowych od daty podpisania umowy.

## 4. Warunki udziału w postępowaniu i warunki realizacji Zamawiania

Oczekuje się, że Zamówienie zostanie zrealizowane przez co najmniej 2 osoby posiadające doświadczenie w realizacji w ciągu ostatnich 3 lat co najmniej 3 audytach systemów teleinformatycznych, w trakcie których realizowane były testy penetracyjne w zakresie opisanym w punkcie 2. Dla potwierdzenia spełnienia tego Warunku zamawiający wymaga potwierdzenia wydanego przez podmiot na, rzecz którego usługa ta była świadczona. Każda z wyżej wymienionych osób musi posiadać co najmniej dwa z certyfikaty z zakresu bezpieczeństwa spośród poniżej wymienionych:

* certyfikat CISM: Certified Information Security Manager (http://www.isaca.org) lub równoważny,
* certyfikat CISA: Certified Information System Auditor (http://www.isaca.org) lub równoważny,
* certyfikat CISSP: Certified Information System Security Professional (http://www.isc2.org) lub równoważny,
* certyfikat CEH: Certified Ethical Hacker (http://www.eccouncil.org/) lub równoważny.

### 4.1. Termin realizacji usługi

1. Wykonawca zobowiązuje się zakończyć realizację Etapów umowy w terminie nieprzekraczającym 60 (sześćdziesięciu) dni od daty jej podpisania.
2. Etap 1 zostanie zakończony w terminie 10 (dziesięciu) dni od daty podpisania umowy.
3. Pod pojęciem zakończenia Etapu Umowy rozumie się podpisanie przez Zamawiającego Protokołu Odbioru Etapu bez zastrzeżeń.
4. Pod pojęciem zakończenia Umowy rozumie się zakończenie wszystkich etapów umowy.
5. W trakcie procedury Odbioru Produktów Realizacji Etapów 1, 2 i 3 Zamawiający dokona weryfikacji, czy przedmiot Odbioru spełnia wymagania Zamawijacego.
6. W przypadku stwierdzenia przez Zamawiającego rozbieżności pomiędzy przekazanym
do weryfikacji produktami, a wymaganiami określonymi w umowie Kierownik Projektu Zamawiającego sporządzi i przekaże Kierownikowi Projektu Wykonawcy uwagi z opisem rozbieżności uniemożliwiającymi Odbiór.
7. Brak przedstawienia przez Zamawiającego uwag do przedmiotu Odbioru nie oznacza Odbioru
i akceptacji przedmiotu Odbioru przez Zamawiającego.
8. W przypadku stwierdzenia przez Zamawiającego niezgodności Produktu podlegającej Odbiorowi z Umową, Wykonawca poprawi przedmiot Odbioru w terminie wskazanym przez Zamawiającego. W takim przypadku procedurę Odbioru opisaną powyżej powtarza się aż do czasu dokonania przez Zamawiającego Odbioru bez zastrzeżeń albo skorzystania przez Zamawiającego z prawa do wypowiedzenia Umowy zgodnie z przepisami prawa lub Umową.
9. Za datę odbioru Produktu Realizacji Etapu 1, 2 i 3 uznaje się odpowiednią datę wynikającą
z zapisów § 3 umowy, pod warunkiem, że Produkt Realizacji Etapu zostanie zaakceptowany przez Zamawiającego przy pierwszym Odbiorze. W przypadku stwierdzenia nieprawidłowości w zgłoszonym do Odbioru produkcie, terminem odbioru produktu będzie podpisanie stosownego Protokołu Odbioru Etapu bez zastrzeżeń przez Zamawiającego.

## 5. Kryteria oceny oferty

Cena – 100%

## 6. Osoba uprawniona do porozumiewania się z potencjalnymi wykonawcami

Janusz Rydlakowski, adres e-mailowy: jrydlakowski@pfron.org.pl

## 7. Miejsce, termin i sposób złożenia oferty

Ofertę zawierającą cenę za realizację całości zamówienia oraz dokumenty poświadczające spełnianie wymagań udziału w postępowaniu należy przesłać na adres: jrydlakowski@pfron.org.pl do dnia 28.09.2017 r. roku do godz. 10:00. Podana w ofercie cena musi być podana z dokładnością do jednego grosza, cena podana w ofercie ma uwzględniać wszystkie koszty związane z wykonywaniem umowy.

## 8. Składanie ofert

Składane oferty stanowią informacje dotyczące oszacowania przedmiotu zamówienia. W toku badania ofert Zamawiający może żądać od Wykonawcy wyjaśnień dotyczących treści złożonych ofert oraz ich uzupełnienia.

## 9. Unieważnienie postępowania

Zamawiający zastrzega sobie możliwość unieważnienia postępowania na każdym etapie bez podania przyczyny. W przypadku unieważnienia postępowania, Zamawiający nie ponosi kosztów postępowania.