Zapytanie ofertowe na usługę audytu bezpieczeństwa teleinformatycznego

Kod CPV: 79212200-5 Usługi audytu wewnętrznego

1. Nazwa i adres zamawiającego:

Państwowy Fundusz Rehabilitacji Osób Niepełnosprawnych
00-828 Warszawa
Al. Jana Pawła II 13
Tel. (22) 50-55-663

Postępowanie prowadzone 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 .

2. Opis Przedmiotu Zamówienia

Przedmiotem Zamówienia jest przeprowadzenie testów bezpieczeństwa systemów informatycznych Zamawiającego. Wymaga się aby przedmiot Zamówienia został zrealizowany przez wywiady z pracownikami, weryfikacje konfiguracji systemów informatycznych, wizje lokalne, weryfikacje konfiguracji wybranych stacji roboczych oraz analizę procedur i dostarczonej dokumentacji. Testy będą wykonywane na środowiskach testowych, w razie uzasadnionej potrzeby Zamawiającego dopuszcza się przeprowadzenie testów na środowiskach produkcyjnych. Prace będą nadzorowane przez pracowników Zamawiającego
w dni robocze w godzinach 9:00 - 15:00. Pracę będą odbywać się Biurze Funduszu,
w zewnętrznych lokalizacjach hostingodawców, oraz w 16 Oddziałach Funduszu.
W ramach realizacji Przedmiotu Zamówienia Wykonawca przeprowadzi testy bezpieczeństwa systemów teleinformatycznych oraz dokona weryfikacji procedur dotyczących bezpieczeństwa teleinformatycznego, w tym również w obszarze ochrony danych osobowych pod kątem realizacji Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. o ochronie danych osobowych (RODO). Audyt i testy muszą uwzględnić wszystkie systemy teleinformatyczne Zamawiającego, wliczając te, w których są przetwarzane dane osobowe oraz wszystkie procedury Zamawiającego dotyczące przetwarzania danych osobowych.

2.1 Systemy i warstwy poddane testowaniu i audytowi

- systemy CMS/aplikacje www,
- sieciowe urządzenia brzegowe,
- routery ekranujące i bramy,
- systemy firewall,
- serwery Proxy,
- usługi VPN,
- systemy antywirusowe,
- systemy tworzenia i odtwarzania kopii zapasowych,
- serwery aplikacji,
- systemy monitorowania dostępności,
- serwery DNS,
- serwery i usługi poczty elektronicznej,
- systemy operacyjne,
- systemy baz danych,

- system usług katalogowych(Active Directory),
- warstwy dostępowe do usług bankowości elektronicznej,
- system obiegu dokumentów,
- usługi dostępu do danych dedykowane dla urządzeń mobilnych oraz konfiguracje urządzeń mobilnych,
- 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:mlukasiak@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 oraz Oddziałach Funduszu. W szczególności audytowi poddane zostaną:

- warstwa procedur organizacyjnych mający na celu utrzymanie określonych poziomów bezpieczeństwa i dostępności systemów teleinformatycznych,
- 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.

2.3. Produkty Zamówienia

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,
- listę wykrytych zagrożeń i nieprawidłowości w tym niezgodności z RODO,
- ocenę wykrytych zagrożeń i niezgodności z RODO według skali uzgodnionej z Zamawiającym,
- rekomendacje usprawnień natury organizacyjnej, fizycznej lub technicznej pozwalających na wyeliminowanie lub ograniczenie wykrytych zagrożeń i niezgodności z RODO. 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.

Wykonawca wytworzy i dostarczy projekt dokumentu Polityki Bezpieczeństwa Informacji zapewniający spełnianie wymagań i rekomendacji wynikających z przeprowadzonych testów i audytu, a także wymagań zawartych w Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. o ochronie danych osobowych (RODO), Rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych którego integralną oraz Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Częścią projektu dokumentu Polityki będą procedury postępowania oraz zbiory wytycznych, zapewniające spełnianie wymagań RODO na które składać się będą między innymi dokumenty określające swoim zakresem zagadnienia dotyczące:

- ciągłości działania,
- użytkowania stacji roboczych,
- dostępu do systemów,
- dostępu do pomieszczeń i stacji roboczych,
- używania urządzeń mobilnych,
- korzystania z nośników danych.

Do projektów planów, regulaminów i procedur powinny zostać dołączone projekty szablony wniosków i innych dokumentów niezbędnych do ich operacyjnej realizacji.

3. Termin realizacji Zamówienia

Oczekuje się, ze zamówienie zostanie zrealizowane w ciągu 70 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.

Każdy z produktów umowy najpóźniej na 20 dni kalendarzowych przed datą końca umowy musi być dostarczony do Zamawiającego w stanie kompletnym, uwzględniającym uwagi i wytyczne pracowników Zamawiającego zgłaszane w trakcie trwania umowy. Zamawiający w ciągu 5 dni kalendarzowych zaopiniuje dostarczony projekt, a Wykonawca niezwłocznie wprowadzi do niego zmiany wymagane przez Zamawiającego. Procedura ta będzie powtarzana aż do czynności odbioru produktów przez Zamawiającego, co w przypadku przekroczenia granicznego terminu realizacji umowy nie zwalnia Wykonawcy z odpowiedzialności wynikającej z zapisów o karach umownych.

5. Kryteria oceny ofert

Cena – 100%

6. Kary umowne

Wykonawca zapłaci karę o wysokości 2% wartości zamówienia za każdy dzień zwłoki w realizacji Przedmiotu Zamówienia lub zadania opisanego w punkcie 5.3. Jeśli suma naliczonych kar przekroczy wartość 35% wartości zamówienia, Zamawiający będzie uprawniony do natychmiastowego rozwiązania Umowy. Zamawiający zastrzega sobie możliwość dochodzenia odszkodowania na zasadach ogólnych.

7. Osoba uprawniona do porozumiewania się z potencjalnymi wykonawcami

Mirosław Łukasiak, adres e-mailowy: mlukasiak@pfron.org.pl

8. 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: mlukasiak@pfron.org.pl do dnia 22.02.2017 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.

9. Tryb oceny ofert

W toku badania i oceny ofert Zamawiający może żądać od Wykonawcy wyjaśnień dotyczących treści złożonych ofert oraz ich uzupełnienia.

10. Unieważnienie postępowania

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

Dyrektor Departamentu
ds. Teleinformatyki
Damian Dynda