SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

1. Przedmiotem zamówienia jest przeprowadzanie testów bezpieczeństwa aplikacji internetowych oraz sieci lokalnej.

1.1. Zamawiający będzie zlecał wykonanie testów bezpieczeństwa zgodnie z bieżącym zapotrzebowaniem do maksymalnej wartości umowy.

1.2. Pracochłonność świadczenia usług będzie odbywać się zgodnie z pkt 5 SOPZ.

2. Termin realizacji przedmiotu zamówienia

2.1. Planowany okres wykonywania przedmiotu zamówienia wynosi 36 (trzydzieści sześć) miesięcy licząc od dnia zawarcia umowy, chyba, że wcześniej zostanie wyczerpana kwota przeznaczona przez Zamawiającego na sfinansowanie zamówienia.

2.2. Zamawiający przewiduje możliwość skorzystania z prawa opcji, polegającego na przedłużeniu umowy maksymalnie o kolejne 12 miesięcy (słownie: dwanaście miesięcy) w stosunku do umowy pierwotnej.

2.3. Zamawiający zastrzega sobie możliwość wcześniejszego uruchomienia prawa opcji, przed upływem 36 miesięcy od dnia zawarcia umowy.

3. W ramach realizacji przedmiotu zamówienia mieści się:

3.1. Przedmiotem zamówienia jest świadczenie na rzecz Zamawiającego przez Wykonawcę usług polegających na przeprowadzaniu testów bezpieczeństwa aplikacji internetowych oraz sieci lokalnej tj.:

- 3.1.1. przeprowadzaniu audytów kodu aplikacji internetowych,
- 3.1.2. przeprowadzaniu testów penetracyjnych aplikacji internetowych,
- 3.1.3. przeprowadzaniu testów penetracyjnych sieci lokalnej,
- 3.1.4. sporządzaniu raportów z wykonanych usług,
- 3.1.5. przeprowadzaniu retestów.

3.2. Celem zlecanych prac jest identyfikacja możliwie jak największej liczby podatności stanowiących lub mogących stanowić zagrożenie dla bezpieczeństwa przetwarzanych i przechowywanych informacji oraz danych, a także usług biznesowych realizowanych przez systemy teleinformatyczne Centrum.

3.3. W ramach zlecanych prac Wykonawca przeprowadzi następujące działania:

- 3.3.1. audyty kodu aplikacji internetowych,
- 3.3.2. testy penetracyjne aplikacji internetowych,
- 3.3.3. testy penetracyjne sieci lokalnej,
- 3.3.4. opracowania wyników wykonanych prac w formie raportu.
- 3.3.5. Zlecenia mogą obejmować również przeprowadzenie retestów w celu weryfikacji poprawności wdrożenia rekomendacji sformułowanych przez Wykonawcę w ramach wcześniejszych zleceń. Produktem retestów będzie również raport z realizacji zlecenia

3.4. Testom bezpieczeństwa podlegać będą systemy głównie oparte o technologię PHP, PostgreSQL, Typescript. Dodatkowo mogą wystąpić: JavaScript (jquery), JSP/Java,

ASP/ASP.NET, Ruby on Rails, relacyjne bazy danych. Nie można jednak wykluczyć innych technologii.

3.5. Przykładowe aplikacje Zamawiającego planowane do objęcia testami (nie jest to katalog zamknięty):
   3.5.1. LSI 1.0
   3.5.2. LSI 2.0
   3.5.3. AAAA

3.6. Testy bezpieczeństwa i audyty kodu obejmować będą co najmniej następujące elementy:
   3.6.1. Audyt kodu aplikacji internetowej
      a. Określenie powierzchni ataku
      b. Określenie obszarów podwyższonego ryzyka
      c. Określenie zgodności ze standardami organizacji
      d. Identyfikacja klas podatności
      e. Weryfikacja wdrożonych zaleceń w przypadku retestów
   3.6.2. Test penetracyjny aplikacji internetowej (testy automatyczne i manualne)
      a. Testy penetracyjne serwera WWW/ aplikacyjnego
      b. Testy penetracyjne aplikacji (komponenty dostępne publicznie)
      c. Testy penetracyjne aplikacji po uwierzytelnieniu
      d. Testy penetracyjne interfejsów bazy danych
      e. Testy penetracyjne bazy danych z poziomu użytkownika
   3.6.3. Test penetracyjny sieci lokalnej (testy automatyczne i manualne)
      a. Testy penetracyjne punktu styku z Internetem
      b. Kontrolowana próba obejścia zabezpieczeń
      c. Testy uwierzytelniania sieciowego
      d. Testy szczelności VLAN-ów i poufności przesyłanych informacji
      e. Testy penetracyjne systemów operacyjnych

4. Ogólne warunki realizacji zamówienia

4.1. Realizacja przedmiotu zamówienia odbywać się będzie co do zasady zdalnie, niemniej jednak w uzasadnionych przypadkach Zamawiający zakłada realizację zleconych prac w siedzibie Zamawiającego. Realizacja zleconych zadań będzie wymagać obecności Wykonawcy w siedzibie Zamawiającego, jeżeli zdalna realizacja będzie niemożliwa lub może negatywnie wpływać na jakość wykonania zlecenia jednostkowego.

4.2. Realizując zlecone prace Wykonawca będzie stosował „dobre praktyki" z zakresu bezpieczeństwa systemów informatycznych m.in. takie jak:
   4.2.1. Open Web Application Security Project (OWASP),
   4.2.2. Open Source Security Testing Methodology Manual (OSSTMM),
   4.2.3. Weryfikacja błędów znajdujących się na liście OWASP Top 10, aktualnej na dzień przyjęcia zlecenia.

4.3. Testy bezpieczeństwa aplikacji będą przeprowadzane na udostępnionym przez Zamawiającego środowisku nieprodukcyjnym.

4.4. Dostęp do środowiska nieprodukcyjnego będzie udzielony za pośrednictwem połączenia VPN.

4.5. Realizując zlecenie Wykonawca zweryfikuje całość udostępnionego kodu nie stosując próbkowania, chyba że Zamawiający określi inaczej w zleceniu jednostkowym.

4.6. Testy bezpieczeństwa składać się będą z następujących po sobie etapów:

4.6.1. rozpoznanie badanego systemu informatycznego oraz jego elementów,

4.6.2. analiza podatności na zagrożenia na podstawie uzyskanych informacji,

4.6.3. wykonanie kontrolowanych ataków i zweryfikowanie podatności, ataki typu DDoS (unieruchomienia usługi) powinny być wykonane w uzgodnionym z Zamawiającym terminie. Wykonawca przed wykonaniem ataku typu DDoS ustali możliwość wykonania takich testów oraz termin ich wykonania z osobami reprezentującymi Zamawiającego, wymienionymi w Umowie.

4.6.4. sporządzenie raportu ze zlecenia z listą wykrytych luk, dowodów istnienia luki (poc) wraz z oceną realnego zagrożenia oraz rekomendacją sposobu usunięcia podatności.

4.7. Wykonawca zobowiązany jest wskazać w raporcie z realizacji zlecenia wszystkie miejsca występowania podatności powszechnie znanych na dzień wykonania zlecenia jednostkowego, jeżeli takie podatności występują w weryfikowanej aplikacji lub sieci lokalnej. Za powszechnie znane podatności uznaje się co najmniej te wymienione na liście OWASP Top 10 oraz umieszczone w słowniku CVE (Common Vulnerabilities and Exposures).

4.8. Wszystkie testy bezpieczeństwa będą przeprowadzane za pomocą narzędzi Wykonawcy.

4.9. Testy bezpieczeństwa sieci Zamawiającego.

4.9.1. Testom zostaną poddane:

a. sieciowe urządzenia brzegowe (routery, przełączniki),
b. firewalle,
c. urządzenia obsługujące połączenia VPN,
d. systemy wykrywania włamań (IDS),
e. systemy przeciwdziałania włamaniom (IPS),
f. serwery aplikacji,
g. serwery DNS,
h. serwery poczty elektronicznej,
i. systemy operacyjne,
j. systemy równoważenia obciążenia.

4.9.2. Powyższe testy powinny umożliwić wykrycie:

a. możliwości uzyskania nieautoryzowanego dostępu do sieci wewnętrznej Centrum,
b. możliwości wykorzystania sieci Centrum do przeprowadzania ataków na inne sieci,
c. możliwości omijania wdrożonych systemów zabezpieczeń,
d. obecności znanych błędów i luk bezpieczeństwa w stosowanych urządzeniach sieciowych i oprogramowaniu,
e. podatności sieci na propagację złośliwego oprogramowania,
f. zagrożeń dla dostępności, poufności oraz integralności przetwarzanych danych i informacji,
g. możliwości przejęcia nieautoryzowanej kontroli nad usługami lub serwerami,

h. możliwości nieautoryzowanego zwiększenia uprawnień przez użytkowników usług,
i. możliwości manipulacji usługami świadczonymi przez serwery,
j. możliwości destabilizacji i zablokowania pracy serwerów.

4.10. Testy bezpieczeństwa aplikacji internetowych oraz audyt kodu

4.10.1. Każde zlecenie dotyczące testów bezpieczeństwa aplikacji internetowych wiąże się z przeprowadzeniem audytu kodu aplikacji, chyba że Zamawiający określi inaczej w zleceniu jednostkowym. Jedynie testy penetracyjne sieci nie będą zawierały audytu kodu.

4.10.2. Kod źródłowy lub dostęp do niego Wykonawca otrzyma od Zamawiającego, Wykonawca testować będzie na swojej infrastrukturze oraz za pomocą narzędzi które posiada. Testy penetracyjne Wykonawca realizuje zdalnie, na testowej instancji aplikacji, udostępnionej przez Zamawiającego.

4.10.3. Testy bezpieczeństwa aplikacji oraz audyt kodu powinny umożliwiać wykrycie:

a. luk związanych z zastosowaną architekturą aplikacji,
b. luk wynikających z zastosowanych wzorców projektowych,
c. luk związanych z zastosowanymi technologiami na poziomie warstwy prezentacji danych,
d. luk związanych z zastosowanymi technologiami na poziomie warstwy aplikacji,
e. luk związanych z zastosowanymi serwerami WWW lub ich niewłaściwej konfiguracji,
f. luk związanych z zastosowanym środowiskiem aplikacyjnym lub jego niewłaściwą konfiguracją,
g. luk związanych z niewłaściwą walidacją danych wejściowych,
h. luk związanych z zaimplementowanymi mechanizmami uwierzytelniania i autoryzacji.

4.10.4. Testy aplikacji internetowych mają być przeprowadzane zarówno z perspektywy użytkownika zalogowanego jak i niezalogowanego. Jeżeli to będzie konieczne Zamawiający dostarczy Wykonawcy parametry dostępu do konta istniejącego w aplikacji użytkownika.

5. Zasady zlecania i realizacji prac,

5.1. Wykonawca będzie realizował zamówienie na podstawie zaakceptowanych zleceń jednostkowych. Zlecenie jednostkowe może zostać zaakceptowane przez osoby wskazane w Umowie.

5.2. Zamawiający przygotowuje zlecenie jednostkowe dokładając wszelkiej staranności, aby możliwie dokładnie opisać oczekiwania stawiane wobec Wykonawcy co do rezultatów zlecanych prac. Zlecenie opracowane przez Zamawiającego będzie zawierać co najmniej:

5.2.1. opis testowanej aplikacji
5.2.2. adres testowanej aplikacji
5.2.3. zakres testów bezpieczeństwa / retestów ze szczegółowymi wymaganiami
5.2.4. opis technologii wykorzystywanych przez testowaną aplikację

5.2.5. inne informacje specyficzne dla przedmiotu zlecenia

5.2.6. wersję testowanej aplikacji

5.2.7. sumę kontrolną paczki z kodem źródłowym aplikacji lub dostęp do repozytorium kodu aplikacji (jeżeli będzie przekazywany kod źródłowy aplikacji)

5.3. Opracowane przez Zamawiającego zlecenie przekazywane będzie za pośrednictwem poczty elektronicznej do Wykonawcy, celem dokonania przez Wykonawcę oceny pracochłonności zakresu prac opisanych w zleceniu oraz szacowanego terminu zakończenia prac objętych zleceniem.

5.4. Wykonawca po otrzymaniu opisu zlecenia dokona rzetelnej oceny pracochłonności wykonania zlecenia i przedstawi ją Zamawiającemu w terminie nie dłuższym niż 3 dni robocze od dnia otrzymania opisu zlecenia.

5.5. W przypadku, gdy Wykonawca uzna, że opis zadań przedstawiony w zleceniu jest niewystarczający do przeprowadzenia rzetelnej oceny pracochłonności oraz wykonania zlecenia, ma prawo jednokrotnie zgłosić do Zamawiającego prośbę doprecyzowania opisu zlecenia, przy czym Wykonawca wskaże w punktach fragmenty opisu zlecenia, które budzą jego wątpliwości. Termin na przekazanie prośby o doprecyzowanie opisu zlecenia jednostkowego jest taki sam jak dla przekazania wyników oceny pracochłonności.

5.6. Zamawiający zobowiązany jest przesłać wyjaśnienia doprecyzowujące treść zlecenia w terminie do 5 dni roboczych od dnia otrzymania takiej prośby od Wykonawcy.

5.7. Wskazany przez Wykonawcę termin wykonania zlecenia może ulec wydłużeniu w wyniku zaistnienia nieprzewidzianych problemów z realizacją zleconych prac, niemniej jednak zmiana terminu nie może wpływać na ustaloną pracochłonność zlecenia jednostkowego. Zgłaszając prośbę o zmianę terminu wykonania zlecenia Wykonawca zobowiązany jest podać obiektywne przyczyny takiej zmiany. Ustalenie nowego terminu następuje za zgodą Zamawiającego, potwierdzoną za pośrednictwem poczty elektronicznej na adresy Zamawiającego wskazane w Umowie.

5.8. Wykonawca może wnioskować o zmianę terminu wykonania zlecenia nie później niż 3 dni robocze przed upływem obowiązującego terminu wykonania zlecenia. Wniosek o zmianę terminu wykonania zlecenia jednostkowego Wykonawca przesyła na adresy poczty elektronicznej Zamawiającego, wskazane w Umowie.

5.9. Po przekazaniu Zamawiającemu wyników oceny pracochłonności, Zamawiający może uznać oszacowanie Wykonawcy za akceptowalne i zlecić realizację zlecenia, może podjąć negocjacje z Wykonawcą lub zrezygnować z realizacji danego zlecenia. Decyzja Zamawiającego przekazywana jest Wykonawcy za pośrednictwem poczty elektronicznej na adres Wykonawcy wskazany w Umowie.

5.9.1. W przypadku pozytywnej decyzji dotyczącej oceny pracochłonności Zamawiający przekazuje zlecenie jednostkowe do realizacji, a Wykonawca rozpoczyna jego realizację. Ocena pracochłonności, która uzyska akceptację Zamawiającego stanowi podstawę do ustalenia kwoty rozliczenia Zamawiającego z Wykonawcą.

5.9.2. W przypadku negatywnej decyzji dotyczącej oceny pracochłonności, Zamawiający może żądać od Wykonawcy szczegółowego uzasadnienia przeprowadzonej oceny pracochłonności, w którym przedstawione zostaną co najmniej następujące elementy:
   a. liczba osób potrzebnych do realizacji zlecenia z podziałem na role pełnione w danym zleceniu,
   b. liczba roboczogodzin potrzebnych na realizację zleceń, w podziale na poszczególne osoby biorące udział w realizacji zleceń,
   c. szczegółowy podział zakresu prac na elementy niezbędne, bez których realizacja zleceń nie może się odbyć i elementy opcjonalne, które nie mają lub mają niewielki wpływ na końcowy produkt,
   d. pracochłonność przypisaną do poszczególnych elementów niezbędnych i opcjonalnych.

5.10. Wykonawca na prośbę Zamawiającego zobowiązany jest przedstawić uzasadnienie do oszacowanej pracochłonności w terminie 3 dni roboczych od otrzymania takiego żądania. Zamawiający przesyła żądanie wyjaśnień na adres poczty elektronicznej Wykonawcy wskazany w Umowie. Wykonawca może w ramach wyjaśnień zaproponować mniejszą wartość pracochłonności zlecenia.

5.11. Zamawiający po weryfikacji przedstawionej oceny pracochłonności może dokonać modyfikacji zlecenia. Modyfikacja zlecenia może spowodować zamianę zakresu zlecanych prac oraz wzrost lub zmniejszenie liczby roboczogodzin potrzebnych na realizację zlecenia. Jeżeli w wyniku negocjacji nie dojdzie do porozumienia stron, Zamawiający może zrezygnować ze zlecenia jednostkowego.

5.12. Realizacja zlecenia. Po akceptacji przez Zamawiającego oceny pracochłonności Wykonawcy, zaakceptowane zlecenie przekazywane jest Wykonawcy do realizacji na warunkach określonych w zatwierdzonym formularzu zlecenia jednostkowego. Informacja o przekazaniu zlecenia do realizacji przekazywana jest na adres mailowy Wykonawcy, określony w Umowie. Po otrzymaniu informacji ze strony Zamawiającego o akceptacji oceny pracochłonności zlecenia jednostkowego, Wykonawca przystępuje do realizacji zlecenia w ciągu maksymalnie 5 dni roboczych.

5.13. Wykonawca zgłasza do odbioru wykonane zlecenie, przekazując informację o zakończeniu prac wraz z raportem, stanowiącym podsumowanie wykonanego zlecenia. Informacja przekazywana jest na adres poczty elektronicznej Zamawiającego wskazany w Umowie. Raport musi być zabezpieczony hasłem, chroniącym przed dostępem osób niepowołanych. Hasło do dokumentu przekazywane jest innym kanałem komunikacji np. telefonicznie, pisemnie na adres jednej z osób reprezentujących Zamawiającego, zgodnie z Umową. Sposób przekazania hasła Wykonawca każdorazowo ustali z osobami reprezentującymi Zamawiającego zgodnie z Umową.

5.14. **Odbiór zlecenia:**

5.14.1. Po zgłoszeniu przez Wykonawcę zrealizowanego zlecenia do odbioru, Zamawiający w ciągu 5 dni roboczych zweryfikuje zgodność wykonania zlecenia z warunkami określonymi w zleceniu jednostkowym przekazanym do realizacji.

5.14.2. Raport musi być zgodny z wymogami określonymi w punkcie 4 OPZ.

5.14.3. Zamawiający uprawniony jest do wniesienia zastrzeżeń do przedstawionego raportu, o którym mowa w pkt 4.2, zgłoszonego do odbioru.

5.14.4. W przypadku przedstawienia przez Zamawiającego uwag do raportu, Wykonawca w terminie 3 dni roboczych od ich otrzymania przedstawi Zamawiającemu poprawiony raport w wersji elektronicznej (e-mail) zgodnie z procedurą określoną w pkt 3.13 lub niezwłocznie uzasadni drogą elektroniczną niemożliwość lub niecelowość ich uwzględnienia.

5.14.5. Zamawiający w terminie 3 dni roboczych od ponownego otrzymania raportu, dokona jego akceptacji lub zgłosi uwagi na adres poczty elektronicznej Wykonawcy, wskazany w Umowie.

5.14.6. Zamawiającemu przysługuje prawo do przedstawienia kolejnych uwag do poprawionego raportu. Po każdych uwagach przekazanych Wykonawcy, Wykonawca ma do 3 dni roboczych na wprowadzenie poprawek.

5.14.7. Odbiór zlecenia potwierdzany jest każdorazowo protokołem odbioru zlecenia, do którego załączona jest ostateczna wersja raportu ze zrealizowanych prac podpisanym elektronicznie przez obie strony Umowy zgodnie z reprezentacją określoną zgodnie z Umową.

5.15. Przyjęcie zlecenia do realizacji przez Wykonawcę oznacza akceptację warunków zlecenia oraz że zakres zlecanych prac jest dla niego zrozumiały i nie wymaga doprecyzowania.

5.16. W przypadku niemożliwości realizacji zlecenia z przyczyn obiektywnych, Wykonawca ma obowiązek pisemnego uzasadnienia oraz przedstawienia Zamawiającemu alternatywnego rozwiązania, którego rezultat będzie identyczny lub zbliżony do oczekiwanego przez Zamawiającego. Zamawiający może, lecz nie musi zaakceptować alternatywnego rozwiązania.

6. Wymagania w zakresie jakości

6.1. Zamawiający oczekuje od Wykonawcy szczególnej staranności w zakresie wykonania przekazanych zleceń z zastosowaniem „dobrych praktyk" i standardów związanych z realizacją prac w zakresie testów bezpieczeństwa aplikacji webowych.

6.2. Każdorazowo po wykonaniu zlecenia, Wykonawca przedstawi raport zawierający co najmniej:

6.2.1. Listę zidentyfikowanych podatności, wraz z ich szczegółowym opisem zawierającym sposób działania, wpływ na inne elementy, potencjalne konsekwencje występowania. Co do zasady tam gdzie to możliwe każda podatność powinna być oznaczone kodem ze słownika CVE (Common Vulnerabilities and Exposures).

6.2.2. Treść raportu powinna zawierać jednoznaczne stwierdzenia odnośnie znalezionych podatności / braków zabezpieczeń i wnioski z przeprowadzonych prac. Treść raportu musi odnosić się do faktycznie występujących w systemie podatności, dokładny „proof of concept" umożliwiający Zamawiającemu samodzielne potwierdzenie zgodności treści raportu ze stanem faktycznym.

6.2.3. Szczegółowe propozycje, rekomendacje dotyczące naprawy zidentyfikowanych podatności.

6.2.4. Syntetyczną ocenę bezpieczeństwa badanego systemu, przygotowaną na podstawie przeprowadzonych testów oraz audytu kodu.

6.2.5. Użyte narzędzia/oprogramowanie

6.2.6. Raport powinien być zabezpieczony przed możliwością przejęcia i odczytania zawartości przez podmioty nie biorące udziału w realizacji przedmiotu umowy.

6.3. Raport przekazywany Zamawiającemu nie może wyłącznie być zrzutem danych automatycznie wygenerowanych z narzędzi wspierających przeprowadzania pentestów. Informacje zawarte w raporcie muszą być efektem interpretacji wyników testów bezpieczeństwa, dokonanej przez eksperta z dziedziny bezpieczeństwa systemów informatycznych.

6.4. Każda z osób uczestniczących w realizacji zamówienia zobligowana będzie do złożenia oświadczenia o zachowaniu poufności informacji, zgodnie ze wzorem stanowiącym Załącznik nr 1 do wzoru Umowy o zachowaniu poufności informacji.