Szczegółowy Opis Przedmiotu Zamówienia   
*(Audyt bezpieczeństwa PEF)*

# Kontekst zamówienia

Minister Rozwoju zarządza Platformą Elektronicznego Fakturowania (PEF).

Platforma PEF służy do obsługi i dokumentowania procesu realizacji przez zamawiających i wykonawców dostaw publicznych w fazie po udzieleniu zamówienia, w tym wymiany faktur elektronicznych zgodnych z Normą Europejską dla elektronicznej faktury w zamówieniach publicznych. Udostępnione na platformie PEF e-usługi są zgodne ze standardami stowarzyszenia OpenPeppol.

Funkcjonalność platformy PeF pozwala na realizowanie następujących e-usług publicznych:

* 1. usługa zamawiania dostawy,
  2. usługa awizowania dostawy,
  3. usługa potwierdzania odbioru,
  4. usługa fakturowania,
  5. usługa wystawiania faktury korygującej,
  6. usługa wystawiania noty księgowej,
  7. usługa generowania raportów i zestawień dla władz publicznych.

# Opis przedmiotu zamówienia

**Przedmiotem zamówienia jest przeprowadzenie audytu bezpieczeństwa dwóch systemów informatycznych platformy PEF udostępnianych przez Brokerów PEF**.

Celem głównym audytów jest określenie poziomu bezpieczeństwa platformy, wskazanie punktów obniżających ten poziom oraz, w przypadku wykrycia takich punktów, zaproponowanie rozwiązań, które doprowadzą środowisko do akceptowalnego przez Zamawiającego poziomu bezpieczeństwa.

W celu przeprowadzenia audytu **Wykonawca powinien współpracować zarówno z Brokerami PEF jak i z Zamawiającym**.

Przedmiotowy audyt powinien objąć badanie bezpieczeństwa obu systemów informatycznych platformy PEF dla każdego z dwóch Brokerów. Proces audytowy powinien zakończyć się sporządzeniem raportu końcowego wraz z zaleceniami z audytu w terminie do 60 dni od podpisania umowy.

Zamawiający wystawi zlecenie zawierające datę rozpoczęcia i zakończenia prac. Wykonawca przedstawi szczegółowe plany przeprowadzenia audytu w odniesieniu do przedstawionych wymagań i standardów. Przedstawiony plan audytu będzie podlegał zatwierdzeniu przez Zamawiającego. Przedstawienie Zamawiającemu szczegółowego planu audytu przez Wykonawcę nastąpi w terminie 14 dni od wystawienia zlecenia. Plan będzie podlegał zatwierdzeniu przez Zamawiającego w ciągu 14 dni od daty ich otrzymania.

Kod CPV: 72810000-1 Usługi audytu komputerowego

## Audyt bezpieczeństwa

Audytem zostanie objęte nie więcej niż 15 serwerów fizycznych/wirtualnych dla każdego z dwóch systemów informatycznych. Zakres audytów obejmuje dwa portale internetowe. Dla każdego z systemów audytem objęte zostanie nie więcej niż 20 formularzy HTML oraz nie więcej niż 2 zapory sieciowe. Dla każdego z systemów audytem powinno być objęte nie więcej niż 10 przełączników, nie więcej niż 2 load-balancery oraz nie więcej niż 2 routery (trasowniki). Dla każdego z systemów zakres audytu obejmuje nie więcej niż 5 dedykowanych systemów bezpieczeństwa – typy minimum IDS/IPS, UTM, WAF. Każdy z systemów posiada nie więcej niż 5 hostów w puli adresacji zewnętrznej.

W ramach audytu Wykonawca jest zobowiązany do:

1. **przeprowadzenia** **badań i testów** bezpieczeństwa systemu informatycznego platformy PEF każdego z dwóch Brokerów,
2. **opracowania oceny eksperckiej** (w tym zgodności z normami, kryteriami, wymaganiami, itp.) dla każdego z badanych i testowanych obszarów bezpieczeństwa, odrębnie dla każdego z Brokerów,
3. **przedstawienia** (na podstawie wyników oceny) **wiążącego stanowiska** dotyczącego potrzeb wprowadzenia zmian w systemie informatycznym i świadczonych e-usługach platformy PEF dla każdego z Brokerów,
4. **przedstawienia rekomendacji zmian** (jeżeli będą wskazane potrzeby zmian) w zakresie bezpieczeństwa systemu informatycznego platformy PEF każdego z dwóch Brokerów.

Celem szczegółowym audytu jest przeprowadzenie badań i analiz umożliwiających wskazanie zagrożeń wynikających z:

1. cech zaprojektowanej i wykorzystywanej architektury systemu i środowiska informatycznego platformy PEF oraz współpracy z innymi systemami informatycznymi (w tym siecią PEPPOL, systemami ERP zamawiających i dostawców w procedurach realizacji zamówień publicznych),
2. zastosowanych technologii i standardów zabezpieczeń,
3. jakości oprogramowania systemu informatycznego PEF i jego implementacji,
4. metod i protokołów wymiany danych oraz architektury interfejsów międzysystemowych i międzysieciowych,
5. poprawności konfiguracji komponentów rozwiązania, takich jak, systemy obsługi transmisji, systemy zaporowe i inne systemy usługowe i pomocnicze

**Wymagania metodyczne**

**Standardy testowania bezpieczeństwa**

Zamawiający wymaga w ramach realizacji zadania wykonywania testów penetracyjnych wykorzystania standardów testowania bezpieczeństwa lub równoważnych (za równoważne Zamawiający uzna standardy opisujące przebieg procesu testowania bezpieczeństwa systemów IT oraz obszary systemowe, które muszą podlegać weryfikacji):

1. OWASP (Open Web Application Security Project) ASVS 2019 ,
2. Open Source Security Testing Methodology Manual (OSSTMM) ,
3. Penetration Testing Execution Standard (PTES).

Wymagania dotyczące poziomu realizacji testów:

Audyt na poziomie 1. (https://owasp-aasvs.readthedocs.io/en/latest/level1.html)

Listy OWASP (Open Web Application Security Project) Top 10 - 2017 w zakresie:

1. A1:2017 – Injection
2. A2:2017 – Broken Authentication
3. A3:2017 – Sensitive Data Exposure
4. A4:2017 – XML External Entities (XXE)
5. A5:2017 – Broken Access Control
6. A6:2017 – Security Misconfiguration
7. A7:2017 – Cross-Site Scripting (XSS)
8. A8:2017 – Insecure Deserialization
9. A9:2017 – Using Components with Known Vulnerabilities
10. A10:2017 – Insufficient Logging&Monitoring

**Opracowanie potrzeb w zakresie poziomu pokrycia testami**

Zamawiający wymaga wykorzystania następujących poziomów pokrycia systemu testami bezpieczeństwa.

1. **Poziom 0** ma stanowić elastyczny poziom początkowy w hierarchii weryfikacyjnej. Wskazuje on, że aplikacja została poddana określonego rodzaju weryfikacji. Na poziomie 0 na potrzeby realizacji automatycznego, pobieżnego skanowania wszystkich posiadanych aplikacji zewnętrznych należy korzystać z wybranego narzędzia komercyjnego, podczas gdy inne mogą zdefiniować wymagania Poziomu 0 na podstawie danych odnośnie ostatnich przypadków naruszenia bezpieczeństwa. W przeciwieństwie do pozostałych poziomów, Poziom 0 nie jest niezbędny dla realizacji innych poziomów. Wykonywana na tym poziomie weryfikacja ręczna nie ma na celu zapewnienie kompletnej weryfikacji bezpieczeństwa, tylko upewnienie się, że wyniki testów automatycznych są poprawne i nie stanowią fałszywych wskazań.
2. **Poziom 1** obejmuje zagrożenia, które weryfikujący może zidentyfikować przy minimalnym lub umiarkowanym wysiłku. Poziomu 1 nie należy postrzegać jako poziomu szczegółowej kontroli lub weryfikacji aplikacji, lecz jako poziom szybkiej kontroli. Poziom 1 jest zwykle odpowiedni dla aplikacji, dla których wymagany jest pewien poziom zaufania co do poprawnego użycia mechanizmów bezpieczeństwa, bądź też w celu szybkiego pokrycia całego zbioru aplikacji instytucji oraz ułatwienia opracowania planu bardziej szczegółowych kontroli, które będą realizowane w późniejszym terminie. Typowymi zagrożeniami dla bezpieczeństwa aplikacji będą w tym przypadku napastnicy stosujący proste techniki umożliwiające łatwe wykrycie i zbadanie zagrożeń. Stanowią oni przeciwieństwo napastników zdeterminowanych, które wkładają większy wysiłek ukierunkowany na daną aplikację.
3. **Poziom 2** zapewnia, że mechanizmy bezpieczeństwa funkcjonują w sposób prawidłowy i są użyte w aplikacji wszędzie tam, gdzie powinny być użyte by egzekwować polityki specyficzne dla aplikacji. Poziom 2 stanowi standard branżowy, któremu podlega większość wrażliwych aplikacji stosowanych przez organizacje. Poziom 2 jest zwykle odpowiedni dla aplikacji, które obsługują istotne transakcje biznesowe pomiędzy firmami. Typowymi zagrożeniami dla bezpieczeństwa będą w tym przypadku napastnicy liczący na okazję oraz zdeterminowani napastnicy (wykwalifikowani i zmotywowani, skupieni na określonych celach, używający m.in. specjalnie przystosowanych narzędzi skanujących).
4. **Poziom 3** jest jedynym poziomem, który wymaga również kontroli projektu aplikacji. Ponadto obowiązują w tym przypadku następujące wymagania:

* wszelkie istotne mechanizmy bezpieczeństwa, których oddziaływanie ma charakter przekrojowy (obejmując kontrolę danych wejściowych i proces uwierzytelniania) powinny zostać wdrożone w sposób scentralizowany,
* mechanizmy bezpieczeństwa dokonujące kontroli bezpieczeństwa powinny podejmować decyzje w oparciu o listę dozwolonych wyników (model pozytywny),
* kontroli danych wejściowych nie należy stosować jako jedynego mechanizmu obronnego względem praktyk tworzenia skryptów i wstrzykiwania kodów. Mechanizm ten powinien być stosowany jako dodatkowa linia obrony, uzupełniając parametryzację i kodowanie danych wejściowych. Weryfikacja na Poziomie 3 jest zwykle odpowiednia dla krytycznych aplikacji, od których zależy życie i bezpieczeństwo, krytyczna infrastruktura lub zadania związane z obronnością, bądź też które mogą ułatwić spowodowanie znacznych strat dla organizacji. Poziom 3 może być również odpowiedni dla aplikacji służących do przetwarzania wrażliwych aktywów. Zagrożeniami dla bezpieczeństwa w tym przypadku będą zdeterminowani napastnicy (wykwalifikowani i zmotywowani napastnicy skupieni na określonych celach, używający m.in. specjalnie przystosowanych narzędzi skanujących).

**Wykorzystanie baz danych o znanych podatnościach i słabościach bezpieczeństwa**

Zamawiający wymaga wykorzystania znanych baz danych o podatnościach i słabościach bezpieczeństwa systemów informatycznych, w trakcie prac prowadzonych przez Wykonawcę w ramach przedmiotu zamówienia, np.:

* 1. SANS Top 20 Critical Security Controls,
  2. Common Vulnerabilities and Exposures,
  3. WASC (Web Application Security Consortium) Threat Classification,

lub równoważnych (za równoważne Zamawiający uzna takie bazy danych, które stanowią aktualne źródło informacji o lukach bezpieczeństwa, są publikowane lub utrzymywane przez uznane powszechnie organizacje, działające na rzecz zapewnienia bezpieczeństwa systemów informatycznych).

**Wykorzystanie list kontrolnych**

Zamawiający wymaga aby w ramach realizacji audytu bezpieczeństwa do oceny wykorzystywane były listy kontrolne udostępniane przez uznane organizacje pracujące na rzecz bezpieczeństwa systemów IT, tj.:

* 1. National Security Agency (NSA) – minimalny zakres list kontrolnych do wykorzystania:
     + Top 10 Mitigation Strategies (March 2018)
     + Steps to Secure Web Browsing (May 2018)
     + Identity Theft Threat and Mitigations (September 2018)
  2. Center for Internet Security (CIS)
     + https://www.cisecurity.org/controls/

lub równoważnych (w szczególności takich, które stanowią aktualne źródło informacji o bezpiecznej konfiguracji, są publikowane lub utrzymywane przez uznane powszechnie organizacje, działające na rzecz zapewnienia bezpieczeństwa systemów informatycznych).

**Uwzględnienie typowych dla testowania penetracyjnego zadań**

Zamawiający wymaga, aby w ramach realizacji testów penetracyjnych obejmowały one typowe, wymienione niżej zadania (będące elementem każdej metodyki testów penetracyjnych):

* 1. Target Scoping (Zakres Docelowy – ustalenie charakteru i zasięgu testów),
  2. Information Gathering (Gromadzenie Informacji – pasywne zbieranie informacji na temat obiektu testów),
  3. Target Discovery (Odkrywanie Celu – pół-pasywne zbieranie informacji, poznanie celów, identyfikacja podsieci, rodzaju architektury, systemów operacyjnych),
  4. Enumerating Target (Wyliczanie Elementów – aktywne zbieranie informacji, enumeracja usług, portów, wykrywanie systemów bezpieczeństwa IDS/UPS, FV),
  5. Vulnerability Mapping (Mapowanie Podatności – poszukiwanie podatności w elementach znalezionych w poprzednich fazach),
  6. Target Exploitation (Docelowa Eksploatacja – stworzenie wektora inicjalizującego atak, który ma na celu ominąć zabezpieczenia w celu naruszenia poufności, integralności oraz dostępności danych osobowych, przejęcia systemów, odcięcia systemu od sieci zewnętrznej),
  7. Privilage Escalation (Eskalacja Uprawnień – zwiększenie uprawnień w przełamanym systemie i przeniesienie kontroli na kolejne usługi lub systemy),
  8. Maintaining Access (Utrzymanie Dostępu – utrzymanie dostępu do skompromitowanego systemu, instalacja tylnych furtek, rootkit-ów,
  9. Documentation & Reporting (Dokumentacja i Raportowanie – raport powinien zawierać informacje o znalezionych podatnościach oraz zauważonych problemach).

**Obszary bezpieczeństwa**

Zamawiający wymaga aby zakres weryfikacji bezpieczeństwa adresował ryzyka występujące w poniższej przedstawionych obszarach:

* 1. Uwierzytelnianie
  2. Zarządzanie sesją
  3. Kontrola dostępu
  4. Walidacja wejścia
  5. Kryptografia
  6. Obsługa błędów i logowanie
  7. Ochrona danych
  8. Bezpieczeństwo komunikacji
  9. Wyszukiwanie złośliwego kodu
  10. Logika biznesowa
  11. Weryfikacja zasobów i plików

**Wykładnia wymagań środków technicznych** zalecanych do realizacji usług przez Brokerów PEF, która będzie podstawą sprawdzenia przez wykonawcę audytu bezpieczeństwa systemu informatycznego PEF:

1. Środowisko systemu będzie utrzymywane przez Brokera Platformy PEF w serwerowni gwarantującej odpowiedni poziom bezpieczeństwa zgodnie wymogami normy ISO 27001.
2. Serwerownia, w której utrzymywany będzie system Platformy PEF, będzie posiadała odpowiednie zabezpieczenia przed nieautoryzowanym dostępem.
3. Zostaną wykorzystane mechanizmy uwierzytelniania (np.: SSO [ang. *Single Sign-On*]) i kontroli dostępu dla użytkowników systemu (np.: oparte o protokół SAML [ang. *Security Assertion Markup Language*]).
4. Platforma PEF będzie zapewniała bezpieczne mechanizmy komunikacji pomiędzy działającymi w ramach jej systemu teleinformatycznego komponentami wymiany danych, urządzeniami końcowymi oraz zewnętrznymi platformami/systemami. (Transmisja może być niezaszyfrowana tylko w przypadkach komunikacji pomiędzy wewnętrznymi komponentami każdego z modułów systemu).
5. System platformy PEF będzie zabezpieczał transmisję danych pomiędzy urządzeniem końcowym, a serwerami aplikacyjnymi za pomocą protokołu SSL (ang. Secure Socket Layer).
6. System platformy PEF będzie nadawał każdemu użytkownikowi indywidualny i unikalny identyfikator.
7. System platformy PEF będzie miał zaimplementowany model uprawnień użytkowników zgodny ze specyfikacją RBAC (ang. Role-based Access Control) NIST (ang. National Institute of Standards and Technology).
8. System platformy PEF będzie zapewniał mechanizmy kontroli uprawnień oparte   
   na rolach i umożliwi kontrolę poziomu dostępu każdego użytkownika w zakresie dostępu do przetwarzanych danych jak i korzystania z funkcjonalności systemu.
9. System platformy PEF będzie zawierał mechanizmy zapobiegające możliwości wprowadzenia i uruchomienia złośliwego kodu.
10. System platformy PEF będzie odporny na znane ataki, np.: „Cross-site scripting (XSS)” i „Cross-site request forgery (XSRF)”, "SQL Injection", “Distributed Denial of Service(DDoS)”.
11. System platformy PEF będzie wykorzystywał mechanizmy synchronizacji czasu w oparciu o protokół NTP (ang. Network Time Protocol).
12. System platformy PEF będzie umożliwiał definiowanie reguł określających wymaganą siłę stosowanych haseł dla różnych grup użytkowników. System będzie umożliwiał bezpieczne odzyskiwanie haseł użytkowników.
13. System platformy PEF będzie przechowywał i przesyłał hasła użytkowników oraz inne chronione dane wyłącznie w postaci zabezpieczonej z wykorzystaniem bezpiecznych metod szyfrowania.
14. System platformy PEF będzie automatycznie zamykał sesje dostępu użytkownika   
    po upływie określonego w konfiguracji systemu czasu od przerwania pracy z systemem (np. zamknięcia przeglądarki lub braku aktywności użytkownika).
15. System platformy PEF będzie umożliwiał wykonywanie i zarządzanie archiwizacją oraz kopiami bezpieczeństwa systemu i związanych z nim danymi (wg harmonogramu zgodnego z polityką bezpieczeństwa lub na żądanie w trakcie pracy systemu).
16. System platformy PEF będzie umożliwiał odtworzenie systemu i danych na podstawie wykonanych kopii zapasowych.
17. System platformy PEF będzie posiadał zabezpieczenie przed niekontrolowanym obciążeniem wywołanym wskutek nadmiernego ruchu.
18. System platformy PEF będzie posiadał mechanizmy logowania operacji, logowania i wylogowania użytkownika, modyfikacji danych oraz rejestracji wykonanych najważniejszych akcji w systemie wraz z rejestracją czasu operacji, identyfikacji użytkownika oraz wyniku operacji. System będzie zapewniał mechanizmy uniemożliwiające edycję, usuwanie i archiwizację plików zawierających logi zdarzeń systemowych oraz chroniące przed możliwością ich przepełnienia. System będzie zapewniał mechanizmy przechowywania plików zawierających rejestr działań użytkowników i będzie przechowywał te dane zgodnie z wymaganiami nałożonymi przepisami prawa.
19. System platformy PEF będzie zapewniał mechanizmy powiadamiania i raportowania o wykrytych incydentach związanych z naruszeniem bezpieczeństwa i integralności podstawowych elementów systemu.
20. Rozwiązania techniczne Systemu PEF powinny korzystać ze sprzętowego modułu bezpieczeństwa HSM (Hardware Security Module). Urządzenia HSM muszą być certyfikowane na poziomie bezpieczeństwa minimum FIPS 140-2 Level 2 lub CC EAL 4+.

Zakres weryfikacji normy ISO/IEC 27001 zostanie ustalony z Zamawiającym na etapie realizacji audytu. Jeżeli będzie wymagane przeprowadzenie audytu stacjonarnego, jego zakres zostanie ustalony z Zamawiającym na etapie realizacji audytu. W takim przypadku Wykonawca uzyska dostęp do infrastruktury w zakresie ustalonym z Zamawiającym. Serwerownie znajdują się w okolicach Lublina oraz Katowic. Zamawiający nie dopuszcza możliwości włączenia maszyny Wykonawcy do sieci w audytowanej infrastrukturze.

Zakres usług realizowanych w ramach **Audytu bezpieczeństwa systemu informatycznego platformy PEF** - obejmuje przeprowadzenie audytu, ze szczególnym uwzględnieniem poniższych aspektów:

1. **Audytu spójności i zgodności.**

Audyt obejmuje kontrolę spójności oraz zgodności z przepisami prawa wewnętrznych regulacji dotyczących bezpieczeństwa, weryfikację poziomu przestrzegania tych regulacji i kwalifikacji personelu bezpieczeństwa systemu informatycznego platformy PEF.

Zakres audytu:

Weryfikacja dokumentacji bezpieczeństwa systemu PEF (w tym polityka bezpieczeństwa wraz z dokumentami szczegółowymi i procedurami bezpieczeństwa, system uprawnień i polityka dostępu) pod kątem aktualności, kompletności oraz poprawności merytorycznej, kwalifikacji personelu bezpieczeństwa SI platformy PEF, a także zgodności z obowiązującym prawem i standardami (w szczególności kontrola zgodności z wymaganiami określonymi w Rozporządzeniu Rady Ministrów z 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).

1. **Audytu bezpieczeństwa przetwarzania danych.**

Audyt **bezpieczeństwa przetwarzania danych** będzie realizowany zgodnie z wymaganiami wymienionymi w rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności oraz zgodnie z normami: ISO 27001 „Technika informatyczna. Techniki Bezpieczeństwa. systemu zarządzania bezpieczeństwem informacji. Wymagania” i ISO 27002 „Technika informatyczna – Praktyczne zasady zarządzania bezpieczeństwem informacji”.

Na platformie PEF nie będą przetwarzane dane niejawne w rozumieniu ustawy o ochronie informacji niejawnych z 5 sierpnia 2010 (Dz. U. z 2010 r. nr 182, poz. 1228).

Platforma PEF zgodnie z rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych będzie zapewniała **wysoki** poziom bezpieczeństwa tych danych (w rozumieniu ww. rozporządzenia).

W obszarze zapewnienia bezpieczeństwa przetwarzanych danych oraz ochrony danych, platforma PEF powinna zagwarantować:

1. poufność – zabezpieczenie danych przed ich udostępnieniem nieuprawnionemu odbiorcy,
2. integralność – zabezpieczenie danych przed modyfikacją lub zniekształceniem przez nieuprawnionych użytkowników,
3. rozliczalność – określenie i weryfikowanie odpowiedzialności za wykorzystanie systemu,
4. autentyczność – weryfikacje tożsamości podmiotów i prawdziwości zasobów,
5. niezawodność – gwarancja oczekiwanego zachowania systemu.

**Audyt obejmuje sprawdzenie aktualnego stanu przetwarzania danych osobowych** zarówno pod kątem zagadnień technicznych, organizacyjnych oraz prawnych ze szczególnym uwzględnieniem wymagań opisanych w ustawie o ochronie danych osobowych.

Zakres audytu:

* 1. Przegląd i analiza dokumentacji, w tym analiza dokumentacji polityk bezpieczeństwa i procedur, pod kątem zgodności z wymaganiami (w zakresie jak wyżej) Rozporządzenia, ze szczególnym uwzględnieniem zagadnień IT.
  2. Weryfikacja zgodności systemów z wymaganiami Rozporządzenia (w zakresie jak wyżej), ze szczególnym uwzględnieniem zagadnień IT.
  3. Weryfikacja kwalifikacji personelu odpowiedzialnego za bezpieczeństwo systemu IT platformy PEF oraz przestrzegania procedur bezpieczeństwa przez pracowników (realizujących postanowienia polityk bezpieczeństwa).

1. **Audytu bezpieczeństwa systemów teleinformatycznych.**

Celem audytu jest wykrycie faktycznych oraz potencjalnych luk i błędów w oprogramowaniu, konfiguracji urządzeń informatycznych, portalach i aplikacjach webowych, które mogą być wykorzystane do naruszenia bezpieczeństwa przetwarzanych informacji, a także bezpieczeństwa Zamawiającego lub użytkowników systemów.

Zakres audytu:

* 1. analiza architektury sieciowej,
     + weryfikacja sieci LAN na strefy sieciowe (w tym wykorzystanie urządzeń typu firewall oraz VLAN),
     + określenie usług działających w wybranych podsieciach (do 10 podsieci – nie więcej niż 15 hostów dla jednego systemu),
     + poszukiwanie podatności w wybranych podsieciach (do 10 podsieci – nie więcej niż 15 hostów dla jednego systemu),
     + weryfikacja mechanizmów ochronnych w warstwie 2 i 3 modelu OSI,
     + weryfikacja dostępu do Internetu z LAN,
     + szczegółowa analiza komunikacji sieciowej,
     + weryfikacja zasad utrzymania sieci,
* analiza wersji oprogramowania pod kątem znanych podatności (firmware),
* analiza konfiguracji dostępu do urządzenia,
* przegląd konfiguracji dot. użytkowników korzystających z urządzenia, praw dostępu, list dostępów, testy słabych haseł,
* analiza konfiguracji i reguł VPN,
* analiza wykorzystanych mechanizmów kryptograficznych,
* analiza zasad filtracji ruchu sieciowego,
* analiza pod kątem obecności niepożądanych usług,
* analiza mechanizmów logowania zdarzeń
  1. analiza brzegu sieci
* weryfikacja topologii/architektury sieci,
* testy szczelności systemów klasy firewall (w tym działania funkcji IPS obsługującej w czasie rzeczywistym zagrożenia typu nadużycie protokołu, próby tunelowania, oprogramowania typu exploit, kontrola aplikacji, ataki ogólnego typu bez predefiniowanych sygnatur, ruchu generowanego przez szkodliwe oprogramowanie, podatności serwera i klienta wraz z możliwością definiowania własnych sygnatur, regularności aktualizacji firewall w celu przeciwdziałania nowym zagrożeniom, itp.)
* ogólna analiza komunikacji sieciowej z poziomu sieci Internet,
* skanowanie portów różnymi technikami, w celu wykrycia potencjalnych luk bezpieczeństwa w udostępnianych usługach,
* wykrywanie usług sieciowych udostępnionych w sieci Internet,
* próba detekcji wersji oraz typu oprogramowania systemowego zainstalowanego na urządzeniach dostępnych z sieci Internet,
* testowanie odporności usług wystawionych do sieci Internet na ataki „Denial of Service” co najmniej 2 metodami zaproponowanymi przez Wykonawcę,
* testowanie odporności usług wystawionych do sieci Internet, za pomocą narzędzi eksploatujących typowe luki bezpieczeństwa.
  1. analiza bezpieczeństwa konfiguracji systemów informatycznych (urządzeń i aplikacji)
     + analiza zgodności konfiguracji i sposobu funkcjonowania urządzeń:
       - weryfikacja udostępnionych usług sieciowych,
       - weryfikacja zbędnych usług wraz ze wskazaniem ich podatności,
       - weryfikacja zaimplementowanych systemów aktualizacji,
       - weryfikacja zaimplementowanych systemów logowania zdarzeń,
       - weryfikacja mechanizmów administracji zdalnej,
       - weryfikacja przypisania użytkowników do właściwych grup,
       - weryfikacja uprawnień zgodnie z pryncypium jak najmniejszych uprawnień (ang. „least privilige”),
       - przeprowadzenie prób obejścia uprawnień i uzyskania nieautoryzowanego dostępu do informacji,
       - weryfikacja sposobu udostępniania baz danych na poziomie sieciowym,
       - analiza implementacji podstawowych zasad hardeningowych bazy danych (np. wyłączenie nieużywanych usług, wyłączenie nieużywanych metod dostępu, konfiguracja uprawnień do obiektów, logowanie zdarzeń, składowanie logów, monitorowanie dostępu do obiektów, monitorowanie instrukcji języka SQL),
       - analiza architektury baz danych (np. wykorzystanie mechanizmów autoryzacji oraz uwierzytelniania, segmentacja uprawnień, wykorzystywanie widoków, wykorzystywanie procedur składowych, przechowywanie oraz dostęp do danych wrażliwych, przechowywanie oraz dostęp do danych audytowych, szyfrowanie danych),
       - analiza komunikacji z klientami bazodanowymi (mechanizmy kryptograficzne, transfery danych).
     + analiza podatności aplikacji
       - wytypowanie wrażliwych punktów w aplikacji,
       - inspekcja mechanizmów uwierzytelniania / autoryzacji,
       - zabezpieczenia interfejsu użytkownika za pomocą captcha oraz za pomocą zweryfikowanego certyfikatu,
       - weryfikacja implementacji mechanizmów ochronnych dla serwerów aplikacyjnych,
       - weryfikacja obsługi błędów,
       - analiza poziomu bezpieczeństwa oferowanego przez aplikacje,
       - analiza kodu aplikacji, w tym:
         * zastosowanie dobrych praktyk zalecanych przez producenta(-ów) technologii, w których aplikacja została wytworzona
         * zastosowanie wytycznych właściwych dla zastosowanej technologii
         * konsekwencja w stosowaniu standardów, konwencji, itp.
         * stosowanie wzorców projektowych
         * stosowanie właściwych podziałów na warstwy i komponenty z zachowaniem zasad rozłącznego i osobliwego zastosowania (Separation of Concerns)
         * analiza użytych funkcji lub komponentów pod kątem elementów przestarzałych („deprecated”) lub elementów posiadających znane luki bezpieczeństwa lub podatności,
         * dokumentowanie autorskiego kodu aplikacji, w sposób umożliwiający automatyczne wygenerowanie dokumentacji API
  2. przeprowadzenie testów penetracyjnych i symulowanych ataków (wg najnowszych wytycznych OWASP wymienionych na liście TOP10 aktualnej na dzień realizacji audytu) obejmujących:
     + testy bezpieczeństwa aplikacji pod kątem:
       - ataków semantycznych na adres URL,
       - ataków związanych z ładowaniem plików,
       - ataków typu Cross-Site Scripting,
       - ataków typu Cross-Site Request Forgery,
       - ataków typu MITM (Man in the Middle),
       - ataków typu Cross Site Tracing,
       - ataków typu Session Hijacking / Session Fixation,
       - ataków typu Forced Browsing,
       - ujawnienia kodu/ścieżki dostępu (Path Disclousure),
       - ujawnienia parametrów ograniczających (Parameter Delimiter)
       - podrabiania zarządzania formularza,
       - sfałszowania żądania http,
       - ujawnienia danych przechowywanych w bazie,
       - trawersowania katalogów (Path Traversal),
       - ujawniania kodu źródłowego,
       - przepełnienia bufora lub stosu,
       - wstrzykiwania kodu wykonywalnego innych języków programowania (np. SQL Injection / JSON Injection),
       - niepożądanego przekierowania,
     + badanie enumeracji i wykorzystania znanych podatności w celu uzyskania nieautoryzowanego dostępu,
     + badanie możliwości podszywania się pod użytkowników i uzyskania nieautoryzowanego dostępu do systemu
     + badanie możliwości podszywania się pod użytkowników uprzywilejowanych i uzyskanie dostępu do systemu
     + badanie możliwości blokowania/umożliwienia dostępu do systemu wszystkim lub wybranym jej użytkownikom,
     + badanie możliwości modyfikacji/usunięcia danych z systemu.

1. **Audytu funkcjonowania systemów bezpieczeństwa.**

Audyt obejmuje analizę i ocenę funkcjonowania następujących systemów bezpieczeństwa:

* 1. System antywirusowy.
  2. System antyspamowy.
  3. System DLP (Data Leak Prevention/Data Loss Prevention).
  4. System Firewall.
  5. System backupowy wraz z testem odtworzenia systemu PEF z backupu (Zamawiający nie wymaga odtwarzania systemu na zasobach Wykonawcy), ocena lokalizacji baz danych zawierających kopie bezpieczeństwa (bezpieczeństwo ośrodka, ośrodek zapasowy).
  6. System zasilania awaryjnego.

Zakres audytu:

* 1. Kompleksowa analiza skuteczności działania.
  2. Analizę procedur utrzymaniowych i monitorowania systemów bezpieczeństwa.
  3. Weryfikacja poprawności konfiguracji systemów bezpieczeństwa.
  4. Weryfikacja i/lub opracowanie wskaźników efektywności.

**W wyniku przeprowadzonego audytu Wykonawca dostarczy raport zawierający:**

1. Opis przeprowadzonych działań (w tym weryfikacji dokumentacji i wykonanych testów)
2. Wyniki testów i ich interpretację, w szczególności:
   * Informacje dotyczące ogólnej oceny poziomu bezpieczeństwa oraz odporności na ataki badanych systemów zawierające podsumowanie ilości stwierdzonych nieprawidłowości w podziale na systemy i krytyczności,
   * Opis lokalizacji wykrytych podatności - sposobu, w jaki można zlokalizować i powtórzyć testowy atak na podatność,
   * Informacje na temat poziomu ochrony realizowanego przez system zabezpieczeń
3. Wnioski z audytu (określenie ilościowego i jakościowego poziomu niebezpieczeństwa podatności)
4. Rekomendacje i zalecenia pozwalające na usunięcie wykrytych słabości, a tym samym podniesienie poziomu bezpieczeństwa badanych systemów (określenia sposobu naprawy wykrytych podatności w tym zmian konfiguracyjnych)
5. Raport musi być dostarczony Zamawiającemu, w formie elektronicznej – w formacie .DOC i .PDF., najpóźniej w ostatnim dniu realizacji audytu.

# Wymagania dotyczące współpracy zamawiającego z Wykonawcą

W ramach współpracy z Zamawiającym Wykonawca i Zamawiający wyznaczają w swoich strukturach osobę prowadzącą zlecenie oraz osobę zastępującą prowadzącego zlecenie w przypadku jego nieobecności. Wykonawca zobowiązany jest do sprawnej i terminowej realizacji zamówienia oraz stałej współpracy z Zamawiającym, w tym:

1. pozostawania w stałym kontakcie (kontakt telefoniczny oraz drogą elektroniczną; spotkania z Zamawiającym w miarę potrzeb; wyznaczenie osoby do kontaktów roboczych);
2. informowania o stanie prac, pojawiających się problemach i innych zagadnieniach istotnych dla realizacji badania.

# Umowa na realizację zamówienia

Umowa z Wykonawcą zostanie zawarta według zapisów zgodnych z IPU, które znajdują się

w załączniku 2 do SOPZ. Wykonawca, składając ofertę, jednocześnie akceptuje te zapisy.

# Sposób składania ofert

* + 1. Wymagania niezbędne wobec Wykonawcy

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 audytu bezpieczeństwa systemu informatycznego, w ramach których wykonane zostały m. in. testy penetracyjne.

Do każdej usługi przedstawionej w ofercie należy przedstawić dokument potwierdzający, że ta usługa została wykonana należycie.

* + 1. Kryteria wyboru oferty
* Doświadczenie Wykonawcy – wg reguły „spełnia – nie spełnia”
* Cena całkowita – oferty będą oceniane według następującego wzoru:

Punkty w kryterium „cena” = cena oferty najtańszej / cena oferty badanej \* 100 pkt

* + 1. Treść oferty

Oferta Wykonawcy powinna zawierać:

a) informacje i dokumenty potwierdzające spełnianie przez Wykonawcę warunków

w zakresie zrealizowanych usług, o których mowa w punkcie V.1 SOPZ, przedstawione na wzorze tabeli w załączniku 1;

b) koszty wykonania zamówienia w kwocie brutto; koszty te muszą obejmować wszystkie czynności związane z wykonaniem zadania. Koszty te muszą zostać podane zgodnie z poniższym wyszczególnieniem:

|  |  |  |
| --- | --- | --- |
| Usługa | Cena netto usługi | Cena brutto usługi |
| Przeprowadzenie audytu bezpieczeństwa PEF |  |  |

* + 1. Termin i sposób składania ofert

Termin składania ofert upływa w dniu 31 sierpnia 2020 r. o godzinie 16:00. Oferty, które wpłyną po terminie, nie będą rozpatrywane.

Oferty prosimy składać w formie elektronicznej na adres e-mail: [efakturowanie@mr.gov.pl](mailto:efakturowanie@mr.gov.pl)

UWAGA

Niniejsza oferta nie stanowi oferty w myśl art. 66 Kodeksu Cywilnego, jak również nie jest ogłoszeniem w rozumieniu ustawy Prawo zamówień publicznych. Zamawiający zastrzega sobie prawo do odstąpienia od udzielenia zamówienia bez podania przyczyn.

Zamawiający informuje, iż całościowa oferowana cena stanowi informację publiczną

w rozumieniu Ustawy o dostępie do informacji publicznej z dnia 6 września 2001 r. (Dz. U.

z 2001 r. Nr 112 poz 1198 z poźn. zm.).

Zamawiający zastrzega sobie prawo do kontaktu z Oferentami w celu doprecyzowania ofert

i uzyskania dodatkowych wyjaśnień.

Zamawiający zastrzega sobie prawo do odpowiedzi tylko na ofertę wybraną, jako najkorzystniejszą. Wykonawca wybrany do wykonania przedmiotowego zamówienia obowiązany będzie przedstawić aktualny odpis z właściwego rejestru wystawiony nie wcześniej niż 6 miesięcy przed dniem zawarcia umowy albo aktualne zaświadczenie o wpisie do ewidencji działalności gospodarczej. O terminie podpisania umowy Zamawiający powiadomi Wykonawcę z 3-dniowym wyprzedzeniem.

Okres związania ofertą wynosi 30 dni od upływu terminu składania ofert.

Za najkorzystniejszą zostanie uznana oferta z najniższą ceną brutto za przedmiot zamówienia.

ZAŁĄCZNIKI

1. Wzór wykazu usług;

2. Istotne postanowienia umowy;