**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA**

**Przeprowadzenie audytu bezpieczeństwa systemu iSDA-2.0**

# Kontekst zamówienia

Prokuratura Krajowa realizuje projekt „Rozwój Systemu Digitalizacji Akt Postępowań Przygotowawczych w Sprawach Karnych (iSDA-2.0)” współfinansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Polska Cyfrowa, Oś priorytetowa nr 2 „E-Administracja i otwarty rząd”, Działanie 2.1.

Projekt iSDA-2.0 jest kontynuacją poprzedniego Projektu iSDA, który został przerwany po zrealizowaniu Etapu 1 umowy zawartej w ramach postepowania postępowania POS-1 ze względów organizacyjno-formalnych.

Projekt iSDA-2.0 został podzielony na cztery komponenty:

1. System PROK-SYS.
2. Centralne Usługi Infrastrukturalne.
3. Platforma ITS.
4. Farma Stacji Roboczych.

# Przedmiot zamówienia

Przedmiotem zamówienia jest usługa przeprowadzenia badania bezpieczeństwa systemu informatycznego, będącego wynikiem realizacji projektu iSDA-2.0, tj. obejmującego centralne usługi infrastrukturalne oraz system PROK-SYS, łącznie zwane dalej Systemem.

# Realizacja zamówienia

Przedmiot zlecenia będzie realizowany w 2 etapach:

1. etap I – audyt bezpieczeństwa Systemu w tym przegląd bezpieczeństwa oraz testy penetracyjne,
2. etap II – powtórne testy penetracyjne (retesty) w celu potwierdzenia usunięcia przez Zamawiającego wszystkich podatności oraz słabości Systemu wykrytych przez Wykonawcę w trakcie realizacji   
   etapu I.

# Ogólny opis architektury Systemu

W ramach Systemu wydzielone będą dwie strefy bezpieczeństwa:

* Strefa Wewnętrzna – będą w niej umieszczone wyłącznie elementy Systemu do której będą miały dostęp wszystkie jednostki prokuratury połączone poprzez dedykowaną sieć WAN-PROK. Rozwiązania bezpieczeństwa Strefy Wewnętrznej pozwolą również na wymianę danych z instytucjami współpracującymi z prokuraturą poprzez specjalne dedykowane łącza.
* Strefa Zewnętrzna – w której będą zainstalowane elementy Systemu zapewniające dostęp wydzielonych zasobów z Internetu.

Strefa Wewnętrzna ze Strefą Zewnętrzną posiada tylko jeden punkt styku – zwany dalej „Bramą W-Z” - umożliwiający przekazanie danych ze Strefy Wewnętrznej do Zewnętrznej. „Brama W-Z” pełni rolę rozwiązania zapewniającego jednokierunkową, bezpieczną wymianę danych.

Wysokopoziomowy diagram komponentów Systemu stanowi Załącznik nr 1 do OPZ.

Schemat architektury fizycznej Systemu stanowi załącznik nr 2 do OPZ.

Schemat architektury logicznej Systemu stanowi załącznik nr 3 do OPZ.

# Zakres testów bezpieczeństwa

Zakres testów bezpieczeństwa obejmuje w szczególności następujące obszary:

1. Portal zewnętrzny,
2. Portal wewnętrzny,
3. Podsystem aplikacji portalowych,
4. Podsystem Libra3,
5. węzły dostępowe dla instytucji zewnętrznych,
6. bramę W-Z.

# Charakter wykonywanych prac

Audyt bezpieczeństwa złożony będzie z następujących zadań:

1. przeglądu bezpieczeństwa – mających na celu identyfikację potencjalnych podatności w Systemie,
2. testów penetracyjnych – których celem jest weryfikacja odporności wybranych komponentów Systemu (np. styku z siecią Internet, aplikacją webową, serwerem bazy danych) na realistyczne próby przełamania zabezpieczeń dokonywane z sieci wewnętrznej Zamawiającego lub z Internetu.

Przegląd bezpieczeństwa zostanie wykonany poprzez analizę i ocenę architektury i konfiguracji poszczególnych komponentów na poziomie dokumentacji oraz bezpośrednio w środowisku informatycznym Zamawiającego.

Testy penetracyjne prowadzone będą metodą „szarej skrzynki” (ang. „gray box”), w której osoba testująca posiadać będzie dostęp do dokumentacji, jak struktur danych, ale nie będzie posiadać dostępu do kodów źródłowych.

# Miejsce prowadzenia testów

Testy wykonywane będą z lokalizacji Zamawiającego z wyłączaniem testów badających interfejsy na styku z siecią Internet od strony zewnętrznej, które mogą być prowadzone zdalnie z lokalizacji Wykonawcy.

# Metodyka prowadzenia testów bezpieczeństwa

Zamawiający wymaga, aby Wykonawca przedstawił w ofercie metodykę realizacji testów bezpieczeństwa. Metodyka musi posiadać następujące cechy:

1. Bazować na uznanych standardach w zakresie testowania bezpieczeństwa systemów i oprogramowania, w aktualnych wersjach w momencie realizacji prac, tj.:
   * Open Web Application Security Project (OWASP) - OWASP Testing Guide
   * Open Source Security Testing Methodology Manual (OSSTMM)
   * Penetration Testing Execution Standard (PTES)
   * lub równoważnych (za równoważne Zamawiający uzna, standardy opisujące przebieg procesów testowania bezpieczeństwa systemów IT oraz obszary systemowe, które muszą podlegać weryfikacji)
2. Wykorzystać bazy danych o znanych podatnościach i słabościach bezpieczeństwa:
   * Common Weakness Enumeration (CWE)
   * Common Vulnerabilities and Exposures (CVE)
   * Common Configration Enumeration (CCE)
   * OWASP Top 10 Application Security Risks
   * SANS Top 20 Critical Security Controls
3. Wykorzystać listy kontrolne udostępnione przez uznane organizacje pracujące na rzecz bezpieczeństwa systemów IT, tj.:
   * Application Security Verification Standard (ASVS)
   * National Security Agency (NSA)
   * Center for Internet Security (CIS).

# Struktura prac

Dla każdego badanego komponentu struktura prac Wykonawcy powinna obejmować następujące punkty:

1. rekonesans – faza badania mająca na celu zdobycie jak największej liczby informacji o sprawdzanym komponencie w celu wykorzystania ich do konstrukcji dalszych ataków. Może przyjmować dwie formy – aktywną i pasywną, gdzie:
   1. rekonesans aktywny – ma na celu identyfikację badanego komponentu (wersja OS, serwerów aplikacyjnych, baz danych itp.) oraz używanych usług sieciowych ze szczególnym uwzględnieniem niewykorzystywanych usług sieciowych. W ramach rekonesansu aktywnego sprawdzane otwarte porty TCP i UDP, badane są usługi ICMP, SMTP/POP3/IMAP, HTTP/HTTPS, FTP, SSH, Telnet, DNS (wersja, numer seryjny, czas odświeżania, termin wygasania, analiza rekordów SOA, MX, NS, A, PTR, SRV, HINFO, TXT, CNAME, RP, parametry transferów stref, poddomeny); rozszerzenia ASP.net, OWA, PHP, OpenSSL, systemy CMS. W ramach rekonesansu aktywnego weryfikowane jest również stosowanie domyślnych/ fabrycznych haseł dostępowych do badanych komponentów oraz struktura katalogów serwisów WWW.
   2. rekonesans pasywny – ma również na celu zebranie dostępnych informacji dotyczących badanych komponentów, przy czym źródłami informacji są dane i metadane dostępne poza organizacją - zapisane w rejestrach organizacji odpowiedzialnych za funkcjonowanie publicznej sieci Internet (RIPE, IANA - zakresy adresów publicznych, numery AS BGP), publiczne strony WWW, informacje z rejestrów biznesowych (KRS), dane finansowe, dane teleadresowe - lokalizacje, telefony, e-mail, portale Social/Business networks, publicznie dostępne dane o przetargach.
2. identyfikacja słabości – na podstawie informacji zebranych w trakcie wykonywania rekonesansu rozpoznanie potencjalnych braków, niedoskonałości wykorzystywanego oprogramowania i konfiguracji. Identyfikacja powinna obejmować powszechnie dostępne bazy danych o często popełnianiach błędach projektowania i implementowania zabezpieczeń oprogramowania, w tym listy kontrolne takie jak, CIS Benchmark, OWASP ASVS. W przypadku testów penetracyjnych wykonywanych metodą „szarej skrzynki” w ramach identyfikacji słabości należy uwzględnić przegląd dokumentacji, przegląd dzienników, zaimplementowane reguły zabezpieczające, w tym dane konfiguracyjne aplikacji, usług i systemów bezpieczeństwa.
3. identyfikacja podatności – faza służąca do zdefiniowania scenariuszy możliwych do zastosowania technik przełamania zabezpieczeń badanych komponentów i może być wykonywana za pomocą narzędzi automatycznych oraz za pomocą technik manualnych, przy czym:
   1. skanowanie automatyczne – służy do uzyskania informacji o znanych, istniejących w badanych systemach podatnościach, błędach w konfiguracji oraz sposobach ich mitygacji. Dodatkowo w zależności od przyjętego scenariusza skanowanie może być wykonywane bez lub z autoryzowanym dostępem do badanego komponentu poprzez interfejs sieciowy lub lokalnie. W ramach identyfikacji podatności wykorzystywane są informacje o podatnościach w publicznych bazach (CVE, NISTGov, Expoit-DB, Rapid7). W ramach skanowania automatycznego sprawdzane jest użycie w badanych komponentach domyślnych haseł, jak również przeprowadzane są ataki słownikowe. Skanowanie może być przeprowadzane na różnych poziomach agresywności – od skanowania, które nie wpływa w znaczący sposób na działanie badanego komponentu do takiego, które może istotnie degradować poziom dostępności,
   2. skanowanie ręczne – służy do weryfikacji potencjalnych podatności zidentyfikowanych w fazie skanowania automatycznego przy użyciu technik manualnych, w tym skryptów, dodatkowych narzędzi, przeglądarki WWW, aplikacji klienckiej. Faza ta ma celu potwierdzenie, które z podatności są false-positives oraz false-negatives oraz identyfikację zależności między podatnościami, które przy zbiorczym wykorzystaniu mogą ułatwić przełamanie zabezpieczeń badanych komponentów.
4. weryfikacja podatności/ Proof-of-Concept (PoC) – opracowanie i weryfikacja scenariuszy exploitacji badanych komponentów, które mają na celu potwierdzenie możliwości przeprowadzenia skutecznego ataku. W ramach weryfikacji podatności wykorzystywane są dedykowane narzędzia i techniki pozwalające na uzyskanie dostępu do badanego komponentu, podniesienie uprawnień, umieszczenie szkodliwej zawartości, uzyskanie nieautoryzowanego dostępu do danych, pobranie w sposób nieautoryzowany danych. Typowy scenariusz zakłada następujące elementy weryfikacji podatności:
   1. uzyskanie nieautoryzowanego dostępu,
   2. podniesienie uprawnień atakującego,
   3. infiltracja badanego komponentu, tj. zdobycie użytecznych danych,
   4. instalacja dodatkowych narzędzi pozwalających na dalszą infiltrację,
   5. zatarcie śladów penetracji.
5. analiza istotności - zweryfikowane podatności są przedmiotem analizy istotności, która powinna być oparta na bazie zaleceń metodologii System Common Weakness Scoring (CWSS) lub System Common Vulnerability Scoring System (CVSS), tj. powinna oceniać co najmniej następujące cechy podatności:
   1. wektor ataku (sieciowy AV:N, sąsiadujący AV:A; lokalny AV:L, fizyczny AV:P),
   2. złożoność ataku (niska AC:L, wysoka AC:H),
   3. wymagane uprawnienia (brak PR:N, niskie PR:L, wysokie PR:H),
   4. wymagana interakcja z użytkownikiem (brak UI:N, wymagana UI:R),
   5. zakres oddziaływania podatności (badany obiekt S:U, powiązane komponenty S:C),
   6. wpływ podatności na poufność (brak C:N, niska C:L, wysoka C:H),
   7. wpływ podatności na integralność (brak I:N, niska I:L, wysoka I:H),
   8. wpływ podatności na dostępność (brak A:N, niska A:L, wysoka A:H),
   9. aktualny status skuteczności wykorzystania podatności (niezdefiniowany E:X; nieudowodniony E:U; PoC E:P; funkcjonalny E;F; wysoki E:H),
   10. aktualny status mitygacji podatności (niezdefiniowany RL:X; oficjalna łata RL:O; tymczasowa łata RL:T; obejście RL:W; brak RL:U),
   11. poziom udokumentowania podatności (niezdefiniowany RC:X; nieznany RC:U; rozsądny RC:R; potwierdzony RC:C).

Podatności poddane są kwalifikacji na jednym z pięciu poziomów: krytyczne, wysokie, średnie, niskie, informacyjne.

1. raportowanie – w ramach którego wszystkie opisane powyżej czynności zostaną udokumentowane w raporcie z audytu, którego struktura i zawartość opisana jest w punkcie 7.

# Produkt prac

Produktem prac będzie raport, tzw. Raport z audytu, zawierający: obserwacje oraz rekomendacje Wykonawcy dotyczące sposobów mitygacji podatności. Raport, zawierać będzie następujące pozycje:

* 1. Wstęp - zakres wykonanych prac audytowych.
  2. Wykaz osób realizujących testy - z uwzględnieniem nazwisk osób odpowiedzialnych za wykonanie badań, przeprowadzenie analizy wyników, opracowanie i kontrolę jakości dokumentacji.
  3. Termin, miejsce i rodzaj prowadzonych prac audytowych.
  4. Streszczenie dla kierownictwa zawierające:
     1. Informacje o komponentach Systemu poddanych testom bezpieczeństwa.
     2. Syntetyczny opis prowadzonych prac audytowych.
     3. Zestawienie zidentyfikowanych podatności i słabości ze wskazanym poziomem ryzyka oraz krótką charakterystykę podatności i słabości o krytycznym lub wysokim poziomie ryzyka, uszeregowanych od najbardziej do najmniej krytycznych.
  5. Szczegółowa część techniczna zawierająca:
     1. Opis zastosowanej metodyki.
     2. Wykaz sprawdzonych obszarów, zadań wykonywanych przy sprawdzeniu poszczególnych obszarów wraz ze statusem wykonania zadań, zawierający również rodzaje przeprowadzonych testów i badań, dla których nie zostały wykryte żadne istotne podatności.
     3. Listę i opis wykrytych podatności i słabości wraz z ich klasyfikacją, zgodnie z tabelą poniżej.

Tabela 1. Charakterystyka podatności i słabości

| **Pole** | **Opis** |
| --- | --- |
| Nazwa | Nazwa wykrytej podatności |
| Data wykrycia | Data wykrycia podatności |
| Kategoria | Ogólna kategoria podatności zgodnie z wybraną metodyką (np. OWASP, ASVS, CVE, CWE) |
| Podatne zasoby | Nazwy zasobów (adresy IP, adresy URL, aplikacje, urządzenia), na których wykryto daną podatność |
| Poziom istotności | Poziom istotności podatności, zgodnie z klasyfikacją zdefiniowaną w metodyce |
| Priorytet działań naprawczych | Poziom priorytetu działań naprawczych, określony przez Wykonawcę, zgodnie z klasyfikacją zdefiniowaną w metodyce |
| CVSS / CWSS | Ocena ryzyka podatności na podstawie klasyfikacji CVSS lub CWSS |
| Opis podatności | Szczegółowy techniczny opis zasady działania i skutków wykorzystania podatności lub słabości |
| Warunki | Zidentyfikowane specyficzne okoliczności sprawdzenia lub stany komponentu, od których mogło zależeć ujawnienie podatności/słabości (np. uprzednie zalogowanie, wyłączenie usługi, szczególne miejsce, z którego wykonano test, uzyskane wcześniej hasło) |
| Przykładowy wektor ataku | Opis przykładowego scenariusa wykorzystania opisywanej luki lub słabości do wykonania ataku |
| Opis skutków | Opis skutków jakie może wywołać wykorzystanie wykrytej podatności lub słabości |
| Rekomendowane działania naprawcze | Rekomendowane, w opinii Wykonawcy, działania naprawcze mające na celu wyeliminowanie wykrytych zagrożeń, gdzie przedstawione rekomendacje mogą dzielić się na rekomendacje tymczasowe (tj. doraźnie rozwiązanie problemu) oraz rekomendacje docelowe, czyli opis stanu oczekiwanego, którego osiągnięcie pozwala na całkowite wyeliminowanie podatności lub słabości |
| Narzędzia | Narzędzia i sposób ich użycia do wykrycia i wykorzystania podatności/słabości |
| Ewidencja istnienia podatności | Dowody, w tym np. zrzuty ekranu, przykładowe zapytania, wyniki narzędzi automatycznych dokumentujących odkrycie lub wykorzystanie podatności/słabości |
| Referencje | Zewnętrzne źródła dodatkowych informacji na temat podatności lub słabości |
| Uwagi | Dodatkowe uwagi dotyczące ograniczeń przeprowadzonego badania, zakresu ważności jego wyników, niepewności, zaobserwowanych anomalii lub czynników mogących mieć wpływ na powtarzalność wykrycia lub wykorzystanie podatności lub słabości (np. okoliczność losowa) |

* + 1. Opis ewentualnych dodatkowych działań sprawdzających lub dodatkowych testów, które według Wykonawcy powinny zostać przeprowadzone w odniesieniu do badanych systemów.
  1. Zestawienie wyników przeglądu realizacji wymagań standardu ASVS z określonym dla każdego punktu stopniem zgodności (tj. zgodny, częściowo zgodny, niezgodny, nie dotyczy), krótkim wyjaśnieniem, na czym ewentualna niezgodność polega, a także odsyłaczem do opisanej w Szczegółowej części technicznej słabości lub podatności, jaka wynika z ewentualnej niezgodności.
  2. Ewidencja prac (raporty z narzędzi automatycznych, logi, zrzuty ekranu, sesje z narzędzi audytowych) niepowiązana bezpośrednio z żadną z podatności lub powiązana z wieloma.

Załącznik nr 1. Wysokopoziomowy diagram komponentów Systemu.



Załącznik nr 2. Schemat architektury fizycznej Systemu.



Załącznik nr 3. Schemat architektury logicznej Systemu.

