

Opis Przedmiotu Zamówienia

**Testy bezpieczeństwa sieci WLAN
w Najwyższej Izbie Kontroli**

Spis Treści

1.	Słownik użytych pojęć	3
2.	Przedmiot zamówienia	3
3.	Harmonogram realizacji przedmiotu zamówienia	3
4.	Plan testów	4
5.	Zakres testów i wymagania	4
6.	Wyłączenia z testów	5
7.	Raport z testów	5
8.	Zastrzeżenia i wymagania	6
9.	Komunikacja między Wykonawcą a Zamawiającym	7

1. Słownik użytych pojęć

Siedziba NIK	Budynek Najwyższej Izby Kontroli ul. Filtrowa 57 w Warszawie.
Strony	Zamawiający i Wykonawca.
Wykonawca	Podmiot realizujący Umowę.
Zamawiający	Najwyższa Izba Kontroli (NIK).
Umowa	Umowa wraz z jej Załącznikami i wszelkimi Aneksami zawarta pomiędzy Zamawiającym a Wykonawcą.
OPZ	Opis przedmiotu zamówienia (niniejszy dokument).
Testy / Testy Bezpieczeństwa	Testy bezpieczeństwa WLAN (Wi-Fi) przeprowadzone przez Wykonawcę.
Harmonogram	Wykaz poszczególnych etapów prac i ram czasowych ich realizacji przedstawiony w pkt 3.

2. Przedmiot zamówienia

2.1 Przedmiotem zamówienia jest wykonanie testów bezpieczeństwa sieci WLAN na terenie Najwyższej Izby Kontroli przy ulicy Filtrowej 57, 02-056 Warszawa, a następnie sporządzenie i przekazanie Zamawiającemu raportu z przeprowadzonych prac.

2.2 Zakres przedmiotu zamówienia:

- a) opracowanie przez Wykonawcę Planu Testów, zgodnie z wymaganiami określonymi w pkt 4 i 5,
- b) przeprowadzenie testów bezpieczeństwa WLAN zgodnie z:
 - Harmonogramem realizacji przedmiotu zamówienia (pkt 3),
 - Planem Testów (pkt 4),
 - Zakresem testów i wymaganiami (pkt 5),
 - Wyłączeniami z testów (pkt 6).
- c) opracowanie raportu zgodnie z wytycznymi określonymi w pkt 7.2.

3. Harmonogram realizacji przedmiotu zamówienia

etap	opis zadania	termin
I.	Opracowanie przez Wykonawcę Planu Testów.	do 7 dni od podpisania Umowy przez Strony
II.	Zatwierdzenie przez Zamawiającego Planu Testów lub zgłoszenie Wykonawcy uwag (w formie komentarzy) do punktów, względem których wystąpiły wątpliwości.	do 7 dni od otrzymania Planu Testów od Wykonawcy
III.	Odniesienie się przez Wykonawcę do uwag dotyczących Planu Testów (jeżeli zostały zgłoszone przez Zamawiającego) i udzielenie odpowiedzi Zamawiającemu.	do 7 dni od otrzymania uwag od Zamawiającego
IV.	Przeprowadzenie Testów i poinformowanie Zamawiającego o ich zakończeniu.	zgodnie z terminem przedstawionym w ramowym harmonogramie testów – maksymalnie 30 dni od

		zaakceptowania Planu Testów przez Zamawiającego
V.	Sporządzenie przez Wykonawcę Raportu z przeprowadzonych Testów i udostępnienie go Zamawiającemu.	do 10 dni od poinformowania Zamawiającego o ukończeniu Testów

4. Plan testów

- 4.1 Wykonawca zobowiązany jest do sporządzenia dokumentu „Plan testów” i dostarczenia go Zamawiającemu w terminie zgodnym z etapem I Harmonogramu.
- 4.2 Dokument „Plan testów” musi zawierać:
- spójny i czytelny plan realizacji prac wykonanych w ramach Testów,
 - przyjęte standardy przeprowadzanych Testów,
 - oprogramowanie oraz narzędzia, które będą używane podczas Testów,
 - zakres i rodzaje symulowanych ataków / testów penetracyjnych,
 - rodzaje działań, które mogą powodować zakłócenia lub brak dostępności sieci WLAN,
 - wymagania techniczne i organizacyjne, jakie musi spełnić Zamawiający, aby realizacja Testów mogła odbyć się z zachowaniem standardów bezpieczeństwa i zapewnienia nieprzerwanej pracy testowanych zasobów,
 - analizę ryzyka związanego z przeprowadzeniem Testów,
 - ramowy harmonogram testów.

5. Zakres testów i wymagania

- 5.1 Testy będą przeprowadzone stacjonarnie, w Siedzibie NIK oraz w bliskim otoczeniu Siedziby NIK.
- 5.2 Testy będą przeprowadzane w formule Black Box.
- 5.3 Testy mogą być prowadzone metodami manualnymi oraz automatycznymi.
- 5.4 Minimalne wymagania dotyczące testowanych obszarów:
- identyfikacja punktów dostępowych WLAN (widoczne + ukryte):
 - wokół budynku Siedziby NIK (wardriving),
 - wewnątrz budynku Siedziby NIK, na poszczególnych kondygnacjach,
 - weryfikacja zasięgu,
 - identyfikacja podatności sieci WLAN należących do NIK,
 - próby wykrycia i wykorzystania m.in.:
 - Deployment of Vulnerable WEP Protocol,
 - Man-in-the-Middle Attacks,
 - Default SSIDs and Passwords,
 - Misconfigured Firewalls,
 - WPA2 Crack Vulnerability (weak encryption),
 - NetSpectre – Remote Spectre Exploit,
 - Packet Sniffing,
 - Evil Twin,
 - SSID Broadcasting,

- Rogue AP Detection.
- e) analiza konfiguracji punktów dostępowych WLAN:
 - szyfrowanie i uwierzytelnianie,
 - stosowane protokoły.
- 5.5 Wykonawca zobowiązany jest do niezwłocznego poinformowania Zamawiającego o krytycznych podatnościach wykrytych w czasie prowadzenia Testów.

6. Wyłączenia z testów

- 6.1 Niedozwolone są: testy penetracyjne, identyfikacja zabezpieczeń oraz eksploatacja sieci WLAN innych, niż należących do NIK. Lista nazw sieci należących do NIK zostanie udostępniona Wykonawcy po podpisaniu Umowy.
- 6.2 Niedozwolone jest korzystanie z zabiegów socjotechnicznych.

7. Raport z testów

- 7.1 Raport z Testów zostanie przygotowany w siedzibie Wykonawcy, a następnie dostarczony do Zamawiającego zgodnie z warunkami Umowy, w terminie zgodnym z etapem V Harmonogramu.
- 7.2 Raport z Testów musi zawierać następujące elementy:
 - a) cel i zakres testów WLAN,
 - b) przyjęte standardy przeprowadzanych testów,
 - c) skład zespołu biorącego udział w testach wraz z informacją o pełnionych funkcjach i posiadanych certyfikatach,
 - d) urządzenia i oprogramowanie wykorzystane do przeprowadzenia testów,
 - e) adresy IP, z których były prowadzone testy,
 - f) krótkie podsumowanie z przeprowadzonych prac,
 - g) wykryte podatności wraz z opisem, sposobem ich wykrycia i dołączonymi zrzutami ekranu (opisy muszą pozwolić Zamawiającemu na odwzorowanie czynności przeprowadzonych przez Wykonawcę),
 - h) ocenę ryzyka znalezionych podatności,
 - i) rekomendacje dotyczące wdrożenia poprawek oraz ocenę poziomu ich złożoności i orientacyjnego czasu wdrożenia,
 - j) ogólne rekomendacje dotyczących podniesienia poziomu bezpieczeństwa sieci WLAN.

8. Zastrzeżenia i wymagania

- 8.1 Zespół realizujący przedmiot zamówienia musi liczyć minimum 2 osoby, a każda z nich musi posiadać co najmniej jeden z poniższych certyfikatów:
 - a) CEH (Certified Ethical Hacker),
 - b) OSCP (Offensive Security Certified Professional)
 - c) OSCE (Offensive Security Certified Expert),
 - d) CISSP (Certified Information Systems Security Professional),
 - e) CISA (Certified Information Systems Auditor).
- 8.2 Co najmniej jedna z osób w zespole realizującym zamówienie musi posiadać następujące certyfikaty:
 - a) OSCP lub OSCE,

- b) CISSP lub CISA.
- 8.3 Testy muszą być wykonane zgodnie z normą: ISO/IEC/IEEE 29119-3 „Software and Systems Engineering - Software Testing” lub równoważną.
- 8.4 Testy muszą uwzględniać wytyczne następujących standardów:
 - a) normy ISO dotyczące zarządzania jakością z rodziny 9000 (obecnie 2500x), 90003 lub równoważne,
 - b) IEEE (np. 829, 1012, 1044) lub równoważne,
 - c) ISTQB (Agile, Advanced & Expert Level Syllabus) lub równoważne.
- 8.5 Testy muszą zostać wykonane w oparciu o najlepsze standardy wykonywania testów bezpieczeństwa sieci WLAN.
- 8.6 Jeżeli Wykonawca przewiduje w ramach prowadzonych Testów wykonywanie działań, które mogą spowodować zakłócenia lub brak dostępności sieci WLAN, musi je zgłosić Zamawiającemu.
- 8.7 Działania mogące spowodować zakłócenia lub brak dostępności sieci WLAN mogą być prowadzone od godziny 17:00 w dni robocze oraz w dni wolne od pracy, po wcześniejszym uzgodnieniu terminu z Zamawiającym.
- 8.8 Zamawiający wymaga, aby wszystkie dokumenty wytworzone w ramach realizacji Umowy charakteryzowały się:
 - a) wysoką jakością merytoryczną,
 - b) czytelną i zrozumiałą strukturą (z podziałem na rozdziały, podrozdziały i sekcje),
 - c) spójnością wizualną.
- 8.9 Zamawiający wymaga, aby cała dokumentacja, o której mowa w OPZ, podlegała jego akceptacji przed zakończeniem realizacji Umowy zgodnie z terminami określonymi w harmonogramie.

9. Komunikacja między Wykonawcą a Zamawiającym

- 9.1 Wszystkie prace będą realizowane przy udziale lub w konsultacji z wyznaczonymi do tego zadania pracownikami Zamawiającego.
- 9.2 Możliwe kanały komunikacji:
 - a) wideokonferencja (obsługę zapewnia Zamawiający),
 - b) telefon,
 - c) e-mail,
 - d) spotkanie w Siedzibie NIK.
- 9.3 Wykonawca będzie konsultował z Zamawiającym wszystkie przyjmowane założenia poczynione w związku z realizacją Umowy. W związku z tym, w razie potrzeby dostarczy wszelkich niezbędnych wyjaśnień i materiałów dodatkowych (opisów, dokumentacji itp.) wyznaczonym pracownikom Zamawiającego tak, aby było możliwe ich jednoznaczne zrozumienie.
- 9.4 Wszystkie ustalenia poczynione za pośrednictwem wideokonferencji, telefonicznie lub w trakcie spotkań muszą zostać niezwłocznie zaakceptowane przez Zamawiającego za pośrednictwem wiadomości e-mail.
- 9.5 Wykonawca zobowiązany jest poinformować Zamawiającego o wszystkich zdarzeniach lub przeszkodach mogących spowodować opóźnienie w wykonaniu Umowy w stosunku do terminów przewidzianych w Umowie.