Urząd Zamówień Publicznych

Biuro Dyrektora Generalnego
Dyrektor
Szymon Giderewicz

Znak pisma BDG.ZZP.272.10.2026.AK

Warszawa, dnia 23 listopada 2026 roku

ODPOWIEDZI NA WNIOSEK O WYJAŚNIENIE TREŚCI SWZ I ZMIANA TREŚCI SWZ

Dotyczy postępowania numer: IX/2026 – „Testy bezpieczeństwa klasy APT dla usług internetowych i infrastruktury sieciowej oraz oprogramowanie do skanowania podatności”

Zamówienie realizowane w ramach projektu Krajowego Planu Odbudowy i Zwiększania Odporności finansowanego ze środków Instrumentu na Rzecz Odbudowy i Zwiększania Odporności Inwestycja C3.1.1. Cyberbezpieczeństwo – CyberPL, infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo Cyberbezpieczeństwo - Cyberbezpieczny Rząd; konkurs grantowy pn. “Cyberbezpieczny Rząd” o numerze KPOD.05.10-CR.01-001/25"

Zamawiający działając na podstawie art. 284 ust. 6 z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. z 2026 poz. 793 t.j.) zwanej dalej „ustawą Pzp, przekazuje wnioski o wyjaśnienie treści Specyfikacji Warunków Zamówienia (zwanej dalej „SWZ") wraz z udzielonymi odpowiedziami:

Zamawiający informuje, że pytania oraz odpowiedzi na nie stają się integralną częścią SWZ i będą wiążące przy składaniu ofert.

Pytanie 1:

1. Dla jakiego SIEM będą miały być przygotowane reguły?

Odpowiedź:

Forti SIEM.

Pytanie 2:

W związku z tym, że zamówienie dotyczy usług typu Red Team, a osiągnięcie celów w takich ćwiczeniach może zależeć w dużym stopniu od poświęconego na ćwiczenie czasu, ile czasu w roboczogodzinach zamawiający zakłada na realizację poszczególnych etapów?

Odpowiedź:

Zamawiający nie definiuje oczekiwań co do poświęconego na ćwiczenie czasu.

Pytanie 3:

Threat modeling strategiczny (Zadanie A)

1. W zakresie fragmentu zakresu„audyt konfiguracji mechanizmów ochrony obwodowej" – jakie konkretnie urządzenia (typ, producent, wersja, liczba sztuk danego urządzenia) mają podlegać audytowi?

Odpowiedź:

Jedno urządzenie NGFW, producent: Barracuda.

Pytanie 4:

Test Assumed Breach z laptopa użytkownika

1. W zakresie fragmentu zakresu „Rekomendacje poprawy ochrony endpointu + szkoleń użytkowników” – czy chodzi o szkolenia w zakresie ochrony endpointów, czy inaczej należy rozumieć tą część zakresu?

Odpowiedź:

Poprzez „+ szkoleń użytkowników” Zamawiający rozumie:
Szkolenie dla zespołu użytkowników (administratorów) obejmujące swoim zakresem wyjaśnienia dot. wad obecnej konfiguracji i rekomendowanych zmian w konfiguracji ochrony endpoint.

Pytanie 5:

TP serwisów www

1. Czy zakres prac obejmuje TB aplikacji po zalogowaniu dla poniższych domen:
   - espd.uzp.gov.pl
   - miniportal.uzp.gov.pl
   - aukcje.uzp.gov.pl
   - bzp.uzp.gov.pl
   - pzp.gov.pl
   - formularz.uzp.gov.pl
   - orzeczenia.uzp.gov.pl
   - wokanda.uzp.gov.pl
   - elearning.uzp.gov.pl
   - ekomentarzpzp.uzp.gov.pl

Jeśli odpowiedź na powyższe pytanie brzmi tak, prosimy o udzielenie odpowiedzi na poniższe pytania dla każdej aplikacji webowej:

1. Krótki opis do czego służy aplikacja (np. aplikacja do realizacji transakcji bankowych, sklep internetowy) oraz kluczowe funkcje (lista głównych funkcji) oraz opis kategorii przetwarzanych danych (dane osobowe klientów, dane kartowe, dane transakcyjne, dane o stanie zdrowia etc.).

2. Lista metod logowania/uwierzytelniania: (np. ID, hasło, certyfikat, token, kod sms), które mają zostać objęte testami.
3. Lista metod autoryzacji operacji (jeśli występuje): (np. certyfikat, token (sprzętowy), kod sms, urządzenia HSM (Hardware Security Module, inne - proszę podać jakie), które mają zostać objęte testami.
4. Liczba ról, które mają podlegać testom (np. gość, użytkownik zwykły, użytkownik rozszerzony, operator, administrator, itp.) wraz z krótkim opisem (np. administrator – zarządza prawami dostępu innych użytkowników), które mają zostać objęte testami.
5. Sumaryczna, orientacyjna liczba pól we wszystkich formularzach, które mają zostać objęte testami.
6. Zamawiający oczekuje „Rekomendacje techniczne (konkretne zmiany w kodzie, konfiguracji, architekturze)" – jak rozumiemy jednak wykonawca nie będzie miał dostępu do kodu czy konfiguracji, by móc zarekomendować ww. zmiany konkretnie, a wyłącznie ogólnie – czy możemy prosić o potwierdzenie takiego podejścia?
7. Wiele z narzędzi wymienionych przez Zamawiającego to skanery podatności, czy wymaganiem jest wykonanie wyłącznie skanów przy pomocy skanerów, czy wykonania manualnych testów apliakcji?

Odpowiedź:

Zamawiający zmienia listę serwisów podlegającym testom, usuwając portal elearning.uzp.gov.pl.

Ad.1, 2, 3, 4, 5.

Serwis	Do czego służy + kluczowe funkcje	Kategorie danych
espd	Wypełnianie i ponowne wykorzystanie Jednolitego Europejskiego Dokumentu Zamówienia (eESPD); kreator 5-	W usłudze nie dochodzi do zapisu danych

Serwis	Do czego służy + kluczowe funkcje	Kategorie danych
	etapowy, import/eksport eESPD (XML/PDF), 24 języki	
miniportal	Platforma ofertowania i komunikacji w postępowaniach; lista postępowań, składanie i szyfrowanie ofert, komunikacja z zamawiającym, komunikaty systemowe, przegląd postępowań	dane osobowe zamawiających
bzp (+searchbzp)	Publikacja ogłoszeń o zamówieniach, wynikach i umowach; wyszukiwarka ogłoszeń; publiczny SOAP WebService; sprawozdania roczne	dane zamawiających (NIP/REGON, nazwa, adres, osoby kontaktowe), treść ogłoszeń, dane wykonawców w sprawozdaniach; dane jawne — UDIP art. 1 ust. 1
aukcje	Platforma aukcji elektronicznych: zakładanie i prowadzenie aukcji, postąpienia, wiadomości zamawiający↔wykonawca, archiwum zakończonych aukcji	dane identyfikacyjne zamawiającego i wykonawców, dane postępowań, dokumenty ofertowe z podpisem, komunikaty, dane personalizacji (login, e-mail, telefon)
pzp.gov.pl	Portal informacyjny: Wiedza (baza artykułów i wytycznych), Forum (wątki, komentarze, tagi,	dane osobowe użytkowników (imię, nazwisko, nick, e-mail,

Serwis	Do czego służy + kluczowe funkcje	Kategorie danych
	zgłaszanie naruszeń), Konsorcjum (ogłoszenia o partnerstwach), Wyszukiwarka orzeczeń, Centrum pomocy, Biuletyn Zamówień Publicznych, Aktówka, Newsletter, powiadomienia, personalizacja konta, zgłaszanie problemów	telefon), treść postów i komentarzy, załączniki, preferencje i personalizacja, dane redakcyjne
formularz	Zestaw formularzy zgłoszeniowych na szkolenia	dane osobowe zgłaszających (imię, nazwisko, e-mail służbowy, adres, instytucja)
orzeczenia	Wyszukiwarka orzeczeń KIO: wyszukiwanie pełnotekstowe, zaawansowane (9 kryteriów, 198 opcji), wybór rodzaju orzeczenia, sygnatura, zakres dat, wyszukiwarka TSUE, pobieranie PDF	treść orzeczeń i dane stron postępowań (sędziowie, pełnomocnicy, NIP-y, kwoty) — dane jawne
wokanda	Wokanda rozpraw KIO: dzisiejsza, archiwalna, informacje o toku postępowania odwoławczego (wyszukiwanie po sygnaturze)	Dane jawne
ekomentarzpzp	Wydawnictwo — komentarz do Prawa zamówień publicznych (wyd. II), 13 działów, bibliografia, wyszukiwarka client-side	Dane jawne

Serwis	Role do testów
miniportal	**1 — zamawiający** • **zamawiający** — zakłada postępowania (formularz miniPortal → generuje ID Postępowania), zarządza postępowaniem, publikuje załączniki
bzp	**1 — zamawiający** Zamawiający wypełnia formularz publikacji ogłoszenia o zamówieniu publicznym.
aukcje	**2 — zamawiający + wykonawca** • **zamawiający** — zakłada i prowadzi aukcje, tworzy konta wykonawców, generuje i przesyła LOGIN/HASŁO, wysyła wiadomości, weryfikuje postąpienia. • **wykonawca** — składa postąpienia w **jednej** aukcji, wysyła wiadomości do zamawiającego; konto jednorazowe (jedna aukcja -brak dostępu do innych aukcji).
pzp.gov.pl	**2 — zamawiający + wykonawca**
espd	nie dotyczy (1 rola wg ankiety — osoba wypełniająca — bez uwierzytelnienia)
formularz	nie dotyczy
orzeczenia	nie dotyczy
wokanda	nie dotyczy
ekomentarzpzp	nie dotyczy

Wszystkie metody logowania oparte są o uwierzytelnienie za pomocą loginu i hasła. Brak specjalnych metod potwierdzania wykonania czynności.

Ad. 6.

Zamawiający usuwa wymaganie „Rekomendacje techniczne (konkretne zmiany w kodzie, konfiguracji, architekturze)” z sekcji „rezultat zadania”.

Ad.7.

Wymagane są testy manualne. Zakres obejmuje w szczególności analizę i wykorzystanie podatności, obejście logiki biznesowej oraz ocenę skuteczności zastosowanych kontroli. Skanery automatyczne (np. nuclei, Nikto, OWASP ZAP, Nmap) stanowią wyłącznie narzędzie wspomagające i nie zastępują testów manualnych. Wykonawca wskaże w raporcie, dla których ustaleń metoda manualna była niezbędna.

Dostarczanie i wdrażanie platformy skanującej nie stanowi zakresu niniejszego zamówienia.

Pytanie 6:

Dostęp fizyczny (Zadanie E)

1. Czy dobrze rozumiemy, że w teście ma na bieżąco uczestniczyć przedstawiciel Zamawiającego jako obserwator, który dodatkowo ma podejmować decyzje o możliwości gromadzenia dowodów (fotografie)?

   Odpowiedź:

   Zamawiający wskaże obserwatora testów fizycznych. Wykonawca musi powiadomić koordynatora o planowanych próbach i formach ich przeprowadzenia. Wykonawca ma obowiązek powiadomić obserwatora o uzyskaniu dostępu, a w celach dokumentacyjnych, przed wykonaniem zdjęć na potwierdzenie tego faktu – powiadomić i uzyskać zgodę koordynatora.

2. Czy ta ww. osoba będzie miała być obecna np. podczas prowadzenia ataku socjotechnicznego, prób odwrócenia uwagi ochrony itp.? Zwracamy uwagę, że to może powodować ograniczenia dla testu i jakości jego wyników.

   Odpowiedź:

   Zamawiający zmienia wymaganie:

   - Wykonawca prowadzi test w obecności obserwatora Zamawiającego.

   Na:

   - Wykonawca prowadzi test za wiedzą obserwatora Zamawiającego.

3. W jakim mieście/miastach i ilu budynkach mają odbywać się testy dostępu fizycznego?

   Odpowiedź:

   Warszawa, ul. Postępu 17A.

ZMIANA TREŚCI SWZ

Działając na podstawie art. 286 ust. 1 ustawy Pzp Zamawiający - Urząd Zamówień Publicznych dokonuje zmiany treści SWZ, zgodnie z poniższym zakresem:

I. W Załączniku nr 1 do SWZ- Opis przedmiotu zamówienia tj.:

1. **W pkt. 3.2. Lista serwisów www objętych testami.**

   Jest:

   Testom penetracyjnym podlega 10 aktywnych serwisów www w domenie *.uzp.gov.pl.

   # URL

   1. espd.uzp.gov.pl
   2. miniportal.uzp.gov.pl
   3. aukcje.uzp.gov.pl
   4. bzp.uzp.gov.pl
   5. pzp.gov.pl
   6. formularz.uzp.gov.pl
   7. orzeczenia.uzp.gov.pl
   8. wokanda.uzp.gov.pl
   9. elearning.uzp.gov.pl
   10. ekomentarzpzp.uzp.gov.pl

   Powinno być:

   Testom penetracyjnym podlega 9 aktywnych serwisów www w domenie *.uzp.gov.pl.

   # URL

   1. espd.uzp.gov.pl

2. miniportal.uzp.gov.pl
3. aukcje.uzp.gov.pl
4. bzp.uzp.gov.pl
5. pzp.gov.pl
6. formularz.uzp.gov.pl
7. orzeczenia.uzp.gov.pl
8. wokanda.uzp.gov.pl
9. ekomentarzpzp.uzp.gov.pl

2. **W pkt. 4.2. CZĘŚĆ II — Pen-testy 10 serwisów www (Zadanie B)**

Jest:

Rezultat zadania:

- Raport per serwis (10 raportów,) zawierający:
  - Streszczenie dla Kirownictwa (max 1 strona).
  - Scope i ograniczenia (tryb, ramy czasowe, konfiguracja).
  - Metodyki i narzędzia użyte (Burp, Nmap, sqlmap, nuclei, OWASP ZAP, custom scripts).
  - Znalezione podatności z klasyfikacją CVSS 3.1 / CVSS 4.0.
  - Szczegółowy opis każdej podatności (POC, request/response, reprodukcja).
  - Rekomendacje techniczne (konkretne zmiany w kodzie, konfiguracji, architekturze).
- Wspólny Executive Summary (max 5 stron, dla DDI i Sponsora).
- Sesja podsumowująca per serwis (30min/serwis) + sesja zbiorcza (4h).

Powinno być:

Rezultat zadania:

- Raport per serwis (10 raportów,) zawierający:
  - Streszczenie dla Kirownictwa (max 1 strona).
  - Scope i ograniczenia (tryb, ramy czasowe, konfiguracja).

- Metodyki i narzędzia użyte (Burp, Nmap, sqlmap, nuclei, OWASP ZAP, custom scripts).
- Znalezione podatności z klasyfikacją CVSS 3.1 / CVSS 4.0.
- Szczegółowy opis każdej podatności (POC, request/response, reproduktcja).

- Wspólny Executive Summary (max 5 stron, dla DDI i Sponsora).
- Sesja podsumowująca per serwis (30min/serwis) + sesja zbiorcza (4h).

3. **W pkt. 4.5. CZĘŚĆ V — Dostęp fizyczny (Zadanie E)**

Jest:

Warunki:

1. Wykonawca prowadzi test w obecności obserwatora Zamawiającego

Powinno być:

Warunki:

1. Wykonawca prowadzi test za wiedzą obserwatora Zamawiającego

II. W Specyfikacji Warunków Zamówienia

1. Zmiana nazwy/oznaczenia postępowania:

Jest:

„Testy bezpieczeństwa klasy APT dla usług internetowych i infrastruktury sieciowej oraz oprogramowanie do skanowania podatności ".

Powinno być:

„Testy bezpieczeństwa klasy APT dla usług internetowych i infrastruktury sieciowej ".

Zamawiający informuje, że w związku ze zmianą nazwy postępowania dokumenty i oświadczenia, które będą składane w niniejszym postępowaniu, zawierające dotychczasową nazwę postępowania, będą uznawane za prawidłowe w zakresie oznaczenia nazwy postępowania. Posłużenie się dotychczasową

nazwą nie wymaga poprawienia ani ponownego złożenia tych dokumentów lub oświadczeń.

Szymon Giderewicz; UZP

Elektronicznie podpisany przez Szymon Giderewicz; UZP
Data: 2026.11.23 16:07:10 +01'00'