

BL-VI.2600.2.2026.MZ

Gdańsk, 8 października 2026 r.

ZAPROSZENIE DO SKŁADANIA OFERT

Pomorski Urząd Wojewódzki w Gdańsku (dalej Urząd) ul. Okopowa 21/27, 80-810 Gdańsk zaprasza do złożenia oferty na przeprowadzenie zewnętrznych testów bezpieczeństwa infrastruktury IT dla Urzędu oraz trzech jednostek podległych Wojewodzie Pomorskiemu (dalej Jednostki):

1. Państwowej Straży Rybackiej w Gdańsku,
ul. Na Stoku 50, 80-874 Gdańsk, telefon: 58 302 07 25;
email: psr@psrgdansk.pl
2. Wojewódzkiego Inspektoratu Nadzoru Budowlanego w Gdańsku,
ul. Na Stoku 50, 80-874 Gdańsk; telefon 58 305-19-71, 58 305-19-74;
email: sekretariat @ gda.winb.gov.pl
3. Wojewódzkiego Inspektoratu Farmaceutycznego w Gdańsku.
Ul. Na Stoku 50, 80-874 Gdańsku; telefon: 58 300-00-92, 58 300-00-93;
email: sekretariat@wiif.gdansk.pl

Opis przedmiotu zamówienia

Przedmiotem zamówienia jest przeprowadzenie zewnętrznych testów penetracyjnych (typu Black Box) publicznie dostępnej infrastruktury sieciowej i teleinformatycznej Urzędu oraz Jednostek, mających na celu identyfikację i praktyczną weryfikację podatności bezpieczeństwa możliwych do wykorzystania przez podmiot nieposiadający żadnej wiedzy wewnętrznej o infrastrukturze Zamawiającego oraz Jednostek.

Celem zamówienia jest uzyskanie przez Urząd oraz Jednostki niezależnej, rzetelnej oceny odporności infrastruktury brzegowej na próby nieautoryzowanego dostępu z sieci Internet oraz uzyskanie konkretnych, priorytetyzowanych rekomendacji naprawczych.

Zamawiający może przekazać Wykonawcy zakres publicznych adresów IP należących do organizacji wyłącznie w celu jednoznacznego określenia zakresu testów.

Metodologia

Testy penetracyjne powinny zostać przeprowadzone zgodnie z uznanymi standardami, metodami i dobrymi praktykami w zakresie testowania bezpieczeństwa, odpowiednio do badanego obszaru, w szczególności w oparciu o:

- PTES (Penetration Testing Execution Standard) – jako metodykę prowadzenia testów penetracyjnych, obejmującą m.in. rozpoznanie, analizę podatności, kontrolowane wykorzystanie podatności oraz raportowanie;
- OWASP Web Security Testing Guide (OWASP WSTG) – w zakresie testowania bezpieczeństwa aplikacji internetowych, serwisów WWW, interfejsów API oraz innych usług dostępnych za pośrednictwem protokołów HTTP/HTTPS;
- NIST SP 800-115 (Technical Guide to Information Security Testing and Assessment) – w zakresie planowania, przeprowadzania i dokumentowania technicznych testów bezpieczeństwa infrastruktury teleinformatycznej;
- OSSTMM (Open Source Security Testing Methodology Manual) – w zakresie mającym zastosowanie do testowanej infrastruktury, systemów i usług sieciowych.

Zastosowanie powyższych metodyk nie może ograniczać przeprowadzonych prac wyłącznie do automatycznego skanowania podatności. Testy powinny obejmować również ręczną weryfikację wykrytych podatności oraz, w uzasadnionych przypadkach, kontrolowane próby ich wykorzystania w celu potwierdzenia rzeczywistego poziomu ryzyka, z zachowaniem warunków bezpieczeństwa i ciągłości działania systemów Zamawiającego.

Zamówienie obejmuje następujące elementy:

1. Rekonesans i rozpoznanie powierzchni ataku (OSINT / pasywne)

- 1) Identyfikacja publicznie dostępnej infrastruktury Zamawiającego;
- 2) analiza publicznie dostępnych informacji mogących ujawniać wykorzystywane technologie, systemy oraz wersje oprogramowania (m.in. rekordy DNS, certyfikaty, banery usług, metadane);
- 3) identyfikacja potencjalnie nieużywanych, zapomnianych lub niepotrzebnie udostępnionych usług i zasobów.

2. Skanowanie i identyfikacja usług (aktywne)

- 1) skanowanie portów TCP i UDP publicznych adresów IP Zamawiającego;
- 2) identyfikacja otwartych portów oraz nasłuchujących usług, w tym urządzeń brzegowych (firewalle, routery, bramy VPN, urządzenia bezpieczeństwa) oraz mechanizmów zdalnego dostępu (m.in. VPN, RDP, SSH);
- 3) fingerprinting usług, systemów oraz wersji oprogramowania i firmware w zakresie możliwym do ustalenia metodami Black Box;
- 4) wskazanie usług administracyjnych lub technicznych niepotrzebnie dostępnych z Internetu, w tym publicznie dostępnych interfejsów administracyjnych urządzeń.

3. Identyfikacja podatności

- 1) skanowanie podatności wykrytych usług, urządzeń, systemów oraz aplikacji webowych Zamawiającego;
- 2) identyfikacja znanych podatności CVE oraz podatności wynikających z nieaktualnych wersji oprogramowania lub firmware;
- 3) identyfikacja błędów konfiguracji możliwych do wykrycia z perspektywy Internetu;
- 4) ręczna weryfikacja istotnych wyników skanowania w celu ograniczenia wyników fałszywie pozytywnych;

- 5) określenie, czy wykryta podatność jest wyłącznie potencjalna, czy możliwa do praktycznego wykorzystania.

4. Kontrolowane testy eksploatacji (aktywne testy penetracyjne)

- 1) przeprowadzenie kontrolowanych prób wykorzystania wykrytych podatności w celu potwierdzenia możliwości uzyskania nieautoryzowanego dostępu;
- 2) weryfikacja rzeczywistego wpływu podatności na bezpieczeństwo infrastruktury;
- 3) próby wykorzystania podatności prowadzone w sposób minimalizujący ryzyko zakłócenia pracy systemów produkcyjnych;
- 4) testy nie mogą powodować celowego niszczenia, usuwania ani modyfikowania danych Zamawiającego.

5. Wymagania dodatkowe dla mechanizmów uwierzytelniania i zdalnego dostępu

- 1) identyfikacja typu i wersji wykorzystywanego rozwiązania VPN oraz weryfikacja znanych podatności dotyczących wykrytej wersji;
- 2) ocena mechanizmów uwierzytelniania i autoryzacji, w tym weryfikacja stosowania uwierzytelniania wieloskładnikowego (MFA), jeżeli mechanizm jest wykorzystywany;
- 3) weryfikacja poprawności konfiguracji certyfikatów i mechanizmów szyfrowania;
- 4) kontrolowana weryfikacja odporności mechanizmów uwierzytelniania na ataki typu brute-force / credential stuffing — wyłącznie po wcześniejszym pisemnym uzgodnieniu scenariusza, progów blokady kont i okna czasowego z Zamawiającym.

6. Weryfikacja mechanizmów ochronnych

- 1) sprawdzenie reakcji infrastruktury bezpieczeństwa na skanowanie portów oraz enumerację usług;
- 2) sprawdzenie reakcji na kontrolowane próby wykorzystania podatności (pkt 4-5);
- 3) weryfikacja, czy systemy IDS/IPS wykrywają, rejestrują lub blokują działania wykonywane podczas testów;
- 4) wskazanie działań, które nie zostały wykryte lub zablokowane przez zastosowane mechanizmy bezpieczeństwa.

7. Testy bezpieczeństwa serwisów WWW

- 1) identyfikacja wykorzystywanych technologii, systemów CMS, komponentów i oprogramowania serwerowego;
- 2) weryfikacja występowania znanych podatności oraz nieaktualnych komponentów;
- 3) weryfikacja błędów konfiguracji, niepotrzebnie udostępnionych plików, katalogów, kopii zapasowych oraz informacji technicznych;
- 4) weryfikacja odporności strony na typowe podatności WWW, odpowiednio do dostępnych funkcjonalności;
- 5) weryfikacja konfiguracji HTTP/HTTPS, certyfikatów TLS oraz podstawowych mechanizmów bezpieczeństwa;

- 6) ręczna weryfikacja istotnych podatności wykrytych za pomocą narzędzi automatycznych oraz, w uzasadnionych przypadkach, kontrolowane potwierdzenie możliwości ich wykorzystania;
- 7) testy powinny być prowadzone w sposób minimalizujący ryzyko zakłócenia działania strony oraz bez celowego niszczenia, usuwania lub trwałego modyfikowania danych Zamawiającego.

Warunki organizacyjne:

1. Minimalizacja wpływu na środowisko produkcyjne
 - testy muszą być prowadzone w sposób minimalizujący ryzyko zakłócenia działania infrastruktury;
 - działania mogące mieć wpływ na dostępność systemów wymagają wcześniejszego uzgodnienia z Zamawiającym;
 - w przypadku wystąpienia objawów destabilizacji usługi Wykonawca zobowiązany jest do przerywania danego scenariusza testowego;
 - testy nie mogą powodować niekontrolowanego przestoju systemów produkcyjnych.
2. Natychmiastowa eskalacja podatności krytycznych — w przypadku wykrycia w toku testów podatności o krytycznym wpływie na bezpieczeństwo (w szczególności umożliwiającej uzyskanie pełnego, nieautoryzowanego dostępu do systemu lub danych), Wykonawca zobowiązany jest niezwłocznie, nie później niż w ciągu 4 godzin, powiadomić telefonicznie i e-mailowo osobę wskazaną w pkt 9, przed ujęciem jej w raporcie końcowym.
3. Uzgadnianie scenariuszy testowych:
 - aktywne scenariusze ataków wymagają wcześniejszego uzgodnienia z Urzędem lub poszczególnymi jednostkami;
 - Zamawiający lub odpowiednio kierownicy Jednostek zatwierdzają działania mogące mieć wpływ na działanie infrastruktury;
 - terminy oraz okna czasowe dla działań podwyższonego ryzyka muszą zostać wcześniej ustalone.
4. Sposób prowadzenia testów
 - Wykonawca wykorzystuje własny sprzęt i oprogramowanie testowe;
 - testy prowadzone są spoza infrastruktury Zamawiającego oraz Jednostek;
 - bez zgody Zamawiającego zabronione jest trwałe instalowanie oprogramowania, agentów lub mechanizmów zapewniających utrzymanie dostępu;

- Wykonawca zobowiązany jest do zachowania poufności wszelkich informacji uzyskanych podczas realizacji testów w tym również danych osobowych, dla których administratorem jest Urząd lub poszczególne Jednostki.

Warunki jakie muszą spełniać Wykonawcy

1. Zespół realizujący testy musi posiadać udokumentowane doświadczenie w prowadzeniu testów penetracyjnych infrastruktury sieciowej.
2. Co najmniej 2 osoby w zespole musi posiadać aktualny certyfikat potwierdzający kwalifikacje w zakresie testów penetracyjnych (np. OSCP, OSCE, CREST CRT/CCT, CEH, GPEN lub równoważny).
3. Wykonawca przedstawi Zamawiającemu oraz poszczególnym Jednostkom, przed rozpoczęciem testów, listę adresów IP, z których będą prowadzone testy, w celu ewentualnego wyłączenia ich z automatycznych mechanizmów blokujących.

Raport końcowy

Raport końcowy sporządzony w języku polskim, w formie pisemnej i elektronicznej, zawiera co najmniej:

1. podsumowanie menedżerskie (streszczenie w języku niespecjalistycznym, przeznaczone dla kierownictwa Urzędu oraz Jednostek);
2. dokładny zakres wykonanych testów;
3. opis zastosowanej metodologii wraz ze wskazaniem zgodności ze standardem referencyjnym
4. wykaz wykrytych publicznie dostępnych portów i usług;
5. wykaz zidentyfikowanych podatności wraz ze wskazaniem urządzenia lub usługi, której dotyczy dana podatność;
6. opis techniczny każdej podatności;
7. identyfikator CVE, jeżeli dotyczy;
8. ocenę podatności według CVSS (wraz z wektorem CVSS), jeżeli ma zastosowanie;
9. klasyfikację podatności na krytyczne, wysokie, średnie i niskie;
10. informację, czy podatność została praktycznie potwierdzona, czy pozostaje wyłącznie potencjalna;
11. opis możliwego sposobu wykorzystania podatności;
12. dowody potwierdzające występowanie podatności (zrzuty ekranu, logi, wyniki narzędzi);
13. konkretne zalecenia dotyczące usunięcia lub ograniczenia podatności;
14. rekomendowany priorytet działań naprawczych.

Termin przekazania raportu końcowego: nie później niż 7 dni roboczych od zakończenia testów aktywnych odrębnie dla Urzędu oraz każdej z Jednostek.

11. Retest

Po usunięciu przez Zamawiającego podatności wskazanych w raporcie końcowym, Wykonawca przeprowadzi ponowną weryfikację (retest) potwierdzającą skuteczność wdrożonych działań naprawczych.

- 1) Zamawiający zgłosi gotowość do retestu w terminie do 1 miesiąca od usunięcia podatności przez Urząd oraz Jednostki.
- 2) Retest obejmuje wyłącznie podatności wskazane w raporcie końcowym jako wymagające weryfikacji.
- 3) Wyniki retestu zostaną przekazane w formie uzupełnienia (aneksu) do raportu końcowego, w terminie 5 dni roboczych od zakończenia retestu.

Dokumenty jakie powinni dostarczyć Wykonawcy

1. Wypełniona i podpisana oferta.
2. Wykaz usług zrealizowanych w okresie ostatnich 2 lat przed upływem terminu składania ofert (zał. nr 2), w tym dokumenty potwierdzające należyte wykonanie (listy referencyjne/protokoły odbioru bez uwag).
3. Inne: wykaz osób wyznaczonych do realizacji zamówienia, wraz z informacjami o ich kwalifikacjach zawodowych.

Kryteria oceny ofert

Przy wyborze najkorzystniejszej oferty Zamawiający będzie się kierował następującym kryterium:

- cena – 100% (100 pkt)
cena najniższa brutto

ocena punktowa = ----- x 100 pkt.
cena badana brutto

Za ofertę najkorzystniejszą zostanie uznana oferta, która uzyska największą ilość punktów biorąc pod uwagę kryterium ceny spośród ofert nieodrzuconych i spełniających wszystkie wymagania określone w niniejszym zaproszeniu.

Sposób przygotowania oferty

1. Wypełniony i podpisany przez osobę upoważnioną formularz oferty wraz z załącznikami **16 października 2026 r.** należy:
 - przesłać drogą elektroniczną na adres e-mail: bl@gdansk.uw.gov.pl,
 - lub złożyć w Punkcie Obsługi Klienta, Gdańsk, ul. Okopowa 21/27 (parter, wejście od ulicy Rzeźnickiej),
2. Wiadomość powinna być zatytułowana:
„Oferta na przeprowadzeni testów bezpieczeństwa infrastruktury sieciowej BL-VI.2600.2.2026”

Informacje dodatkowe

1. Termin wykonania przedmiotu zamówienia: po uzgodnieniu z zamawiającym, nie później niż **10 grudnia 2026 r.**
2. Termin związania ofertą: 30 dni od zakończenia terminu składania ofert.
3. Wykonawca może zwrócić się do Zamawiającego o wyjaśnienie dotyczące treści zaproszenia. Zamawiający może udzielić wyjaśnień, o ile uzna to za niezbędne

i w takiej sytuacji przekaże je do wiadomości potencjalnym Wykonawcom w formie w jakiej zostało ogłoszone Zaprośnienie do składania ofert.

4. W toku badania i oceny ofert Zamawiający może żądać od Wykonawców w wyznaczonym przez siebie czasie wyjaśnień dotyczących treści złożonych ofert oraz wezwać do uzupełnienia lub wyjaśnienia załączonych do oferty dokumentów. Zamawiający odrzuci ofertę Wykonawcy, który nie złożył wyjaśnień lub jeżeli dokonana ocena wyjaśnień potwierdza, że oferta jest niezgodna z wymaganiami określonymi w zaproszeniu.
 5. Zamawiający odrzuci ofertę:
 - a) złożoną po terminie;
 - b) złożoną przez Wykonawcę niespełniającego warunków udziału w postępowaniu;
 - c) niezgodną z treścią zapytania ofertowego;
 - d) Zamawiający nie przewiduje zmiany lub korekty oferty przez Wykonawcę po jej złożeniu przed upływem terminu składania ofert,
 - e) zawierające błędy nie będące oczywistymi omyłkami pisarskimi lub rachunkowymi;
 - f) jeżeli cena oferty przekracza kwotę, którą Zamawiający przeznaczył na realizację zamówienia;
 - g) złożoną przez Wykonawcę podlegającego wykluczeniu na podstawie przepisów art. 7 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego;
 - h) złożoną przez Wykonawcę uznanego za dostawcę wysokiego ryzyka, zgodnie z decyzją o której mowa w art. 67b ust. 15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, lub usługę ICT, lub proces ICT określone w tej decyzji.
 6. Wykonawcy ponoszą wszelkie koszty własne związane z przygotowaniem i złożeniem oferty, niezależnie od wyniku postępowania.
 7. Informację o wyborze najkorzystniejszej oferty Zamawiający przekaże jednocześnie wszystkim Wykonawcom, którzy złożyli oferty, w formie, w jakiej zostało ogłoszone Zaprośnienie do składania ofert.
 8. Oferta najkorzystniejsza zostanie wybrana spośród ofert niepodlegających odrzuceniu, na podstawie kryteriów oceny ofert. Wykonawca, którego oferta została wybrana jako najkorzystniejsza, zostanie poinformowany o formie realizacji sprawy.
 9. Osoba upoważniona do kontaktu z Wykonawcami:
- Michał Bielewski – e mail: michal.bielewski@gdansk.uw.gov.pl
Lub e-mail: bl@gdansk.uw.gov.pl,
10. Zamawiający zastrzega sobie prawo do unieważnienia postępowania jeżeli:
 - a. zaistnienia niemożliwej wcześniej do przewidzenia okoliczności prawnej, ekonomicznej;
 - b. nie zostanie złożona żadna oferta;

c. procedura wyboru oferty obarczona jest wadą;

Wykonawcy nie będą przysługiwały żadne roszczenia z tego tytułu.

11. Płatność za przedmiot umowy zostanie zrealizowany przelewem z konta

Zamawiającego w terminie 14 dni od daty otrzymania prawidłowo wystawionej faktury.

/dokument podpisany elektronicznie/

Załączniki:

- wzór formularza ofertowego (zał. nr 1),
- wzór formularza – wykaz usług zrealizowanych w okresie ostatnich 2 lat przed upływem terminu składania ofert (zał. nr 2),
- wzór umowy (zał. nr 3)

Wioletta Zawada

Dyrektor

Biura Logistyki

/dokument podpisany elektronicznie/