

OPIS PRZEDMIOTU ZAMÓWIENIA**Skan bezpieczeństwa aplikacji i systemów IT.**

L.p.	Wymaganie	Opis – wymagania minimalne
1	Przedmiot zamówienia	Przedmiotem zamówienia jest wykonanie jednorazowej usługi skanowania i analizy podatności bezpieczeństwa systemów, aplikacji oraz infrastruktury IT, wraz z kontrolowaną weryfikacją wykrytych podatności. Zamówienie nie obejmuje pełnego testu penetracyjnego ani działań destrukcyjnych, o ile Zamawiający nie wyrazi na określone czynności odrębnej zgody. Badanie obejmie wskazane przez Zamawiającego zasoby, w szczególności serwery, urządzenia sieciowe, systemy operacyjne, usługi sieciowe oraz wykorzystywane systemy i aplikacje. Na potrzeby przygotowania oferty Zamawiający określa zakres ilościowy zasobów objętych badaniem: 10 serwerów, 15 urządzeń sieciowych, 10 systemów/aplikacji oraz maksymalnie 100 adresów IP. Szczegółowa identyfikacja zasobów, w tym adresy IP, nazwy hostów i informacje o konfiguracji, zostanie przekazana Wykonawcy przed rozpoczęciem badania. Rezultatem wykonania zamówienia będzie raport zawierający opis przeprowadzonych czynności, zidentyfikowanych podatności i słabości, ich ocenę

		pod względem poziomu ryzyka oraz zalecenia dotyczące sposobu ich usunięcia lub ograniczenia.
2	Zakres badania	Badaniem zostaną objęte wskazane przez Zamawiającego elementy środowiska IT, w szczególności serwery, urządzenia sieciowe, systemy operacyjne, uruchomione usługi sieciowe, systemy informatyczne oraz wykorzystywane aplikacje. Zakres badania będzie obejmował zasoby pozostające w eksploatacji Zamawiającego i wskazane jako istotne z punktu widzenia bezpieczeństwa środowiska IT. Szczegółowa lista zasobów objętych badaniem, w tym adresów IP, nazw systemów, urządzeń i usług, zostanie przekazana wybranemu Wykonawcy przed rozpoczęciem realizacji usługi. Badanie musi być prowadzone wyłącznie w zakresie uzgodnionym z Zamawiającym i w sposób niepowodujący zakłóceń w funkcjonowaniu środowiska IT.
3	Zakres czynności	W ramach realizacji zamówienia Wykonawca przeprowadzi co najmniej następujące czynności: • identyfikację dostępnych hostów, otwartych portów, uruchomionych usług sieciowych oraz, identyfikację dostępnych hostów, otwartych portów, uruchomionych usług sieciowych oraz ich wersji, jeżeli ich ustalenie jest możliwe przy zastosowaniu standardowych, niedestrukcyjnych metod identyfikacji; przypadki, w których ustalenie wersji nie było możliwe, należy wskazać w raporcie;

		• identyfikację znanych podatności występujących w badanych systemach, urządzeniach i usługach, w szczególności podatności opisanych w publicznie dostępnych bazach, w tym CVE; • identyfikację nieaktualnych wersji oprogramowania, systemów operacyjnych, usług i komponentów oraz brakujących aktualizacji bezpieczeństwa; • identyfikację usług, protokołów lub mechanizmów, których wykorzystanie może zwiększać ryzyko nieuprawnionego dostępu lub naruszenia bezpieczeństwa; • identyfikację podstawowych błędów i słabości konfiguracji mających wpływ na poufność, integralność lub dostępność systemów i danych; • weryfikację wykrytych podatności i nieprawidłowości w zakresie niezbędnym do ograniczenia wyników fałszywie dodatnich; • przypisanie wykrytym podatnościom poziomu ryzyka oraz wskazanie zaleceń dotyczących ich usunięcia, ograniczenia lub dalszej weryfikacji.
4	Sposób realizacji	Usługa może być realizowana zdalnie lub w siedzibie Zamawiającego, w zależności od przyjętej przez Wykonawcę metodyki oraz uzgodnień organizacyjnych i technicznych z Zamawiającym. Skanowanie i testy mogą być wykonywane z wykorzystaniem specjalistycznych narzędzi automatycznych, uzupełnionych w razie potrzeby weryfikacją manualną wyników. W przypadku realizacji zdalnej Zamawiający zapewni uzgodniony z Wykonawcą sposób dostępu do zasobów objętych badaniem, z zachowaniem zasad bezpieczeństwa obowiązujących u Zamawiającego.

		Badanie należy prowadzić w sposób kontrolowany, ograniczający ryzyko wpływu na dostępność, wydajność lub poprawność działania systemów. Wykonawca zobowiązany jest uzgodnić z Zamawiającym termin i sposób prowadzenia czynności, w szczególności tych, które mogą powodować zwiększone obciążenie infrastruktury. Realizacja usługi nie może powodować celowego wyłączania usług, modyfikowania danych ani dokonywania trwałych zmian w konfiguracji systemów bez uprzedniej zgody Zamawiającego.
5	Ograniczenia testów	Wykonawca zobowiązany jest prowadzić badanie w sposób bezpieczny, kontrolowany i ograniczający ryzyko wpływu na ciągłość działania środowiska IT Zamawiającego. Bez uprzedniej, wyraźnej zgody Zamawiającego niedopuszczalne jest w szczególności: • wykonywanie testów typu DoS/DDoS oraz innych działań powodujących celowe przeciążenie systemów lub usług; • usuwanie, niszczenie, modyfikowanie lub szyfrowanie danych; • dokonywanie trwałych zmian w konfiguracji systemów, urządzeń lub usług; • instalowanie dodatkowego oprogramowania, agentów lub komponentów w środowisku Zamawiającego; • podejmowanie prób wykorzystania podatności w sposób mogący spowodować zatrzymanie, destabilizację lub utratę dostępności usług; • wykonywanie innych działań wykraczających poza uzgodniony z Zamawiającym zakres badania.

		W przypadku stwierdzenia podatności, której dalsza weryfikacja mogłaby wiązać się z ryzykiem zakłócenia pracy systemu, Wykonawca powinien przerwać dalsze czynności w tym zakresie i poinformować o tym Zamawiającego.
6	Klasyfikacja podatności	Wykryte podatności i słabości powinny zostać sklasyfikowane według poziomu ryzyka, z uwzględnieniem ich potencjalnego wpływu na poufność, integralność i dostępność systemów oraz danych Zamawiającego. Wykonawca powinien stosować co najmniej następujące poziomy klasyfikacji: • krytyczny, • wysoki, • średni, • niski, • informacyjny. Jeżeli dla danej podatności dostępna jest ocena w standardzie CVSS (Common Vulnerability Scoring System), Wykonawca powinien wskazać odpowiednią wartość punktową oraz, w miarę możliwości, wektor CVSS. W przypadku podatności lub nieprawidłowości, dla których nie jest możliwe zastosowanie CVSS, Wykonawca powinien określić poziom ryzyka na podstawie własnej oceny eksperckiej, z krótkim uzasadnieniem przyjętej klasyfikacji.
7	Raport z wykonania usługi	Po zakończeniu realizacji usługi Wykonawca prześle Zamawiającemu raport podsumowujący przeprowadzone badanie.

		Raport musi zawierać co najmniej: • opis zakresu wykonanych testów; • wskazanie zastosowanej metodyki oraz wykorzystanych narzędzi; • wykaz przebadanych systemów, urządzeń, usług i innych zasobów; • opis zidentyfikowanych podatności, słabości i nieprawidłowości; • przypisany poziom ryzyka dla poszczególnych ustaleń; • odniesienie do identyfikatorów CVE i wartości CVSS, jeżeli mają zastosowanie; • dowody potwierdzające ustalenia, np. wyniki skanowania, zrzuty ekranowe lub inne materiały techniczne, w zakresie niezbędnym do ich weryfikacji; • zalecenia dotyczące sposobu usunięcia, ograniczenia lub dalszej weryfikacji wykrytych podatności; • krótkie podsumowanie najistotniejszych zagrożeń wymagających priorytetowych działań. Raport powinien zostać przekazany w formie elektronicznej, w formacie np. PDF. Na żądanie Zamawiającego Wykonawca udzieli wyjaśnień dotyczących przedstawionych ustaleń i zaleceń.
8	Poufność i bezpieczeństwo informacji	Wykonawca zobowiązany jest do zachowania w poufności wszelkich informacji uzyskanych w związku z realizacją zamówienia, w szczególności informacji dotyczących architektury środowiska IT, adresacji, konfiguracji systemów i urządzeń, wykrytych podatności, danych uwierzytelniających oraz innych informacji mogących mieć znaczenie dla bezpieczeństwa Zamawiającego. Informacje i materiały pozyskane w trakcie realizacji usługi mogą być wykorzystywane wyłącznie w celu

		wykonania przedmiotu zamówienia i nie mogą być udostępniane osobom trzecim bez uprzedniej zgody Zamawiającego. Wykonawca zobowiązany jest stosować odpowiednie środki organizacyjne i techniczne zapewniające ochronę pozyskanych danych przed nieuprawnionym dostępem, utratą, ujawnieniem lub modyfikacją. Po zakończeniu realizacji usługi i przekazaniu Zamawiającemu wymaganej dokumentacji Wykonawca zobowiązany jest do bezpiecznego usunięcia kopii danych i materiałów pozyskanych podczas badania, chyba że ich dalsze przechowywanie wynika z obowiązujących przepisów prawa lub zostanie odrębnie uzgodnione z Zamawiającym. Raport, wyniki skanowania, dane dostępne oraz inne materiały zawierające informacje o podatnościach lub konfiguracji środowiska muszą być przechowywane i przekazywane w sposób zabezpieczony przed dostępem osób nieuprawnionych. Jeżeli materiały zostaną zabezpieczone hasłem lub innym sekretem, dane umożliwiające ich odszyfrowanie należy przekazać Zamawiającemu odrębnym kanałem komunikacji.
9	Wymagania wobec Wykonawcy	Wykonawca powinien posiadać doświadczenie w wykonywaniu testów bezpieczeństwa, skanów podatności lub analiz podatności systemów teleinformatycznych. Za spełnienie wymagania Zamawiający uzna wykazanie, że Wykonawca w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, należycie wykonał co najmniej jedną usługę obejmującą testy bezpieczeństwa,

		skanowanie podatności lub analizę podatności infrastruktury albo systemów IT. Na potwierdzenie spełnienia wymagania Wykonawca przedstawi: • wykaz wykonanych usług, zawierający co najmniej nazwę lub przedmiot usługi, podmiot, na rzecz którego została wykonana, oraz datę realizacji; • dokument potwierdzający należyte wykonanie wskazanej usługi, np. referencję, protokół odbioru, poświadczenie odbiorcy usługi lub inny równoważny dokument. Zamawiający dopuszcza wykazanie doświadczenia zdobytego zarówno przy realizacji usług na rzecz podmiotów publicznych, jak i prywatnych. Wymaganie ma na celu potwierdzenie, że Wykonawca posiada praktyczne doświadczenie niezbędne do prawidłowego i bezpiecznego przeprowadzenia badania podatności środowiska IT Zamawiającego.
10	Odbiór usługi	Podstawą odbioru przedmiotu zamówienia będzie przekazanie Zamawiającemu kompletnego raportu z wykonania usługi, zgodnego z wymaganiami określonymi w OPZ. Zamawiający dokona weryfikacji raportu pod kątem kompletności, zgodności z zakresem zamówienia oraz czytelności przedstawionych ustaleń i zaleceń. Na żądanie Zamawiającego Wykonawca zobowiązany będzie również do omówienia zidentyfikowanych podatności, poziomu ich ryzyka

		oraz zaleceń dotyczących sposobu ich usunięcia lub ograniczenia. Odbiór usługi nastąpi po zaakceptowaniu raportu przez Zamawiającego i zostanie potwierdzony protokołem odbioru podpisanym przez upoważnionych przedstawicieli Stron. W przypadku stwierdzenia braków, nieścisłości lub konieczności doprecyzowania wyników badania Wykonawca zobowiązany będzie do ich wyjaśnienia lub uzupełnienia w terminie nie dłuższym niż 3 dni robocze od dnia przekazania uwag przez Zamawiającego, chyba że Zamawiający wyrazi zgodę na inny termin.
11	Termin wykonania	Do 15 listopada 2026 r.

