

Załącznik nr 1.2 do zapytania ofertowego

OPIS PRZEDMIOTU ZAMÓWIENIA

1. Audyt końcowy

AUDYT KOŃCOWY W OBSZARZE CYBERBEZPIECZEŃSTWA musi spełniać wymagania określone w Załącznik nr 4 – Zakres realizacji przedsięwzięcia do wyboru przedsięwzięcia (tryb konkurencyjny – I nabór – Inwestycja D.1.1.2) AUDYT KOŃCOWY W OBSZARZE CYBERBEZPIECZEŃSTWA

Produkt: ANKIETA WERYFIKACJI DOJRZAŁOŚCI POD KĄTEM CYBERBEZPIECZEŃSTWA

2. Testy penetracyjne

Usługa musi spełniać wymagania określone w Załącznik nr 4 – Zakres realizacji przedsięwzięcia do wyboru przedsięwzięcia (tryb konkurencyjny – I nabór – Inwestycja D.1.1.2) USŁUGI ZARZĄDZANE BEZPIECZEŃSTWA 2) Usługi w zakresie testów bezpieczeństwa) oraz opisane w punktach poniżej

Testy penetracyjne zostaną wykonane po uzgodnieniu z Zamawiającym w terminie nie później niż 14 lipca 2026 r.

W ramach niniejszego postępowania Wykonawca zobowiązuje się wykonać retesty w okresie 12 i 24 miesięcy od przeprowadzenia pierwszych testów penetracyjnych w terminie uzgodnionym z Zamawiającym.

Minimalny zakres testów penetracyjnych (przy czym przez testy penetracyjne należy rozumieć przeprowadzenie testów mających na celu wykrycie nieznanych podatności - skanowanie pod kątem znanych podatności narzędziami typu Nessus, BurpSuite, Rapid7 i inne podobne (komercyjne) wykonanych przez pentestera obejmuje przynajmniej:

2.1. Zewnętrzne testy penetracyjne infrastruktury informatycznej

- Analiza topologii brzegu sieci: Ocena struktury i zabezpieczeń brzegów sieci oddzielających wewnętrzne zasoby od Internetu.
- Weryfikacja mechanizmów ochronnych: Przegląd i testowanie zabezpieczeń zastosowanych na granicy sieci, w tym firewalli, systemów wykrywania i zapobiegania intruzom (IDS/IPS) oraz innych mechanizmów ochronnych.

Załącznik nr 1.2 do zapytania ofertowego

- Wykrywanie usług sieciowych udostępnianych do Internetu: Skanowanie portów i usług dostępnych publicznie w celu identyfikacji potencjalnych wejść dla atakujących.
- Detekcja wersji oraz typu oprogramowania dostępnego z sieci Internet: Identyfikacja wersji oprogramowania serwerowego dostępnego publicznie, co może pomóc w wykryciu znanych podatności.
- Exploatacja dostępnych urządzeń oraz usług wystawionych do sieci Internet: Próby eksploatacji zidentyfikowanych podatności w celu oceny ryzyka.
- Przedstawienie rozwiązań zwiększających bezpieczeństwo styku sieci lokalnej z siecią Internet: Rekomendacje dotyczące wzmocnienia zabezpieczeń brzegu sieci.

2.2. Wewnętrzne testy penetracyjne infrastruktury informatycznej

- Analiza topologii sieci LAN: Ocena struktury i zabezpieczeń wewnętrznej sieci LAN.
- Weryfikacja mechanizmów ochronnych w sieci: Analiza i testowanie wewnętrznych zabezpieczeń sieciowych, w tym segregacji sieci i izolacji urządzeń.
- Analiza komunikacji sieciowej: Monitoring i analiza ruchu sieciowego w poszukiwaniu nietypowych wzorców mogących wskazywać na naruszenia bezpieczeństwa.
- Skanowanie portów TCP/UDP i wykrywanie usług sieciowych: Identyfikacja usług i aplikacji działających w sieci wewnętrznej.
- Skanowanie hostów aktywnych w sieci: Lokalizacja i analiza aktywnych urządzeń w sieci wewnętrznej.
- Exploatacja dostępnych urządzeń oraz usług w sieci LAN: Próby eksploatacji znalezionych podatności w celu oceny wewnętrznych ryzyk bezpieczeństwa.
- Proces tworzenia i odtwarzania kopii zapasowych: Ocena procedur backupu i możliwości odzyskania danych.
- Monitorowanie ruchu sieciowego: Sprawdzenie systemów monitorowania w celu wykrywania podejrzanych aktywności i naruszeń bezpieczeństwa.
- Przedstawienie rozwiązań zwiększających bezpieczeństwo sieci LAN: Rekomendacje dotyczące poprawy zabezpieczeń wewnętrznej sieci LAN.

2.3. Audyt serwisów WWW

- Wersje serwera HTTP i systemu CMS: Sprawdzenie aktualności i bezpieczeństwa zainstalowanych wersji, z naciskiem na znane podatności.
- Bezpieczeństwo komunikacji: Ocena aktualności certyfikatów X.509, wersji protokołu TLS i stosowanych algorytmów kryptograficznych, zapewniająca poufność i integralność przesyłanych danych.

Załącznik nr 1.2 do zapytania ofertowego

2.4. Raport z testów i audytu

- Opis zakresu przeprowadzonych prac audytowych: Szczegółowe przedstawienie metodologii, narzędzi i zakresu wykonanych testów i analiz.
- Analiza informacji zebranych podczas audytów: Przedstawienie i omówienie wyników testów, w tym zidentyfikowanych podatności i potencjalnych ryzyk.
- Wnioski i zalecenia dotyczące rozwiązań występujących problemów: Opracowanie propozycji działań naprawczych, zaleceń dotyczących poprawy bezpieczeństwa oraz strategii minimalizacji ryzyka.
- Weryfikacja aspektów technicznych: Szczegółowa analiza zabezpieczeń serwisów WWW, lokalnych sieci teleinformatycznych oraz połączenia z siecią Internet, wraz z zaleceniami dotyczącymi poprawy i utrzymania wysokiego poziomu bezpieczeństwa.

Audyt ma zostać przeprowadzony w siedzibach: Akademickiego Centrum Zdrowia w Mikołowie sp. z o.o.

Inne istotne warunki zamówienia:

Informacje:	Ilość/szt.: Zamawiający
Ilość lokalizacji działalności organizacji	6
Ilość serwerów fizycznych	10
Ilość serwerów wirtualnych	60
Ilość zewnętrznych adresów IP	2
1. stacji roboczych	1. 160
2. drukarki sieciowe	2. 50
3. routery	3. 0
4. switch-e	4. 22
5. modem	5. 0
6. access point	6. 20
7. UTM	7. 2

.....
(podpisy osób upoważnionych
do reprezentowania wykonawcy)