Rawicz dnia 05.03.2026r.

NLO-3822-01/TP/26

Dotyczy: postępowania o udzielenie zamówienia publicznego pod nazwą**: wykonanie audytu cyberbezpieczeństwa oraz zakup szkoleń w ramach projektu pn.: „Wdrożenie e-usług w Szpitalu Powiatowym w Rawiczu Sp. z o.o.”**

Do wiadomości
Wszyscy Wykonawcy

Szpital Powiatowy w Rawiczu Sp. z o.o. w odpowiedzi na zapytania Wykonawców udziela następujących wyjaśnień:

Pytanie 1
Zakres skanowania podatności
Prosimy o wskazanie przybliżonej liczby adresów IP oraz hostów (serwerów, stacji roboczych, urządzeń sieciowych), które mają zostać objęte testami podatności i analizą konfiguracji, o których mowa w Załączniku nr 1 (Analiza infrastruktury i testy podatności).
Odpowiedź: Liczba hostów 350 szt.

Pytanie nr 2
Liczba serwerów
Prosimy o podanie liczby serwerów fizycznych, maszyn wirtualnych oraz instancji systemów operacyjnych, które mają zostać objęte analizą w ramach audytu.
Odpowiedź Liczba serwerów -7 sztuk; liczba maszyn wirtualnych – 60 szt.

Pytanie nr 3
Urządzenia sieciowe i segmentacja
Prosimy o wskazanie liczby urządzeń sieciowych (firewalle, routery, switche, access pointy) oraz liczby segmentów / VLAN-ów, które wchodzą w zakres infrastruktury wymienionej w Załączniku nr 1.
Odpowiedź: Liczba urządzeń sieciowych (routery, ap, switch, itp.) - 100 szt. W zakresie 5 Vlanów z maską 24.

Pytanie nr 4
Systemy HIS/ERP i systemy krytyczne
Prosimy o podanie listy systemów HIS/ERP oraz innych systemów krytycznych, które Zamawiający przewiduje do objęcia audytem, wraz z informacją o liczbie modułów lub instancji.
Odpowiedź: HIS Eskulap firmy Nexus - 2 instalacje (NG, NT); 8 modułów; ERP firmy Simple – 1 instalacja; 6 modułów, CRM Itcube – 1 instalacja; 3 moduły.

Pytanie nr 5
Scenariusze ataków
Prosimy o doprecyzowanie, jaka jest oczekiwana liczba scenariuszy ataków, które mają zostać przeanalizowane w ramach „analizy odporności na wybrane scenariusze ataków”, oraz czy Zamawiający przewiduje konkretne typy scenariuszy (np. eskalacja uprawnień, ataki na AD, testy konfiguracji usług).
Odpowiedź: Atak phishingowy na pracownika; socjotechnika; Exploit podatności serwera; atak na AD.

Podpisany elektronicznie przez
Renata Pazoła
05.03.2026
7:59:11 +01'00'