Wojewódzki Szpital Specjalistyczny nr 4 w Bytomiu
Aleja Legionów 10, 41-902 Bytom, NIP 626-25-10-567, REGON 000296271
tel. +48 323 964 500, e-mail: szpital@szpital4.bytom.pl, www.wss4.pl

Załącznik nr 2A do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

1. DZIAŁANIE

Projekt	382	Fundusz Przeciwdziałania COVID-19 działań w celu do podniesienia poziomu bezpieczeństwa systemów teleinformatycznych WSS4 w Bytomiu
Postępowanie	104	Wykonanie dokumentacji zarządzania cyberbezpiczeństwem wraz z przeprowadzeniem testów penetracyjnych
Element	101	Opis przedmiotu zamówienia
Wersja	1	2022-10-06

2. WYMAGANIA

Przeprowadzenie testów penetracyjnych w szczególności w zakresie:

- weryfikacja i analiza bezpieczeństwa dostępu do wewnętrznej infrastruktury sieciowej IT,
- weryfikacja systemów oraz zasad zarządzania i monitorowania infrastruktury IT,
- weryfikacja środków technicznych kontroli dostępu do systemów operacyjnych, w tym zabezpieczeń przed możliwością nieautoryzowanych instalacji oprogramowania,
- weryfikacja i analiza danych przetwarzanych przez systemy logowania,
- weryfikacja podatności logicznych środków kontroli dostępu wewnątrz infrastruktury IT
- weryfikacja zabezpieczenia poufności i integralności przetwarzania danych w systemach bazodanowych, w szczególności danych osobowych,
- weryfikacja zasad identyfikacji oraz autentykacji stosowanych w mechanizmach autoryzacji dostępu do zasobów IT,
- weryfikacja podatności systemów i sieci na ataki przy wykorzystaniu znanych podatności
- weryfikacja na podstawie otwartości portów, błędów związanych z autoryzacją dostępu zdalnego do zasobów IT i ocena związanych z tym ryzykiem,
- rozpoznanie i ocena mechanizmów zarządzania aktualizacjami - w tym obecność systemów automatyzujących propagację poprawek bezpieczeństwa,
- weryfikacja zabezpieczeń poufności przesyłu danych przetwarzanych na udostępnionych zasobach plikowych,
- weryfikacja obecności domyślnych i słabych kont użytkowników oraz haseł,
- analiza i ocena dodatkowych systemów bezpieczeństwa tj. dodatkowego oprogramowania antywirusowego, oprogramowania weryfikującego integralność systemów i gwarantującego audytowalność infrastruktury IT,
- weryfikacja i analiza jakościowa odporności infrastruktury IT na bez autoryzacyjne
- weryfikacja podatności serwisów DNS,
- weryfikacja podatności systemów i sieci na ataki takie jak sniffing, spoofing, man-in- the-middle,
- weryfikacja bez autoryzacyjnego dostępu do informacji o rodzaju i wersji wykorzystywanego oprogramowania systemowego i usługowego,
- weryfikacja podatności hostów na ataki w warstwie systemowej (przy wykorzystaniu exploitów),
- weryfikacja podatności hostów na możliwość uzyskania nieautoryzowanego dostępu do zasobów plikowych,
- weryfikacja bez autoryzacyjnej dostępności do danych o czasie pracy krytycznych systemów,
- inwentaryzacja urządzeń IoT wraz z ich lokalizacją
- badanie znanych podatności w wykorzystywanych urządzeniach IoT
- detekcja elementów Shadow IT wraz z lokalizacją
- analiza bezpieczeństwa sieci bezprzewodowych
- analiza interferencji fal sieci bezprzewodowych
- analiza statusu oraz wersji oprogramowania urządzeń sieciowych typu przełącznik (switch) oraz router i AP
- weryfikacja procesu tworzenia kopii zapasowych
- weryfikacja procesu odtwarzania zewnętrznych kopii zapasowych

Przeprowadzenie testów penetracyjnych informacji oraz danych cyfrowych w udostępnionych zewnętrznie w sieci Internet w tym:

- weryfikacja uprawnień i dostępów do zasobów w chmurze
- weryfikacja typu uwierzytelnienia (2FA / MTA)
- analiza bezpieczeństwa serwerów pocztowych oraz przesyłanych wiadomości e-mail
- pozyskanie informacji o ukrytych zasobach poprzez techniki OSINT (biały wywiad)
- test ataków na webaplikację (SQL injection, XSS, CSRF, Command Injection, Directory Traversal)
- próby obejścia systemów proxy poprzez wykorzystanie błędnych konfiguracji web serwera (Incapsula, Cloudflare)