Kraków, dnia 11.03.2024 r.

Dotyczy: usługa przeprowadzenia audytu bezpieczeństwa systemu informatycznego, bezpieczeństwa informacji w narzędziu e-KSSiP wraz ze środowiskiem sieciowym hostingodawcy oraz sporządzenie raportu.

W dniu 6.03.2024 roku do Zamawiającego wpłynęły pytania dotyczące treści zapytania ofertowego. Zamawiający udziela następujących odpowiedzi.

Pytanie 1:

Lista metod logowania/uwierzytelniania: (np. ID, hasło, certyfikat, token, kod sms), które mają zostać objęte testami.

Odpowiedź zamawiającego:

ID, hasło

Pytanie 2:

Lista metod autoryzacji operacji (jeśli występuje): (np. certyfikat, token (sprzętowy), kod sms, urządzenia HSM (Hardware Security Module, inne - proszę podać jakie), które mają zostać objęte testami.

Odpowiedź zamawiającego:

Brak metod autoryzacji

Pytanie 3:

Liczba ról, które mają podlegać testom (np. gość, użytkownik zwykły, użytkownik rozszerzony, operator, administrator, itp.) wraz z krótkim opisem (np. administrator – zarządza prawami dostępu innych użytkowników), które mają zostać objęte testami,

Odpowiedź zamawiającego:

- administrator (zarządza parami dostępu),
- koordynator merytoryczny (zarządza zapisami na szkolenia),
- koordynator planów zjazdów (zarządza szkoleniami dla aplikantów),

- użytkownik zwykły, konto tymczasowe (konto z maksymalnie ograniczonymi uprawnieniami)

Pytanie 4:

Sumaryczna, orientacyjna liczba pól we wszystkich formularzach, które mają zostać objęte testami.

Odpowiedź zamawiającego:

Około 20 – panel logowania oraz edycja panelu użytkownika

Pytanie 5, 6:

Zakres adresacji IP objętych testami. Orientacyjna liczba aktywnych IP w ramach adresacji objętej testami.

Odpowiedź zamawiającego:

3 zewnętrzne IP i 10 wewnętrzych

Pytanie 7:

W jakim modelu mają być wykonane testy:

Black-box – brak jakichkolwiek informacji ze strony Klienta

Gray-box – Klient przekaże informacje na temat wykorzystywanych technologii / reguł content switchingu, itp.

Odpowiedź zamawiającego:

Gray-box

Pytanie 8, 9:

Jakie testy należy przeprowadzić w odniesieniu do infrastruktury: skany pod kątem otwartych portów TCP (65 tys. portów), skany pod kątem otwartych portów UDP (1 000 najbardziej popularnych)

Odpowiedź zamawiającego:

TCP (65 tys. portów) i UDP (1 000 najbardziej popularnych)

Pytanie 10:

Zewnętrzne testy podatności black-box komponentów infrastruktury (bez logowania się do komponentów)

Odpowiedź zamawiającego:

Nie

Pytanie 11:

Zewnętrzne testy podatności gray-box komponentów infrastruktury (z logowaniem się do komponentów) – wymagany jest dostęp administratorski read only

Odpowiedź zamawiającego:

Tak

Pytanie 12:

Weryfikacja konfiguracji bezpieczeństwa komponentów – wymagany jest dostęp administratorski read only.

Odpowiedź zamawiającego:

Tak

Zastępca kierownika Działu Informatycznego
inż. Bartosz Kuźma