Załącznik nr 1 do Zapytania ofertowego

nr BOZ-WZ.25.3.2024.BA

OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ)

Przedmiotem zamówienia jest przeprowadzenie testów bezpieczeństwa infrastruktury teleinformatycznej Zamawiającego zakończonych opracowaniem i dostarczeniem raportu technicznego z przeprowadzonych testów oraz podsumowaniem wyników analiz i testów dla kierownictwa.

I. Wymagania ogólne

1. Testy penetracyjne muszą być przeprowadzone zgodnie z jedną z poniższych metodologii:
   a) OSSTM - Open Source Security Testing Methodology Manual;
   b) NIST SP 800-115 - Technical Guide to Information Security Testing;
   c) PTES - Penetration Test Execution Standard;
   d) OWASP Testing Guide.

II. Zakres testów bezpieczeństwa sieci i urządzeń sieciowych

1. Zakres testów z zewnątrz:
   a) Analiza topologii sieci Zamawiającego z wykorzystaniem profesjonalnego oprogramowania przeznaczonego do przeprowadzania testów i analizy bezpieczeństwa.
   b) Analiza podatności z wykorzystaniem profesjonalnego oprogramowania przeznaczonego do przeprowadzania testów bezpieczeństwa.
   c) Skanowanie portów TCP / UDP.
   d) Skanowanie hostów aktywnych w danej podsieci.
   e) Próba detekcji typu oraz wersji usług sieciowych działających w systemie.
   f) Skanowanie podatności w wykrytych usługach sieciowych.
   g) Próba detekcji wersji oraz typu oprogramowania systemowego zainstalowanego na urządzeniu.
   h) Próba lokalizacji znanych podatności w danych wersjach oprogramowania, po udanej detekcji wersji oprogramowania systemowego.
   i) Próba generacji pakietów o dużym rozmiarze (np. powiększonych pakietów ICMP echo).

j) Testy wskazanych przez Zamawiającego urządzeń sieciowych (np.: serwer, firewall, punkt dostępowy sieci bezprzewodowej, switch).
k) Próba nieautoryzowanego dostępu do urządzeń sieciowych i przejęcia kontroli.
l) Testy szczelności VLAN.
m) Testy uwierzytelniania 802.1x.
n) Lokalizacja podatności w udostępnionych aplikacjach webowych (np. próby ominięcia ekranów logowania, kradzież danych z aplikacji).
o) Próba przejęcia kontroli nad co najmniej jednym z systemów serwerowych (Windows oraz Linux) i klienckich – próba eskalacji ataku na pozostałe maszyny, systemy w sieci LAN Zamawiającego.
p) Weryfikacja podstawowych zasad bezpieczeństwa na min. 10 i maks. 50 stacjach roboczych (udostępnione usługi, poziom dostępu zapewniany dla użytkowników, dostępność oprogramowania klasy antywirus/antymalware, sposoby aktualizacji systemu, konfiguracja lokalnego firewall, itp) wskazanych przez Zamawiającego.
q) Weryfikacja podstawowych zasad bezpieczeństwa na min. 10 i maks. 30 serwerach dostępnych dla użytkowników (udostępnione usługi, poziom dostępu zapewniany dla użytkowników, dostępność oprogramowania klasy antywirus/antymalware, sposoby aktualizacji systemu, konfiguracja lokalnego firewall, itp) wskazanych przez Zamawiającego.
r) Próba uzyskania nieautoryzowanego dostępu do Internetu z sieci LAN.

2. Zakres testów z wewnątrz:
a) Skanowanie portów TCP / UDP.
b) Skanowanie hostów aktywnych w podsieci Zamawiającego.
c) Próba detekcji typu oraz wersji usług sieciowych działających w systemie.
d) Skanowanie podatności w wykrytych usługach sieciowych.
e) Próba detekcji wersji oraz typu oprogramowania systemowego zainstalowanego na urządzeniu.
f) Próba lokalizacji znanych podatności w danych wersjach oprogramowania, po udanej detekcji wersji oprogramowania systemowego.
g) Próba generacji pakietów o dużym rozmiarze (np. powiększonych pakietów ICMP echo).
h) Testy wskazanych przez Zamawiającego urządzeń sieciowych (np.: serwer, firewall).

i) Próba nieautoryzowanego dostępu do urządzeń sieciowych i przejęcia kontroli.
j) Lokalizacja podatności w udostępnionych aplikacjach webowych (np. próby ominięcia ekranów logowania, kradzież danych z aplikacji).
k) Próba przejęcia kontroli nad co najmniej jednym z systemów serwerowych Windows oraz Linux – próba eskalacji ataku na pozostałe maszyny, systemy w sieci LAN Zamawiającego.
l) Próba przełamania zabezpieczeń VPN.
m) Testy urządzeń sieciowych znajdujących się w sieci wewnętrznej (LAN) mogą być realizowane zdalnie.

III. Zakres testów bezpieczeństwa sieci bezprzewodowej WiFi

1. Wykrycie sieci bezprzewodowych (802.11a, 802.11b, 802.11g) w kilku wybranych miejscach w siedzibie Zamawiającego.
2. Określenie typu zabezpieczeń wykrytych sieci.
3. W przypadku wykrycia sieci bezprzewodowej – próba złamania zabezpieczeń i uzyskania dostępu do sieci.
4. Weryfikacja trybu ogłaszania SSID oraz wartości SSID.
5. Próba wykrycia producenta urządzenia Access Point.
6. Określenie wykorzystanych mechanizmów uwierzytelniania stron (na podstawie przekazanych przez Zamawiającego danych dostępowych).
7. Sprawdzenie wykorzystania mechanizmów uwierzytelniania oferowanych przez standard 802.1X oraz próba przełamania lub obejścia tych zabezpieczeń.

IV. Zakres testów aplikacji webowych

1. Testami powinny zostać objęte poniższe aplikacje:
   a) Komunikator MS.
   b) System zarządzania urządzeniami mobilnymi (MDM).
   c) System udostępniania plików.
   d) System pocztowy.
   e) System ochrony poczty elektronicznej
   f) System kontroli sesji zdalnych.
2. Recenzja architektury logicznej zawierająca ocenę zastosowanej architektury aplikacji, jej skalowalność, rozwojowość, koszty, bezpieczeństwo, itp.
3. Podstawowy audyt i testy infrastruktury oraz sieci składający się co najmniej z:
   a) Identyfikacji słabych punktów aplikacji.

   b) Weryfikacji podatności sieci na zagrożenia związane z podszywaniem się pod elementy infrastruktury teleinformatycznej.
   c) Weryfikacji podatności sieci na zagrożenia związane z umyślnymi zakłóceniami.
   d) Testy segmentacji sieciowej.
   e) Sprawdzenia odporności sieci na ataki związane z przeciążeniem zasobów sieciowych.
   f) Weryfikacji sposobu przechowywania przez aplikację danych uwierzytelniających.
4. Zastosowanie technik Google Hacking.
5. Wykorzystanie manualnych oraz automatycznych metod prowadzenia testów bezpieczeństwa (np. OWASP ZAP, Burp Suite Professional, Nessus) z zastosowaniem podejścia black box i gray box.
6. Detekcja błędów aplikacyjnych (kilka testów na każdą z poniższych klas):
   a) SQL injection.
   b) XSS (Cross Site Scripting) – błędy typu reflected oraz stored.
   c) Detekcja zabezpieczeń na podatność CSRF (Cross Site Request Forgery).
   d) Broken Authentication and Session Management (badanie losowości ID sesji, próba detekcji składni nazywania cookie sesyjnego, sprawdzenie bezpieczeństwa budowy formularza logowania).
   e) Authorization Bypass (próby dostępu do zasobów bez uwierzytelnienia użytkownika).
   f) Code Execution (próby wykonania wrogiego kodu na serwerze).
   g) Information Leakage (próby detekcji wycieku istotnych informacji – technicznych i biznesowych – z serwera).
   h) Insecure Communications (np. dostęp do istotnych danych – np. konta administracyjnego bez szyfrowania).
   i) Source Disclosure (próby prowadzące do ujawnienia kodów źródłowych wykorzystanego oprogramowania).
   j) Path Traversal.
   k) Open Redirection.
   l) Denial of Service (DoS).
   m) File Inclusion.
   n) Response Splitting.
7. Testy web serwera obejmujące m.in.:
   a) Bezpieczeństwo skonfigurowanego mechanizmu SSL.
   b) Dostępność komunikatów o błędach.
   c) Analiza podatności występujących w zainstalowanej wersji serwera.

d) Dostępność nadmiarowych metod HTTP.

Testy

V. Zakres testów socjotechnicznych

1. Wykonanie min. 5 telefonów nakłaniających do zainstalowania złośliwego oprogramowania.
2. Wykonanie min. 5 telefonów nakłaniających do przekazania dostępu do komputera/telefonu służbowego.
3. Realizacja dwóch kampanii mailingowych (2xok.200 odbiorców). Kampania nakłaniająca do podania hasła dostępowego do jednego z systemów Zamawiającego oraz nakłaniająca do zainstalowania złośliwego oprogramowania.
4. Próba fizycznego, nieautoryzowanego wejścia na powierzchnię biurową Zamawiającego.
5. Próba nakłaniania pracowników do przekazania dostępu do komputera/telefonu służbowego – min. 5 prób.
6. Próba nakłonienia pracownika do uruchomienia oprogramowania dostarczonego na pendrive – min. 5 prób.

VI. Zakres dokumentacji z przeprowadzonych testów

1. Raport techniczny z przeprowadzonych działań w zakresie, o którym mowa w rozdz. I-V OPZ musi zwierać co najmniej:
   a) Zakres wykonywanych działań
   b) Metodologię testów
   c) Klasyfikację zasobów objętych zakresem analiz i testów
   d) Podsumowanie działań
   e) Podsumowanie wyników analiz i testów
   f) Metodologię oceny ryzyka
   g) Opis wszystkich zidentyfikowanych w ramach testów podatności wraz z rekomendacją sposobu ich usunięcia oraz zwiększenia poziomu bezpieczeństwa systemów Zamawiającego.
   h) Szczegóły techniczne podatności wraz z tzw. proof of concept (PoC) oraz opisem kroków, które należy wykonać, by odtworzyć zgłaszany błąd.
   i) Wykonawca dostarczy raport techniczny z przeprowadzonych testów w wersji elektronicznej w formacie pdf oraz edytowalnym docx.
2. Podsumowanie wyników analiz i testów w zakresie, o którym mowa w rozdz. I-V OPZ dla kierownictwa. Wykonawca dostarczy podsumowanie

wyników analiz i testów dla kierownictwa w wersji elektronicznej w formacie pdf oraz edytowalnym docx.