Opis Przedmiotu Zamówienia (OPZ)

Przedmiotem zamówienia jest przeprowadzenie testów penetracyjnych w siedzibach Głównego Inspektoratu Transportu Drogowego

1. Wprowadzenie

Celem zamówienia jest przeprowadzenie testów penetracyjnych infrastruktury IT w Głównym Inspektoracie Transportu Drogowego. Testy mają na celu identyfikację potencjalnych słabości, luk bezpieczeństwa oraz możliwości nadużyć, które mogą być wykorzystane przez atakujących. Zamówienie obejmuje przeprowadzenie testów penetracyjnych zarówno aplikacji webowych, jak i infrastruktury sieciowej oraz serwerowej.

2. Zakres Prac

2.1. Aplikacje Webowe

2.1.1. Testy penetracyjne aplikacji webowych obejmujące:

2.1.1.1. Identyfikację i eksploatację luk bezpieczeństwa aplikacji webowych – 2 aplikacje zewnętrzne

2.1.1.2. Testy autoryzacji i uwierzytelniania.

2.1.1.3. Analizę i testy zabezpieczeń danych.

2.1.1.4. Testy kontroli dostępu.

2.1.1.5. Testy podatności na ataki typu SQL Injection, XSS, CSRF, RCE, oraz OWASP TOP 10.

2.1.1.6. Analiza konfiguracji serwerów webowych.

2.2. Infrastruktura Sieciowa

2.2.1. Testy penetracyjne infrastruktury sieciowej obejmujące:

2.2.1.1. Skanowanie i analiza portów.

2.2.1.2. Identyfikację i eksploatację luk bezpieczeństwa w sieci.

2.2.1.3. Testy odporności na ataki DoS/DDoS wolumetryczne oraz aplikacyjne

2.2.1.4. Testy zabezpieczeń urządzeń sieciowych (routery, firewalle, przełączniki, punkty dostępowe), wewnętrzne i zewnętrzne.

2.2.1.5. Sprawdzenie polityk zabezpieczeń sieci. (w zakresie podłączania obcych urządzeń, przechodzenia między podsieciami, separacji logicznej sieci itp.)

2.2.1.6. Analiza i testy VPN oraz innych połączeń zdalnych.

2.2.1.7. Testy systemów wykrywania i zapobiegania włamaniom (IDS/IPS).

2.3. Infrastruktura Serwerowa

2.3.1. Testy penetracyjne infrastruktury serwerowej obejmujące:

2.3.1.1. Analizę konfiguracji serwerów pod kątem bezpieczeństwa

2.3.1.2. Analiza bezpieczeństwa Active Directory

2.3.1.3. Identyfikację i eksploatację luk w systemach operacyjnych (Windows, Linux, Unix).
2.3.1.4. Testy podatności na ataki typu privilege escalation.
2.3.1.5. Sprawdzenie polityk zarządzania użytkownikami i kontrolą dostępu.
2.3.1.6. Weryfikacja kont z dostępem administracyjnym i zakresu dostępów.
2.3.1.7. Testy zabezpieczeń usług serwerowych (np. FTP, SSH, HTTP/HTTPS, DNS,DHCP).
2.3.1.8. Analiza i testy zabezpieczeń baz danych.
2.3.1.9. Weryfikacja poprawności stosowania aktualizacji i łat bezpieczeństwa.
2.3.1.10. Testy systemów kopii zapasowych i odzyskiwania danych.

2.4. Testy Phishingowe Użytkowników

2.4.1. Przeprowadzenie Symulowanych Ataków Phishingowych:

2.4.1.1. Przygotowanie i wysyłka wiadomości e-mail do losowych grup użytkowników, symulujących realistyczne ataki phishingowe.
2.4.1.2. Różne scenariusze ataków, zaproponowane przez Wykonawcę
2.4.1.3. Monitorowanie reakcji na użytkowników na otrzymane wiadomości
2.4.1.4. Wykonawca musi sam pozyskać adresy mailowe do wykonania phisingu, maksymalnie 100 adresów (jeżeli Wykonawca nie będzie mógł pozyskać adresów Zamawiający przekaże listę adresów)

3.1. Metodologia Przeprowadzania Testów

3.1.1. Istotne założenia:

3.1.1.1. Czas na realizację testów to 21 dni kalendarzowych.
3.1.1.2. Czas na wytworzenie raportu po zakończeniu prac to 14 dni kalendarzowych.
3.1.1.3. Czas na wsparcie odnośnie wdrażania rekomendowanych poprawek po wykonaniu testów i raportu to maksymalnie 60 dni kalendarzowych.
3.1.1.4. Tryb prowadzonych testów: Black Box / Grey Box
3.1.1.5. W ramach testów nie jest przewidziana próba przełamania zabezpieczeń fizycznych lub sprawdzenia reakcji służb bezpieczeństwa zamawiającego na nieautoryzowany dostęp.
3.1.1.6. Zespół testerów dołoży wszelkich starań w trakcie pozyskiwania informacji i testowania w celu zminimalizowania ingerencji w sieć produkcyjną. Jednak działania testerów mogą być obarczone pewnym prawdopodobieństwem destabilizacji niektórych usług, o czym wykonawca powiadomi zamawiającego przed wykonaniem danego testu.
3.1.1.7. Działania audytowe mogą być prowadzone o dowolnej porze dnia i nocy.
3.1.1.8. Tester użyje komputera niepowiązanego z podmiotem audytowanym przy próbach dostępu do zasobów
3.1.1.9. Testy penetracyjne danej jednostki zostaje zakończony w momencie przekazania raportu zamawiającemu jako zaszyfrowany załącznik w wiadomości email.
3.1.1.10. Przed rozpoczęciem prac audytowych niezbędne będzie wypełnienie stosownej deklaracji osób decyzyjnych zamawiającego oraz jednostki

audytowanej świadczącej o zgodzie na działania i wiedzy nt. potencjalnych skutków działań testerów.

3.1.1.11. Wykonawca, z dniem podpisania protokołu odbioru raportu, przenosi na Zamawiającego autorskie prawa majątkowe do raportu

3.1.2. Przeprowadzenie testów

3.1.3. Raportowanie

3.1.3.1. Zebranie wyników testów bezpieczeństwa

3.1.3.2. Analiza wyników audytu

3.1.3.3. Opisanie podatności wraz z kategoryzacją CVE i CVSS

3.1.3.4. Opisanie rekomendacji

3.1.3.5. Przekazanie raportu

3.1.3.6. Zawartość raportu:

3.1.3.6.1. Executive Summary – główne konkluzje

3.1.3.6.2. Główne rekomendacje

3.1.3.6.3. Przedmiot testów

3.1.3.6.4. Ranking ryzyk

3.1.3.6.5. Metodologia i kryteria testowania

3.1.3.6.6. Wykorzystane narzędzia w trakcie prowadzenia skanów

3.1.3.6.7. Wykaz zidentyfikowanych podatności wraz z odpowiadającym im kodem CVE

3.1.3.6.8. (Common Vulnerability Enumaration) oraz odnośnikiem do opisu luki.

3.1.3.6.9. Podatności będą pogrupowane według ryzyka, zgodnie ze standardem CVSS

3.1.3.6.10. (Common Vulnerability Scoring System).

3.1.3.6.11. Rekomendacje związane z możliwym usunięciem wykrytych podatności

3.1.3.7. Przygotowanie raportu z wynikami testów phishingowych, zawierającego:

3.1.3.7.1. Statystyki dotyczące liczby użytkowników, którzy odpowiedzieli na wiadomości phishingowe.

3.1.3.7.2. Identyfikację wzorców i najsłabszych punktów w zakresie świadomości bezpieczeństwa.

3.1.3.7.3. Rekomendacje dotyczące poprawy polityki bezpieczeństwa i edukacji użytkowników.

3.1.4. Podsumowanie:

3.1.4.1. Prezentacja wyników testów dla zespołu IT

3.1.4.2. Przeprowadzenie sesji Q&A oraz warsztatów dotyczących wdrożenia rekomendowanych zmian.

3.1.4.3. Wsparcie techniczne w implementacji zaleceń wynikających z raportu końcowego dla wszystkich urządzeń oraz serwerów, bez naprawy błędów w aplikacjach dedykowanych.