

Opis Przedmiotu Zamówienia – część 4

Przeprowadzenie testów socjotechnicznych i penetracyjnych (bezpieczeństwa)

I. Testy socjotechniczne weryfikujące świadomość zagrożeń i reakcje personelu z omówieniem

Przedmiotem zamówienia jest wykonanie testów socjotechnicznych mających na celu wyłudzenie poufnych informacji lub uzyskanie nieautoryzowanego dostępu do systemów Zamawiającego poprzez manipulację i wykorzystanie czynnika ludzkiego.

1. Zamówienie obejmuje przygotowanie **2 testów socjotechnicznych** w tym 1-go testu personalizowanego. Każdy test powinien składać się z :
 - a. przygotowania co najmniej 3 zdefiniowanych scenariuszy ataków, na podstawie przekazanych przez Zamawiającego informacji (podejrzane wiadomości e-mail),
 - b. dostosowania przygotowanych scenariuszy do specyfiki Zamawiającego (w oparciu o wspólne uzgodnienie z Zamawiającym),
 - c. przeprowadzenia co najmniej 3 ataków socjotechnicznych mających na celu wyłudzenie poufnych informacji lub uzyskanie nieautoryzowanego dostępu do systemów Zamawiającego poprzez manipulację i wykorzystanie czynnika ludzkiego czynnika jako wektora ataku,
 - d. w przypadku skuteczności ataku – dokonania analizy danych i informacji w skrzynkach pocztowych takich pracowników celem określenia ich przydatności do dalszej eskalacji ataku,
 - e. przygotowania raportu z przeprowadzonych ataków z odniesieniem do scenariuszy ataków, ich skuteczności oraz z podaniem informacji o „złapanych” pracownikach i wrażliwych/przydatnych informacji do dalszej eskalacji ataku, wraz z rekomendacjami.
2. Zamawiający zapewni dodanie serwerów wysyłkowych Wykonawcy do list wykluczeń filtrów antyspamowych i antyphishingowych.
3. Wykonawca zapewni, że „złośliwe” załączniki zawierać będą jedynie prosty program odsyłający na serwer Wykonawcy dane telemetryczne na temat zaatakowanej maszyny bez przejęcia nad nią „całkowitej” kontroli.
4. **Ogólna charakterystyka Zamawiającego:**
 - 1) Zamawiający jest jednostką sektora finansów publicznych – samorządu terytorialnego. Realizuje zadania publiczne wynikające z ustawy o samorządzie gminnym (Dz.U.2024.0.609).
 - 2) Zamawiający realizuje zadania określone w part. 6 i art. 7 Ustawy o samorządzie gminnym.
 - 3) Wszystkie informacje dotyczące Zamawiającego są dostępne na jego stronie internetowej.
 - 4) Liczba pracowników: 54 osób
 - 5) Ilość wszystkich hostów podłączonych do sieci (komputery, urządzenia serwerowe, urządzenia sieciowe jak np. drukarki, routery, przełączniki, Access Pointy, urządzenia VoIP etc.).

W tym:

- a. Ilość komputerów (również przenośnych)- 47 szt.
- b. Ilość serwerów (fizycznych, wirtualnych)
 - Serwery fizyczne centralne: 6 szt.

- Serwery wirtualne: 12 szt.
- c. Ilość pozostałych urządzeń podłączonych do sieci –16 szt.
- 6) Ilość podsieci – 22
- 7) Ilość serwerowni – 2
- 8) Wdrożone Active Directory
- 9) Wymagania dodatkowe:

Dokumentacja:

- a) Raport z realizacji usługi powinien zostać przygotowany w wersji elektronicznej w wersji elektronicznej, zgodnie z wymogami Wytycznych dotyczących realizacji zasad równościowych w ramach funduszy unijnych na lata 2021-2027
- b) Raport należy oznaczyć logotypami programu zgodnie z wytycznymi programu Cyberbezpieczny Samorząd.

II. Przeprowadzenie testów penetracyjnych, tj. testów bezpieczeństwa systemu SZBI wraz ze wsparciem w zakresie wdrożenia rekomendacji po przeprowadzeniu testów

Przedmiotem zamówienia jest wykonanie **4 testów bezpieczeństwa (penetracyjnych)** wybranej przez Zamawiającego wewnętrznej infrastruktury teleinformatycznej, przyjmujących postać zasymulowania zachowania realnego atakującego.

1. Zamówienie obejmuje symulację zachowania prawdziwego atakującego, np. operatora ransomware, który uzyskał dostęp do wewnętrznej infrastruktury teleinformatycznej Zamawiającego.
2. Zamawiający przygotowuje środowisko do testu na jednej maszynie w wybranej przez siebie sieci wewnętrznej i utworzy konto dla Wykonawcy (Pentestera), który uruchomi dedykowany do ataku „implant”, adekwatny do celów, ograniczeń i wyłączeń, o których mowa w ust. 3 poniżej.
3. Zakres ataku w wewnętrznej sieci Zamawiającego zostanie wspólnie uzgodniony przez Strony (cele, wyłączenia, ograniczenia).
4. Wykonawca rozpocznie test od najmniejszych uprawnień i dążyć będzie do uzyskania dostępu do innych maszyn, zidentyfikowania „istotnych” danych i informacji oraz znalezienia podatności, które pozwolą na eskalację uprawnień i ostatecznie do przejęcia całkowitej kontroli nad siecią lub środowiskiem Active Directory. W przypadku przejęcia kontroli nad siecią Wykonawca (Pentester) zobligowany będzie do dalszej analizy dostępnej infrastruktury w celu ustalenia możliwych ścieżek ataku mogących skutkować całkowitym przejęciem sieci Zamawiającego (innych niż wybranej przez Zamawiającego).
5. Atak na wewnętrzną sieć Zamawiającego będzie prowadzony w wariantcie otwartym, co oznacza, że Wydział IT Zamawiającego będzie wiedział o teście i nie będzie próbował aktywnie przeciwdziałać atakowi. Strony będą wzajemnie informować się o ryzykach związanych z zakłóceniem ciągłości działania procesów Zamawiającego.
6. Zamawiający, jak również Wykonawca ma prawo do przerwania testu w każdym momencie w związku z wystąpieniem wspomnianego wyżej ryzyka.

7. W przypadku przejęcia przez Pentestera użytkownika o odpowiednio wysokich uprawnieniach Wykonawca (Pentester) sprawdzi (potwierdzi) możliwość pobrania materiału kryptograficznego z hasłami użytkowników.
8. Wykonawca przygotowuje raport z przeprowadzonego testu z listą podatności, wraz z technicznym opisem problemu oraz określeniem poziomu zagrożenia, a także rekomendacjami, jak je usunąć.
9. **Ogólna charakterystyka Zamawiającego:**
 - 1) Zamawiający jest jednostką sektora finansów publicznych – samorządu terytorialnego. Realizuje zadania publiczne wynikające z ustawy o samorządzie gminnym (Dz.U.2024.0.609).
 - 2) Zamawiający realizuje zadania określone w part. 6 i art. 7 Ustawy o samorządzie gminnym.
 - 3) Wszystkie informacje dotyczące Zamawiającego są dostępne na jego stronie internetowej.
 - 4) Liczba pracowników: 54 osób
 - 5) Ilość wszystkich hostów podłączonych do sieci (komputery, urządzenia serwerowe, urządzenia sieciowe jak np. drukarki, routery, przełączniki, Access Pointy, urządzenia VoIP etc.),
w tym:
 - a) Ilość komputerów (również przenośnych)- 47 szt.
 - b) Ilość serwerów (fizycznych, wirtualnych)
 - Serwery fizyczne centralne: 6 szt.
 - Serwery wirtualne: 12 szt.
 - c) Ilość pozostałych urządzeń podłączonych do sieci -16 szt.
 - 6) Ilość podsieci – 22
 - 7) Ilość serwerowni – 2
 - 8) Wdrożone Active Directory

Wymagania dodatkowe:

Dokumentacja:

- a) Raport z realizacji usługi powinien zostać przygotowany w wersji elektronicznej w wersji elektronicznej, zgodnie z wymogami Wytycznych dotyczących realizacji zasad równościowych w ramach funduszy unijnych na lata 2021-2027 .
- b) Raport należy oznaczyć logotypami programu zgodnie z wytycznymi programu Cyberbezpieczny Samorząd.