**Załącznik nr 1 c**

**Opis Przedmiotu Zamówienia**

**Testy penetracyjne - testy bezpieczeństwa systemu SZBI wraz ze wsparciem w zakresie wdrażania rekomendacji po przeprowadzeniu testów**

Przedmiotem zamówienia jest wykonanie 6 testów 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 przygotuje 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 dążył 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 wariancie 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 przygotuje raport z przeprowadzonego testu z listą podatności, wraz z technicznym opisem problemu oraz określeniem poziomu zagrożenia, a także rekomendacjami, jak je usunąć.

Wymagania dodatkowe:

1. Dokumentacja.
   1. 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
   2. Opracowanie należy oznaczyć logotypami programu zgodnie z wytycznymi programu Cyberbezpieczny Samorząd.

**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. Przybliżona liczba pracowników Zamawiającego to: 60 osób
5. Ilość wszystkich hostów podłączonych do sieci 196 (komputery, urządzenia serwerowe, urządzenia sieciowe jak np. drukarki, routery, przełączniki, Access Pointy, urządzenia VoIP etc.). W tym:

W tym:

a. Ilość komputerów (również przenośnych) - 60 szt.

b. Ilość serwerów (fizycznych, wirtualnych)

* Serwery fizyczne: 3 szt.
* Serwery wirtualne: 21 szt.

c. Ilość pozostałych urządzeń podłączonych do sieci – 109 szt.

1. Ilość adresów zewnętrznych – 5
2. Ilość podsieci – 24
3. Ilość serwerowni – 2
4. Wdrożone Active Directory