Śląska Sieć
Metropolitalna
Sp. z o.o.

Zapytanie ofertowe

testy socjotechniczne i penetracyjne

Śląska Sieć Metropolitalna Sp. z o.o.

zwraca się z prośbą

o przedstawienie oferty cenowej na:

testy socjotechniczne i penetracyjne

I. ZAMAWIAJĄCY

Śląska Sieć Metropolitalna Sp. z o.o.
ul. Bojkowska 37P, 44-100 Gliwice
NIP: 6312578261, REGON: 241069249
Sąd Rejonowy w Gliwicach KRS: 0000322774

II. OPIS PRZEDMIOTU ZAMÓWIENIA

A. Usługi i założenia ogólne

1. Przedmiotem zamówienia jest wykonanie usług w następującym zakresie:

1.1. przeprowadzenie testów socjotechnicznych, mających na celu wyłudzenie poufnych informacji lub uzyskanie nieautoryzowanego dostępu do systemów Zamawiającego poprzez manipulację i wykorzystanie czynnika ludzkiego,

1.2. przeprowadzenie testów penetracyjnych wybranej przez Zamawiającego wewnętrznej infrastruktury teleinformatycznej, przyjmujących postać zasymulowania zachowania realnego atakującego,

zwanych dalej łącznie **„Usługami"** a każda z osobna **„Usługą"**, na warunkach określonych w umowie, o której mowa w ust. 4 poniżej oraz z uwzględnieniem założeń zawartych w Rozdziale II lit. A i B niniejszego OPZ.

2. Harmonogram realizacji Usług musi w szczególności określać czas ich trwania oraz skład zespołu testerów.

3. Faktura VAT zostanie wystawiona z 14 dniowym terminem płatności od daty wystawienia faktury po podpisaniu przez obie Strony protokołu odbioru Usługi bez uwag, na wskazany przez Wykonawcę rachunek bankowy.

4. Usługi będą realizowane na podstawie zawartej umowy.

B. Testy socjotechniczne

1. Zamówienie określone w Rozdziale II lit. A. ust. 1. pkt 1.1. obejmować będzie:

1.1. przygotowanie co najmniej 3 zdefiniowanych scenariuszy ataków, na podstawie przekazanych przez Zamawiającego informacji (podejrzane wiadomości e-mail),

1.2. dostosowanie przygotowanych scenariuszy do specyfiki Zamawiającego (wspólne uzgodnienie z Zamawiającym),

1.3. przeprowadzenie co najmniej 3 ataków socjotechnicznych mających na celu wyłudzenie poufnych informacji lub uzyskanie nieautoryzowanego dostępu do systemów Zamawiającego poprzez manipulację i wykorzystanie ludzkiego czynnika jako wektora ataku,

1.4. w przypadku skuteczności ataku analizę danych i informacji w skrzynkach pocztowych takich pracowników celem określenia ich przydatności do dalszej eskalacji ataku,

1.5. przygotowanie 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.

C. Testy penetracyjne

1. Zamówienie określone w Rozdziale II lit. A. ust. 1. pkt 1.2. obejmować będzie 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.

III. WARUNEK UDZIAŁU W POSTĘPOWANIU

1. Zamawiający wymaga, aby Wykonawca dysponował oraz skierował do realizacji zamówienia zespół testowy składający się z co najmniej 1 osoby (członka), albo osobę, posiadającą wiedzę i doświadczenie popartą co najmniej jednym z niżej wymienionych certyfikatów:

1) OffSecurity Experienced Penetration Tester (OSEP);

2) Certified Ethical Hacker (CEH);

3) CompTIA Pentest+;

4) Certified Information Systems Auditor (CISA);

5) GIAC Penetration Tester (GPEN);

6) Certified Information Systems Security Professional (CISSP).

2. Zamawiający dopuszcza certyfikaty równoważne do wymienionych powyżej, przy czym za certyfikat równoważny uważany będzie certyfikat potwierdzający zakres wiedzy i doświadczenia tożsamy z oficjalnym sylabusem egzaminu, którego równoważność jest wskazywana przez Wykonawcę. Wykonawca, który powołuje się na certyfikaty równoważne jest zobowiązany wykazać, że wskazywane przez niego certyfikaty potwierdzają zakres wiedzy i doświadczenia tożsamy z oficjalnym sylabusem egzaminu, którego równoważność jest wskazywana.

3. Zamawiający wymaga:

1) dołączenia do oferty wykazu osób skierowanych przez Wykonawcę do realizacji zamówienia i odpowiedzialnych za świadczenie Usług, w tym co najmniej 1 osoby spełniającej kwalifikacje wiedzy i doświadczenia wskazane w ust. 1 i 2 powyżej. Jeżeli usługi będą wykonywane przez 1 osobę w wykazie należy wskazać tylko osobę posiadającą odpowiednie kwalifikacje,

2) co najmniej jednego z wymienionych w ust. 1 i 2 powyżej certyfikatów dla osoby skierowanej przez Wykonawcę do realizacji zamówienia i odpowiedzialnej za świadczenie Usług.

4. Wzór wykazu osób, o którym mowa w ust. 3 powyżej, stanowi **Załącznik nr 1** do Zapytania ofertowego.

IV. OPIS PRZYGOTOWANIA OFERTY

1. Oferty składane są za pomocą formularza aktywnego na platformie zakupowej dostępnej pod adresem https://platformazakupowa.pl/pn/ssm_silesia.
2. Termin składania ofert: **26.02.2024 r., godz. 12:00**.
3. Termin związania ofertą: **21** (słownie: dwadzieścia jeden) dni kalendarzowych.
4. Oferty złożone po terminie nie będą rozpatrywane.

V. DODATKOWE INFORMACJE

1. Dodatkowych informacji można uzyskać pod numerem telefonu +48 534 673 473 (kontakt w godzinach 8:00 – 15:00) oraz adresem email: j.suszka@ssm.silesia.pl do wiadomości do@ssm.silesia.pl.
2. Złożenie oferty cenowej nie stanowi zobowiązania po stronie Zamawiającego ani nie stwarza jakichkolwiek roszczeń ze strony oferenta względem Zamawiającego, bądź jego następców prawnych.