Załącznik nr 1
do zapytania cenowego
nr OR.271.1.14.2024.KG

OPIS PRZEDMIOTU ZAMÓWIENIA

na wykonanie zamówienia w zakresie wykonania Audytu Cyberbezpieczeństwa (audyt wstępny i końcowy) wraz z testami penetracyjnymi w ramach projektu „Cyberbezpieczny Samorząd w Gminie Miasto Braniewo”
realizowanego w ramach Programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

Przedmiotem zamówienia jest zrealizowanie usługi polegającej na przeprowadzeniu Audytu Cyberbezpieczeństwa (wstępnego i końcowego) wraz z testami penetracyjnymi w Urzędzie Miasta Braniewa (UM) oraz jednostkach: Zakład Gospodarki Komunalnej (ZGK), Miejski Ośrodek Pomocy Społecznej (MOPS), Miejski Ośrodkek Sportu "Zatoka" (MOS) i Centrum Usług Wspólnych (CUW) w ramach projektu pn.: „Cyberbezpieczny Samorząd w Gminie Miasto Braniewo” zgodnie z zakresem oraz formularzem stanowiącym załącznik do Regulaminu Konkursu Grantowego „Cyberbezpieczny Samorząd”.

Audyt bezpieczeństwa ma zostać przeprowadzony w oparciu o Standardy: Krajowe Ramy Interoperacyjności (KRI), Krajowy System Cyberbezpieczeństwa (KSC), normę ISO27001:2023 oraz Narodowe Standardy Cyberbezpieczeństwa (NSC).

Testy penetracyjne (bezpieczeństwa) mają zostać przeprowadzone zgodnie z Metodologią PTES Standard.

Wykonanie i przekazanie Raportu z Audytu zawierającego w szczególności: opis zakresu przeprowadzonych prac audytowych, analizę informacji zebranych podczas audytów, wnioski i zalecenia związane z rozwiązaniem występujących problemów, analiza złożonego załącznika nr 6 do konkursu grantowego tj. „Ankieta Dojrzałości Cyberbezpieczeństwa w Jednostce Samorządu Terytorialnego (i Jednostkach Podległych)”.

Istotą testów jest bezstronne zapewnienie, że infrastruktura spełnia standardy bezpieczeństwa w obszarze Eksploatacji systemów - zapewnienie ciągłości działania systemów informatycznych z uwzględnieniem aspektów poufności, rozliczalności, dostępności oraz integralności przetwarzanych informacji.

Przygotowanie do audytu:

a) Zebranie wstępnych informacji za pomocą pisemnych i telefonicznych konsultacji z przedstawicielem Zamawiającego, w zależności od złożoności przeprowadzanego audytu i testów.

b) Kompletacja danych istotnych dla audytu i testów.

c) Określenie rodzaju audytu (White Box, Grey Box, Black Box). W przypadku audytu na znanej infrastrukturze, niezbędne jest dostarczenie dokumentacji umożliwiającej określenie topologii sieci.

d) Przeprowadzenie wywiadu technicznego z osobą posiadającą szczegółową wiedzę na temat urządzeń i usług mających wpływ na bezpieczeństwo organizacji.

e) Upewnienie się, że obecna jest osoba uprawniona do zagwarantowania fizycznego dostępu do elementów infrastruktury sieciowej (szczególnie serwerowni, urządzeń brzegowych, przełączników sieciowych, węzłów komunikacyjnych, punktów dostępowych).

f) Przedstawienie przedstawicielowi organizacji zakresu audytu lub testów penetracyjnych wraz ze szczegółowym określeniem zasad, warunków i zakresu przeprowadzanych działań.

Wymagania proceduralne

Audyt zostanie przeprowadzony zgodnie z wymogami dokumentacji konkursowej oraz najlepszymi, obowiązującymi praktykami. Wykonanie testów bezpieczeństwa zostanie zlecone niezależnemu wykonawcy, który nie jest powiązany z żadnym elementem (w tym producentem urządzeń) testowanej

infrastruktury oraz organizacji, co gwarantuje obiektywność i rzetelność przeprowadzonej analizy.

I. AUDYT CYBERBEZPIECZEŃSTWA (wstępny i końcowy)

Audyt cyberbezpieczeństwa informacji obejmuje wszystkie obszary funkcjonowania Zamawiającego w tym:

1. **Audyt organizacyjny:**
   a) weryfikacja regulacji w obszarze zarządzania bezpieczeństwem informacji;
   b) odpowiedzialność za bezpieczeństwo informacji i koordynacja prac związanych z zarządzaniem bezpieczeństwem informacji;
   c) dokumentacja, w tym z zakresu ochrony danych osobowych;
   d) analiza ryzyka;
   e) inwentaryzacja aktywów;
   f) plan postępowania z ryzykiem;
   g) przeprowadzenie wywiadów z wybranymi pracownikami.
2. **Audyt fizyczny i środowiskowy**
   a) weryfikacja zabezpieczeń wejścia/wyjścia;
   b) weryfikacja systemów zabezpieczeń pomieszczeń i urządzeń;
   c) weryfikacja bezpieczeństwa okablowania strukturalnego;
   d) weryfikacja systemów chłodzenia i systemów alarmowych.
3. **Audyt KRI**
   a) SZBI
   - Weryfikacja SZBI pod kątem uwzględnienia takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność;
   - Weryfikacja poprawności opracowania, ustanowienia, wdrożenia, eksploatacji, monitorowania i przeglądania.

   b) Weryfikacja działań najwyższego kierownictwa w zakresie poprawnego zapewnienia warunków umożliwiających realizację i egzekwowanie następujących działań;
   - - zapewnienie i nadzór nad aktualizacją regulacji wewnętrznych m.in. w zakresie dotyczącym zmieniającego się otoczenia;
   - zapewnienie i nadzór nad aktualnością inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji;
   - zapewnienie i nadzór nad przeprowadzaniem okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji;
   - zapewnienie i nadzór nad podejmowaniem działań minimalizujących ryzyko, stosownie do wyników przeprowadzonej analizy;

- zapewnienie właściwego procesu zarządzania systemem nadawania, zmiany, wstrzymywania i odbierania uprawnień;
- zapewnienie szkoleń;
- zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami;
- utworzenie, weryfikacja i nadzór nad regulacjami gwarantującymi bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość;
- zabezpieczenie informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie;
- weryfikacja umów ze stronami trzecimi w zakresie bezpieczeństwa informacji;
- zapewnienie i nadzór nad:
  - aktualizacją oprogramowania;
  - minimalizowaniem ryzyka utraty informacji w wyniku awarii;
  - ochronie przed błędami, utratą, nieuprawnioną modyfikacją;
  - stosowaniem mechanizmów kryptograficznych;
  - zapewnieniem bezpieczeństwa plików systemowych;
  - redukcją ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych;
  - podejmowaniem działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa;
  - kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa.

II. TESTY PENETRACYJNE (bezpieczeństwa)

Testy penetracyjne dotyczyć muszą:

a) Usług oraz zasobów publicznie dostępnych w sieci Internet:

- Ocena podatności na ataki: Wykonanie skanowania pod względem podatności i oceny zgodności z najlepszymi praktykami zabezpieczeń.
- Urządzenia brzegowe: Sprawdzenie konfiguracji firewalli, IPS/IDS, mechanizmów anty DDoS oraz zabezpieczeń SSL/TLS.

b) Bezpieczeństwa poczty elektronicznej

- Weryfikacja poprawności konfiguracji mechanizmów SPF, DMARC, DKIM.
- Szyfrowanie poczty: Ocena implementacji szyfrowania (S/MIME, PGP), bezpieczne przechowywanie i zarządzanie kluczami.

c) Bezpieczeństwa infrastruktury sieciowej

- Konfiguracja urządzeń sieciowych: Szczegółowa analiza konfiguracji firewalli, routerów, przełączników oraz punktów dostępowych, ocena segmentacji sieci i VLAN.
- Analiza bezpieczeństwa sieci wewnętrznych i zewnętrznych, ocena bezpieczeństwa VPN.
- Analiza udostępnionych usług wraz z testami bezpieczeństwa mającymi na celu weryfikację istnienia podatności na ataki sieciowe.

d) Bezpieczeństwa infrastruktury sprzętowej i oprogramowania

- weryfikacja aktualizacji systemów operacyjnych, aplikacji, firmware urządzeń.
- ocena weryfikacja wdrożonych polityk bezpieczeństwa oraz zarządzania zasobami IT pod względem stosowania bezpiecznych praktyk administracyjnych.

e) Bezpiecznej konfiguracja domeny Microsoft Active Directory

- weryfikacja poprawnej konfiguracji domeny oraz wdrożonych polityk bezpieczeństwa wraz z oceną zabezpieczeń Kerberos I analizą polityki haseł.
- Weryfikacja GPO (Group Policy Objects), audyt uprawnień użytkowników i grup, analiza logowania i monitorowania zdarzeń.

f) Bezpieczeństwa aplikacji

- Aplikacje utrzymywane w sieci wewnętrznej zostaną poddane analizie, której celem jest określenie stopnia podatności na ataki.
- W zależności od rodzaju aplikacji występujących w środowisku klienta, zastosowane zostaną dopasowane techniki pozwalające na wykrycie luk oraz błędów w obszarach związanych z daną usługą, w tym zostanie przeprowadzona weryfikacja konfiguracji baz danych, ocena mechanizmów autoryzacji i uwierzytelnienia pod względem podatności na ataki.

g) Bezpieczeństwa danych – backupy

- Ocena polityki backupów w organizacji, w tym częstotliwości tworzenia kopii zapasowych i ich przechowywania.
- Weryfikacja zgodności procedur backupowych z przyjętymi standardami branżowymi.
- Sprawdzenie, czy kopie zapasowe przechowywane są w odseparowanych, bezpiecznych i oddzielnych lokalizacjach.
- Weryfikacja szyfrowania kopii zapasowych w celu ochrony przed nieautoryzowanym dostępem.

h) Poprawności aktualnej dokumentacji

- Sprawdzenie, czy dokumentacja dotycząca bezpieczeństwa jest kompletna i zgodna z obowiązującymi standardami.

i) Testów socjotechnicznych

- Przeprowadzenie symulowanych ataków phishingowych, ocena wyników i opracowanie rekomendacji na podstawie zachowań pracowników.
- Kampania zostanie podzielona na trzy grupy odbiorców, aby ocenić różne poziomy wrażliwości i odpowiedzi na tego typu zagrożenia.

- Szczegółowe wymagania do przeprowadzenia testów socjotechnicznych:
  - Wykonawca będzie zobowiązany do zachowania poufności i przestrzegania przepisów o ochronie danych osobowych oraz do prowadzenia audytu w sposób uczciwy i obiektywny.
  - Przygotowanie co najmniej 3 zdefiniowanych scenariuszy ataków, na podstawie przekazanych przez Zamawiającego informacji (podejrzane wiadomości e-mail).
  - Dostosowanie przygotowanych scenariuszy do specyfiki Zamawiającego (wspólne uzgodnienie z Zamawiającym).
  - Przeprowadzenie co najmniej 6 ataków socjotechnicznych mających na celu wyłudzenie poufnych informacji lub uzyskanie nieautoryzowanego dostępu do systemów Zamawiającego poprzez manipulację i wykorzystanie ludzkiego czynnika jako wektora ataku.
  - W przypadku skuteczności ataku analizę danych i informacji w skrzynkach pocztowych takich pracowników celem określenia ich przydatności do dalszej eskalacji ataku.
  - Przygotowanie raportu z przeprowadzonych ataków z odniesieniem do opisu scenariuszy ataków, oceny skuteczności ataków, Informacji o zaatakowanych pracownikach i wrażliwych danych, rekomendacje dotyczące poprawy bezpieczeństwa.
  - Zamawiający zapewni dodanie serwerów wysyłkowych Wykonawcy do list wykluczeń filtrów antyspamowych i antyphishingowych.
  - 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.
  - Zamawiający wyraża zgodę na wykorzystanie wizerunku Zamawiającego w tym w szczególności: logo, nazwy domeny i grafiki, stopki podpisu wiadomości e-mail w czasie trwania testów bezpieczeństwa w postaci testów socjotechnicznych.

III. Przygotowanie raportu z Audytu

Podsumowanie, przedstawienie wyników, procesów naprawczych w celu poprawy bezpieczeństwa organizacji:

a. Przygotowanie raportu zawierającego szczegółowe wyniki wizji lokalnej.

b. Wyróżnienie obszarów wymagających uwagi oraz silnych stron zabezpieczeń fizycznych.

c. Lista konkretnych podatności z ich nazwami, numerami CVE (Common Vulnerabilities and Exposures), szczegółowymi opisami, oraz rekomendacjami ich usunięcia lub zminimalizowania skutków zidentyfikowanej podatności.

d. Załączenie zrzutów ekranu, logów oraz innych danych wspierających identyfikację podatności.

e. Wskazanie liczby podatności sklasyfikowanych jako niskie, średnie, wysokie i krytyczne.

f. Opis potencjalnych skutków wykorzystania każdej podatności (np. utrata danych, przerwy w dostępności, ataki hakerskie).

g. Wskazanie, które podatności powinny być naprawione jako pierwsze, bazując na ich krytyczności i potencjalnych skutkach.

h. Informacje na temat warunków, w jakich skanowanie zostało przeprowadzone.