Załącznik nr.1

Szczegółowy Opis Przedmiotu Zamówienia

Spis treści

1. SZKOLENIA Z TESTAMI SOCJOTECHNICZNYMI DLA PRACOWNIKÓW ADMINISTRACJI

L.P	Parametr	Charakterystyka (wymagania minimalne) Oferowane parametry
1.	Charakterystyka ogólna	1. Przedmiotem zamówienia jest przeprowadzenie szkoleń z zakresu cyberbezpieczeństwa dla 120 pracowników administracyjnych, które zostaną poprzedzone testami socjotechnicznymi. 2. Dla każdej grupy uczestników szkoleń w każdym z cyklów szkoleniowych z osobna Zamawiający przewiduje ilość godzin szkolenia w wymiarze nie mniej niż 2 godziny; 3. Planowane terminy szkoleń: Zamawiający planuje przeprowadzenie szkoleń z podziałem na 3 grup/y pracowników nie większe niż 40 osób; 4. Po podpisaniu umowy z Wykonawcą Zamawiający dopuszcza rotacje liczby uczestników podczas każdego cyklu szkoleniowego; 5. Szkolenia odbywać się będą w dni robocze od poniedziałku do piątku w godzinach 7:30 – 15:30 6. Szkolenie stacjonarne z zakresu cyberbezpieczeństwa skierowane do pracowników Starostwa obejmujące co najmniej następujące obszary: a. wprowadzenie do cyberbezpieczeństwa: i. czym jest cyberbezpieczeństwo;

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

		ii. kluczowe zagadnienia związane z cyberbezpieczeństwem; iii. przegląd statystyk i trendów w cyberbezpieczeństwie. b. typy zagrożeń w cyberprzestrzeni: iv. malware (wirusy, trojany, robaki itp.); v. ataki typu phishing i spear phishing; vi. ataki DDoS; vii. ataki ransomware; viii. zagrożenia związane z sieciami społecznościowymi. c. zasady bezpieczeństwa i praktyki: ix. zarządzanie hasłami i uwierzytelnianie wieloskładnikowe; x. zasady bezpieczeństwa e-mail; xi. bezpieczeństwo w sieciach bezprzewodowych; xii. bezpieczne przeglądanie internetu; xiii. backup i odzyskiwanie danych. d. reagowanie na incydenty i planowanie awaryjne: xiv. jak zidentyfikować i zgłosić incydent związany z cyberbezpieczeństwem; xv. zasady reagowania na incydenty; xvi. planowanie awaryjne i kontynuacja działalności; xvii. przegląd realnych przypadków naruszeń bezpieczeństwa 7. Zamawiający przewiduje przeprowadzenie testów socjotechnicznych z minimum 7 dniowym wyprzedzeniem, przed potwierdzonym terminem szkoleń dla pracowników Starostwa. 8. Przeprowadzane próby w Organizacji miały na celu zweryfikowanie świadomości pracowników i zabezpieczeń przed atakami socjotechnicznymi. 9. Testy socjotechniczne obejmują swoim zakresem weryfikację zachowania pracowników na możliwe próby ataków. Jednym z najczęstszych sposobów dostanie się do infrastruktury przez atakującego jest wykorzystanie ataku skierowanego na pracownika danej firmy. 10. Plan usługi obejmuje:

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

		a. Testy phishingowe - Przygotowanie spreparowanej wiadomości email, która ma nakłonić pracownika na wejście w podany wiadomości link, podanie poświadczeń itp. b. Testy vishingowe - Rozmowa telefoniczna, podczas której pentester próbuje nakłonić pracownika do przekazania poufnych informacji lub takich, które by mogły pomóc w przeprowadzeniu dalszej fazy ataku. Jednocześnie próbuje nakłonić pracownika na przedstawioną stronę w celu zainstalowania oprogramowania c. Wykonanie raportu zawierającego opis wszystkich elementów, które zostały poddane audytowi podział podatności ze względu na ryzyko: o wysoki o średni o niski d. Wskazanie zaleceń, rekomendacji, najlepszych praktyk – dla każdej znalezionej podatności e. wylistowanie wszystkich podatności ze względu na ryzyko: o wysoki o średni o niski f. określenie bezpieczeństwa informatycznego w organizacji poprzez wskazanie ilości i rodzaju znalezionych podatności g. Wsparcie po audytowe - Udzielenie informacji na temat audytowanych elementów wynikających z raportu.
2.	Wymagania wobec Wykonawcy	– Wykonawca musi posiadać certyfikat PN-EN ISO 9001 w zakresie świadczenia usług szkoleniowych i audytowych w zakresie systemów informatycznych – Wykonawca musi posiadać certyfikat PN-EN ISO 22301 w szczególności w zakresie realizacji usług szkoleniowych i monitorowania infrastruktury teleinformatycznej, analizy zdarzeń, detekcji zagrożeń bezpieczeństwa i reagowania na wykryte incydenty w ramach Security Operation Center – Wykonawca oddeleguje do realizacji zadania prelegenta posiadającego certyfikat Bezpieczeństwa Informacji zgodnie z normą PN-EN ISO 27001 – Zamawiający wymaga, aby Wykonawca posiada potencjał osobowy niezbędny do wykonania zamówienia. Zamawiający wymaga, aby osoby oddelegowane do realizacji zadania łącznie posiadały poniższe certyfikaty: ○ OSCP (Offensive Security Certified Professional) ○ CEH (Certified Ethical Hacker)

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

		○ Audytor wiodący ISO/IEC 22301 ○ Audytor wiodący ISO/IEC 27001 ○ Certified Information Systems Security Professional (CISSP) **Certyfikaty należy dołączyć do oferty** – Wykonawca przeprowadzi szkolenia w języku polskim; – Wykonawca wyda każdemu uczestnikowi szkolenia certyfikat o ukończeniu szkolenia – W ramach organizacji każdego z cykli szkoleń Wykonawca zapewni materiały szkoleniowe dla wszystkich uczestników obejmujące szczegółowy zakres merytoryczny w wersji papierowej. – W ramach szkoleń Wykonawca zapewni dokumentację wszystkich szkoleń: – Listy obecności uczestników szkoleń; – Listy odbioru certyfikatów o ukończonych szkoleniach; – Dzienniki szkoleń zawierające informacje na temat przebiegu oraz o zakresie merytorycznym szkoleń, podpisane przez osobę prowadzącą szkolenia; – Dokumentację fotograficzną z przeprowadzonych szkoleń (forma elektroniczna); – Wykonawca zobowiązuje się w terminie 5 dni od dnia podpisania umowy dostarczyć Zamawiającemu: – Proponowane terminy szkoleń; – Szczegółowy zakres merytoryczny szkoleń; – Harmonogram szkoleń; – Wykonawca zobowiązany jest do współpracy i konsultacji z Zamawiającym oraz do wprowadzania poprawek do sporządzonej dokumentacji zgodnie z sugestiami Zamawiającego na każdym etapie realizacji zamówienia;

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl