Rozdział I. Wprowadzenie

1. Przedmiotowe postępowanie dotyczy realizacji szkolenia z zakresu cyberbezpieczeństwa systemów informatycznych.

Rozdział II. Ogólny Opis przedmiotu zamówienia

1. Przedmiotem zamówienia jest świadczenie usługi polegającej na zorganizowaniu i przeprowadzeniu szkoleń dla 4 uczestników zgodnie z poniższym zestawieniem.

Lp.	Temat szkolenia	Liczba uczestników	Uczestnicy
I.	Bezpieczeństwo Sieci Komputerowych	6	Administratorzy IT
II.	Atakowanie i Ochrona Webaplikacji	6	Administratorzy IT

2. Uczestnikami szkolenia będą administratorzy systemów teleinformatycznych.
3. Szkolenia zostaną przeprowadzone w języku polskim, w formie stacjonarnych warsztatów w siedzibie Zamawiającego. Szkolenia będą składać się głównie z ćwiczeń (laboratoriów) z elementami wykładu, w celu praktycznego przygotowywania uczestników szkolenia.

Rozdział III. Szczegółowy opis przedmiotu zamówienia

III.1 TEMATY REALIZOWANE W RAMACH SZKOLEŃ

III.1.1 Bezpieczeństwo Sieci Komputerowych

1. Celem szkolenia jest nabycie przez uczestnika wiedzy o technikach ataków i programach wykorzystywanych przez współczesnych włamywaczy oraz umiejętności w zakresie zabezpieczenia infrastruktury sieciowej, serwerów i usług na nich pracujących przed atakami w tym wykorzystania narzędzi do testowania bezpieczeństwa sieci.
2. Minimalny zakres szkolenia:

a. Testowanie bezpieczeństwa sieci oraz testy penetracyjne i ich metodyki.
    i. metodyki i rodzaje pentestów,
    ii. OSSTMM / OWASP,
    iii. dokumenty opisujące dobre praktyki (NIST/CIS),
    iv. różnice pomiędzy pentestami a audytami,
b. Organizacja testów penetracyjnych:
    i. prawne aspekty,
    ii. plany testów penetracyjnych,
    iii. problemy spotykane podczas testów penetracyjnych.
c. Poszczególne fazy testu penetracyjnego:
    i. rekonesans
        - pasywne metody zbierania informacji o celu
        - aktywne metody zbierania informacji o celu
        - mapowanie sieci ofiary
        - omijanie firewalli
    ii. enumeracja podatności
        - rodzaje podatności (buffer, overflow, format string, itp.)
        - dopasowywanie kodu exploita do znalezionych podatności
        - drogi wejścia do systemu
    iii. atak,
        - przegląd technik ataków na systemy (Windows/Linux) i sieci komputerowe (ataki w sieci LAN/WAN/Wi-Fi, ataki na urządzenia sieciowe, ataki denial of service, fuzzing, łamanie haseł,
        - atak przy pomocy exploita zdalnego,
        - podniesienie uprawnień do poziomu administratora
    iv. zacieranie śladów,
        - backdoorowanie przejętego systemu
        - zacieranie śladów włamania, oszukiwanie narzędzi do analizy powłamaniowej
    v. sporządzenie raportu z testu penetracyjnego.
        - budowa szczegółowego raportu technicznego
        - raport dla zarządu

d. Metody ochrony przed atakami.
    i. idea honeypotów
    ii. systemy IDS/IPS
    iii. metody hardeningu systemów Windows i Linux
e. **Do każdego z powyższych punktów muszą zostać przygotowane laboratoria, podczas których należy przedstawić praktyczne metody ochrony przed konkretnym atakiem.**

3. Szkolenie "Bezpieczeństwo Sieci Komputerowych" musi trwać **co najmniej 3 dni** szkoleniowe.
4. Szkolenie będzie prowadzone w języku polskim. Wykonawca udostępni uczestnikom środowisko na którym będą odbywały się ćwiczenia. W razie konieczności Wykonawca jest zobowiązany do zapewnienia uczestnikom szkolenia oprogramowania umożliwiającego sprawne połączenie z takim środowiskiem. Wykonawca musi zapewnić odpowiednie środowisko szkoleniowe pozwalające na przeprowadzenie szkolenia w formule ” Bring Your Own Laptop”.
5. Za dzień szkoleniowy przyjmuje się min. 8 godzin lekcyjnych (45 min).
6. Szkolenia powinny być przeprowadzone w terminach uzgodnionych z Zamawiającym, zgodnie z harmonogramem szkolenia.
7. Uczestnicy muszą otrzymać materiały szkoleniowe w języku polskim.

III.1.2 Atakowanie i Ochrona Webaplikacji

2. Szkolenie realizowane w formule warsztatowej tj. oparte o realizację ćwiczeń praktycznych, które umożliwiają omawianie konkretnego ataku oraz rozwój umiejętności obrony przed nim.
3. Minimalny zakres szkolenia:
    a. Współczesne problemy bezpieczeństwa aplikacji webowych.
        i. zagrożenia wynikające z architektury webaplikacji (np. CGI, SSI, etc.)
        ii. zagrożenia wynikające z języków programowania (PHP, JS, etc.) i technologi, np. ASP, JSP
        iii. problem styku webaplikacji z bazą danych
        iv. interfejsy zewnętrzne webaplikacji
        v. zagrożenia po stronie serwera, środowiska, sieci, a zagrożenia po stronie klienta

vi. zagrożenia stron tworzonych pod urządzenia mobilne (telefony, tablety)

b. Ataki na aplikacje webowe – przykłady ataków oraz praktyczne metody ochrony.
   i. wyszukiwanie adresów serwerów deweloperskich
   ii. bezpieczeństwo hostingu i webserwera
   iii. brak obsługi błędów
   iv. manipulacje parametrami (metody GET, POST)
   v. techniki podsłuchu i manipulowania transmisją
   vi. atak Forcefull browsing
   vii. atak Path Traversal
   viii. technika Google Hacking
   ix. wstrzyknięcie kodu (PHP shell) i komend systemowych do webaplikacji
   x. problem filtrowania danych wejściowych
   xi. ataki XSS (persistent, reflected)
   xii. omijanie filtrowania danych wejściowych i encodingu wyjściowych
   xiii. ataki na sesję aplikacji webowej
   xiv. podsłuchiwanie sesji i kradzież ciasteczek HTTP
   xv. jak poprawnie zarządzać sesją w webapikacji?
   xvi. ataki CSRF/XSRF
   xvii. bezpieczny upload plików
   xviii. metody ułatwiające przetrwanie ataków DoS/DDoS
   xix. ataki Clickjacking
   xx. ataki na bazy danych
   xxi. ataki SQL injection i Blind SQL injection
   xxii. ochrona przed atakami SQL injection
   xxiii. szyfrowanie połączenia i ataki na SSL
   xxiv. szyfrowanie danych w webaplikacji
   xxv. ochrona przed spamem i enumeracją zasobów oraz haseł
   xxvi. podsumowanie zagrożeń i przegląd OWASP TOP10
   xxvii. pozaprogramistyczne środki ochrony (systemy IDS/IPS, WAF)
   xxviii. omijanie detekcji przez systemy WAF/IDS/IPS

c. Problemy przeglądarek internetowych.
    i. Same Orgin Policy
    ii. Rich Internet Applications
    iii. dziury w przeglądarkach
    iv. ataki DNS-Rebinding
    v. narzędzia podnoszące bezpieczeństwo i pomagające w testowaniu aplikacji webowych
d. Przegląd narzędzi automatyzujących wykrywanie podatności oraz ich praktyczne wykorzystanie
e. **Do każdego z powyższych punktów muszą zostać przygotowane laboratoria, podczas których należy przedstawić praktyczne metody ochrony przed konkretnym atakiem.**

4. Szkolenie "Atakowanie i Ochrona Webaplikacji" musi trwać **co najmniej 3 dni** szkoleniowe.
5. Szkolenie będzie prowadzone w języku polskim.
6. Wykonawca udostępni uczestnikom środowisko na którym będą odbywały się ćwiczenia. W razie konieczności Wykonawca jest zobowiązany do zapewnienia uczestnikom szkolenia oprogramowania umożliwiającego sprawne połączenie z takim środowiskiem. Wykonawca musi zapewnić odpowiednie środowisko szkoleniowe pozwalające na przeprowadzenie szkolenia w formule ” Bring Your Own Laptop”.
7. Za dzień szkoleniowy przyjmuje się min. 8 godzin lekcyjnych (45 min).
8. Szkolenia powinny być przeprowadzone w terminach uzgodnionych z Zamawiającym, zgodnie z harmonogramem szkolenia.
9. Uczestnicy muszą otrzymać materiały szkoleniowe w języku polskim

III.2 DOKUMENTACJA SZKOLENIOWA

1. Wykonawca przygotuje dokumentację szkoleniową związaną z realizacją tematu szkoleniowego obejmującą:
    a. Harmonogram szkoleń zawierający: temat szkolenia, terminy i godziny zajęć szkoleniowych, nazwiska trenerów.
    b. Program szkoleń uwzględniający zakresy tematyczne szkoleń.

c. Materiały szkoleniowe uwzględniające zakresy tematyczne poszczególnych szkoleń, obejmujące teoretyczne oraz praktyczne aspekty zagadnień poruszanych w trakcie każdego z tematów szkoleń (materiały szkoleniowe zawierać będą instrukcje, prezentacje, opracowania graficzne i treści z zakresu omawianego tematu szkolenia, wykorzystywane w trakcie jego trwania).
d. Listę obecności uczestników.
e. Imienne zaświadczenia o ukończeniu szkolenia.
f. Wypełnione protokoły odbioru szkoleń.

2. Wykonawca, najpóźniej **3 dni** po podpisaniu umowy przekaże Zamawiającemu do zaopiniowania **harmonogram szkoleń**. Zamawiający przekaże Wykonawcy opinię/uwagi/zalecenia do przedstawionego harmonogramu szkoleń w terminie **3 dni** od jego dostarczenia.
3. Wszystkie uwagi do **harmonogramu szkoleń** zgłoszone przez Zamawiającego zostaną wprowadzone przez Wykonawcę, w terminie nie dłuższym niż **2 dni** od dnia ich otrzymania.
4. Zamawiający w terminie **2 dni** od dnia dostarczenia przez Wykonawcę poprawionego **harmonogramu szkoleń**, poinformuje Wykonawcę o jego akceptacji lub konieczności wprowadzenia zmian.
5. Zamawiający nie później niż **5 dni** roboczych przed datą rozpoczęcia szkolenia, przekaże Wykonawcy w formie elektronicznej **wykaz uczestników** danej edycji szkolenia.
6. Wykonawca, najpóźniej **3 dni** przed rozpoczęciem szkolenia, przekaże **materiały szkoleniowe** wszystkim uczestnikom danej edycji szkolenia w formie elektronicznej (e-mail), na adresy poczty elektronicznej wskazane przez Zamawiającego.

III.3 ORGANIZACJA SZKOLEŃ

1. Zamawiający zapewni salę szkoleniową w swojej siedzibie tj. budynku Zachodniopomorskiego Urzędu Wojewódzkiego w Szczecinie przy ul. Wały Chrobrego 4.
2. Zamawiający zapewni w sali szkoleniowej dostęp do sieci Internet oraz sprzęt komputerowy w postaci laptopów dla każdego uczestnika.

3. Szkolenie z danego tematu rozpocznie i zakończy się w jednym tygodniu szkoleniowym w dniach od poniedziałku do piątku (np.: poniedziałek, wtorek, środa lub poniedziałek, środa, piątek itp.)
4. Szkolenia mogą rozpocząć się nie wcześniej niż o godz. 8.00 i zakończyć się nie później niż o godz. 15:00.
5. Wykonawca zapewni odpowiednie rozwiązania teleinformatyczne na potrzeby przeprowadzenia szkoleń, tj. dla każdego uczestnika dostęp do środowiska szkoleniowego, na którym uczestnicy będą wykonywali ćwiczenia i do której dostęp będzie posiadał trener.
6. Wykonawca przygotuje dla każdego z uczestników instrukcję dotyczącą sposobu korzystania z użytego przez Wykonawcę rozwiązania teleinformatycznego wykorzystanego do przeprowadzenia szkoleń.
7. Wykonawca zapewni każdemu uczestnikowi szkolenia komplet materiałów szkoleniowych.
8. Wykonawca po zakończeniu każdego szkolenia przygotuje dla każdego uczestnika imienne zaświadczenie o ukończeniu szkolenia, które będzie zawierało następujące informacje: imię i nazwisko uczestnika szkolenia, tytuł szkolenia, datę przeprowadzenia szkolenia, pieczątkę Wykonawcy, identyfikowalny podpis trenera prowadzącego szkolenie, liczbę godzin.
9. Wykonawca przekaże imienne zaświadczenia w wersji elektronicznej w ciągu **5 dni** od zakończenia każdej edycji szkolenia, na adresy mailowe uczestników każdej edycji szkolenia, a także elektronicznie do Zamawiającego z dołączeniem wykazu wydanych zaświadczeń potwierdzających ukończenie szkolenia.
10. Wypełniony protokół odbioru szkolenia wraz ze sprawozdaniem ze szkolenia, Wykonawca dostarczy Zamawiającemu w formie papierowej w ciągu 7 dni roboczych od zakończenia danej edycji szkolenia.

Rozdział IV. Termin realizacji Przedmiotu Zamówienia

1. Przedmiot zamówienia zostanie zrealizowany w terminie **nie dłuższym niż 30 dni** od dnia podpisania umowy.