Załącznik nr 5 do SWZ

**Szczegółowy opis próbki oraz zasady i zakres demonstracji**

 **Zakres i sposób dostarczenia – odbioru zestawu testowego do prezentacji wymaganych przez Zamawiającego funkcjonalności (dalej: rozwiązanie)**

1. Wykonawca dokona prezentacji oferowanego Systemu Symulator zagrożeń internetowych z wykorzystaniem zestawu testowego.

Zestaw testowy składany jest wraz z ofertą jako załącznik, podpisany przez osobę lub osoby uprawnione do reprezentowania wykonawcy, kwalifikowanym, osobistym lub zaufanym podpisem elektronicznym.

Prezentacja oferowanego rozwiązania odbędzie się na podstawie  scenariusza testowego opisanego w niniejszym dokumencie.

**Zestaw testowy** musi zawierać:

* aplikacja webowa symulator zagrożeń internetowych - adres strony www pod którym dostępna będzie aplikacja oraz dane umożliwiające uruchomienie aplikacji tj. loginy i hasła dostępowe.
1. Dostęp do łącza internetowego na potrzeby prezentacji oraz urządzenie (komputer przenośny- laptop) na którym będzie przeprowadzona prezentacja zapewnia zamawiający.
2. Niezłożenie zestawu testowego w miejscu i terminie wskazanym przez Zamawiającego lub nieprzystąpienie do prezentacji w wyznaczonym terminie skutkować będzie odrzuceniem oferty.
3. Zamawiający nie ponosi odpowiedzialności za:
	1. złożenie przez Wykonawcę zestawu testowego po wyznaczonym terminie,
	2. złożenie zestawu testowego w innym niż określonym przez Zamawiającego miejscu,
	3. złożenie zestawu testowego w sposób uniemożliwiający jego identyfikację lub postępowania, którego dotyczy.
4. Zamawiający nie przewiduje pokrycia kosztów przygotowania zestawu testowego oraz przeprowadzenia prezentacji.
5. Zamawiający nie wykorzysta zestawu testowego, o którym mowa powyżej do celów innych niż przeprowadzenie prezentacji rozwiązania.

**Zasady przeprowadzenia prezentacji wersji demonstracyjnej oferowanego rozwiązania**

1. Prezentacja zostanie przeprowadzona w dniu roboczym w siedzibie Zamawiającego tj. w budynku Urzędu Gminy Wojaszówka
2. Zamawiający powiadomi Wykonawcę, o terminie prezentacji z wyprzedzeniem co najmniej 3 dni roboczych.
3. Zamawiający zapewni na potrzeby przeprowadzenia prezentacji: salę, projektor, ekran, min. jedno gniazdo zasilania energią elektryczną o parametrach: 230 V, 50Hz z zabezpieczeniem 10A, oraz dostęp do łącza internetowego oraz urządzenie- komputer przenośny
4. Zamawiający zapewni komplet kabli i przewodów połączeniowych niezbędnych do przeprowadzenia testów.
5. Zamawiający **nie dopuszcza** prezentacji poglądowych z użyciem oprogramowania prezentacyjnego np. Microsoft Power Point, Zamawiający wymaga, aby prezentacja była przeprowadzona na działającej wersji demonstracyjnej systemu. W oparciu o przeglądarkę internetową
6. Zamawiający dopuszcza udział maksymalnie 3 przedstawicieli Wykonawcy do przeprowadzenia prezentacji.
7. Ze strony Zamawiającego podczas prezentacji będą obecni członkowie zespołu przetargowego powołanego przez Zamawiającego. Zamawiający sporządzi listę obecności osób biorących udział w prezentacji.
8. Zamawiający sporządzi pisemny protokół, w którym opisany będzie przebieg prezentacji. Protokół stanowić będzie załącznik do protokołu z postępowania.
9. Łączny czas prezentacji nie może przekroczyć 2 godzin zegarowych.
10. W trakcie prezentacji komputer z zestawu testowego, może łączyć się z Internetem tylko i wyłącznie w celu realizacji wskazanego scenariusza
11. Wykonawca w trakcie przygotowania się do prezentacji oraz w jej trakcie nie może dokonywać żadnych zmian w rozwiązaniu wynikającym ze zmiany kodów źródłowych.
12. Wykonawca w trakcie przygotowania się do prezentacji oraz w jej trakcie może wykonywać czynności na komputerze wyłącznie w czasie, gdy obraz z komputera jest wyświetlany za pomocą projektora.
13. W przypadku rozpoczęcia prezentacji później niż przewiduje to poniższy harmonogram prezentacji z winy leżącej po stronie Wykonawcy, Zamawiający nie przesunie terminu zakończenia prezentacji. Opóźnienia wynikające z winy Zamawiającego zostaną uwzględnione poprzez odpowiednie wydłużenie czasu prezentacji.
14. Wykonawca będzie zobowiązany do przeprowadzenia wszystkich prezentacji scenariuszy testowych o których mowa poniżej
15. Harmonogram i przebieg prezentacji będzie realizowany zgodnie z poniższym schematem:
	1. **W dniu prezentacji w godzinach 09:00 – 09:15:**
		1. Zamawiający zweryfikuje osoby, które są przedstawicielami Wykonawcy i będą dokonywały prezentacji. W tym celu każda z osób musi posiadać dokument potwierdzający prawo do udziału w prezentacji w imieniu Wykonawcy w czasie prezentacji (np. pełnomocnictwo)
		2. Strony dokonają ustaleń co do stanu faktycznego i kompletności zestawu testowego oraz dalszego przebiegu prezentacji. Wszelkie ustalenia zostaną zapisane w protokole prezentacji.
		3. Wykonawca przygotuje i uruchomi zestaw testowy.
		4. Zamawiający sporządzi listę obecności osób, które biorą udział w prezentacji. Lista obecności zostanie dołączona do protokołu z przeprowadzonej prezentacji.
	2. **W dniu prezentacji w godzinach 09:15 – 10:15**
		1. Wykonawca przystąpi do prezentacji rozwiązania na podstawie scenariusza opisanego przez Zamawiającego w niniejszym załączniku.
		2. Wykonawca będzie dokonywać prezentacji scenariuszy testowych zgodnie z kolejnością przedstawioną w niniejszym załączniku
		3. Wykonawca na wykonanie wszystkich scenariuszy testowych ma łącznie 1 godzinę zegarową licząc od godziny 09:15.
		4. W przypadku niepowodzenia prezentacji danego scenariusza testowego, Wykonawca może powtórzyć go nieograniczoną liczbę razy dokonując rekonfiguracji wersji demonstracyjnej rozwiązania. Przeprowadzenie powtórnej próby scenariusza testowego **nie wydłuża** łącznego czasu (1 godzina zegarowa) na przeprowadzenie prezentacji wszystkich scenariuszy testowych.
		5. W przypadku zaobserwowania usterek sprzętowych lub programowych wymagających wymiany lub naprawy komputera z zestawu testowego, prezentacja zostanie przełożona na inny dzień roboczy, który zostanie ustalony pomiędzy Wykonawcą i Zamawiającym. W przypadku braku możliwości naprawy usterki do tego czasu, skutkować będzie odrzuceniem oferty. Zamawiający dopuszcza **tylko jedną** możliwość przeprowadzenia prezentacji w dodatkowym terminie.
		6. W sytuacji, w której zachodzą przesłanki, o których jest mowa lit. e) powyżej Wykonawca przystąpi do prezentacji rozwiązania w ustalonym z Zamawiającym dodatkowym terminie. Przebieg prezentacji będzie zgodny z zapisami w niniejszym dokumencie.
		7. Zamawiający w trakcie trwania prezentacji **nie przewiduje** przerwy.
	3. W dniu prezentacji w godzinach 10:15 – 11:00
		1. Wykonawca dokona demontażu zestawu testowego i zwróci go Zamawiającemu.
		2. Przedstawiciele Wykonawcy i Zamawiającego podpiszą protokół z przebiegu prezentacji.

**SCENARIUSZ PREZENTACJI**

# OBSZAR: SYMULATOR ZAGROŻEŃ INTERNETOWYCH

Wykonawca w ramach scenariusza zobowiązany jest zaprezentować:

|  |  |
| --- | --- |
| **Lp.** | **Kroki do wykonania/Zakres prezentacji** |
| **1** | 1. Uruchomić przeglądarkę internetową, wpisać adres aplikacji i zalogować się do systemu.
2. Wywołać moduł szkoleniowy umożliwiający wybranie scenariusza dowolnego zagrożenia internetowego pokazujący mechanizmy działania przestępców internetowych
3. Wybrać sekcję która daje możliwość odfiltrowania umieszczonych w symulatorze zagrożeń internetowych - min 8 zagrożeń w szczególności:
4. Phishing Clone,
5. Phishing Spear,
6. Phishing Spear Chat,
7. Phishing Whaling,
8. Pharming,
9. Malware Post,
10. Malware Email,
11. Certyfikaty SSL (Certificate Fraud Chat)
12. Wybrać moduł edukacyjny i zaprezentować dostępne materiały szkoleniowe dotyczące zaimplementowanych w symulatorze scenariuszy cyberzagrożeń. Zaprezentować znajdujące się w symulatorze informacje na temat występowania oraz identyfikacji danego zagrożenia, sposobów zapobiegania, oraz informacji na temat, co użytkownik powinien w pierwszej kolejności zrobić, gdy zostanie już oszukany – czyli gdzie się zgłosić, jakie dane zabezpieczyć, zmienić hasła, czy zablokować karty płatnicze.
13. Przedstawić materiały edukacyjne dostępne na platformie (w formie plików PDF), na co zwrócić szczególną uwagę podczas korzystania portali społecznościowych, różnego rodzaju czatów, serwisów internetowych oraz odbierania wiadomości e-mail.
14. Zasymulować możliwość konwersacji przy wykorzystaniu czatu z fikcyjnymi użytkownikami (czat botami) namawiającymi do przekazywania danych osobowych/ danych poufnych.
15. Wybrać sekcję pozwalającą na przeglądanie wiadomości tekstowych w formie e-mail. Kliknięcie w sekcję pozwoli wyświetlić na ekranie symulowanego klienta pocztowego, który posiada skrzynkę odbiorczą z wiadomościami Email. Użytkownik może otwierać i czytać wybrane wiadomości email, może na nie odpowiadać i pobierać ich załączniki. Niektóre z tych wiadomości mogą stanowić symulację zagrożenia internetowego, a niektóre będą stanowić zwykłą wiadomość tekstową.
16. Wybrać sekcję pozwalającą na przeglądanie fikcyjnych i rzeczywistych postów społecznościowych zawierającą możliwe ataki phishingowe lub pharmingowe. W module postów społecznościowych będą znajdować się zarówno „rzeczywiste” posty nie stanowiące zagrożenia jaki i posty z potencjalnymi symulowanymi cyberatakami.
17. Zaprezentować możliwość dodawania nowych fałszywych witryn (podstron) nakłaniających użytkowników do pobierania zainfekowanych załączników, podawania danych wrażliwych oraz dokonywania płatności internetowych.
18. Przestawić jeden scenariusz dla cyberzagrożenia - ,,malware email’’. Symulacja scenariusza w którym zalogowany na platformie użytkownik otrzymuje podejrzanego mailia z zainfekowanym plikiem powodującym instalację złośliwego oprogramowania. Scenariusz musi zawierać również informacje jak zapobiegać tego typu atakom.
 |