Załącznik nr 10

Szczegółowy specyfikacja przedmiotu zamówienia części II

|  |
| --- |
|  |
| **Przedmiot zamówienia:** | **Szkolenia online z zakresu cyberbezpieczeństwa** | **Potwierdzenie spełnienia wymagań (Należy wpisać SPEŁNIA oraz podać istotne informacje faktyczne oferowanego szkolenia)\*** |
| **Nazwa:** | **(należy wpisać nazwę szkolenia)** |
| **Ilość:** | Dla 20 osób |
| **Okres gwarancji producenta:**  |  |
| **Parametry** |
| Opis | Przedmiotem zamówienia jest kompleksowa usługa „Podnoszenia Świadomości Bezpieczeństwa” (Security Awareness), umożliwiająca przeprowadzenie kampanii edukacyjnej z zakresu podstaw bezpieczeństwa w internecie. Dedykowana jest użytkownikom Zamawiającego i świadczona przez okres 6 miesięcy. |  |
| Usługa musi zawierać: | 1. Platformę szkoleniową zawierającą minimum 45 szkoleń, dostępnych w języku polskim (oraz w jęz. angielskim, niemieckim, hiszpańskim, czeskim, słowackim, serbskim, chorwackim i włoskim), w postaci filmów i prezentacji, zakończonych testami lub quizami sprawdzającymi przyswojenie przedstawianego materiału merytorycznego.
	1. Szkolenia muszą zapewniać zakres tematyczny co najmniej w ujęciu:
		1. Podstawy bezpiecznego internetu
		2. Bezpieczeństwo poczty
		3. Załączniki w poczcie elektronicznej
		4. Phishing
		5. Spyware/malware
		6. Bezpieczeństwo danych osobowych RODO/GDRP
		7. Bezpieczne hasła
		8. Menedżery haseł
		9. Bezpieczeństwo urządzeń mobilnych
		10. Uwierzytelnianie wieloskładnikowe (MFA)
		11. Bezpieczna praca zdalna
		12. Bezpieczna praca w biurze
		13. Sieci społeczne
		14. Socjotechnika stosowana
		15. Zakupy w internecie
	2. Użytkownicy powinni być podzieleni na grupy, dla których będą przygotowane indywidualne harmonogramy szkoleń oraz dedykowane kampanie phishingowe.
	3. Łączny czas trwania wszystkich materiałów szkoleniowych powinien wynosić co najmniej 8 godzin.
2. Dedykowaną platformę phishingową pozwalającą na generowanie i wysyłanie spreparowanych maili phishingowych do wszystkich użytkowników usługi oraz na generowanie, co najmniej, poniższych typów wiadomości e-mail
	1. z linkiem prowadzącym do stronnym internetowej,
	2. z linkiem do portalu podszywającego się pod usługodawcę i pozwalającego na logowanie (weryfikację, czy użytkownicy są gotowi na fałszywej stronie portalu zalogować się swoim loginem i hasłem); platforma musi zapewniać bezpieczeństwo takiej operacji,
	3. z załącznikiem (szyfrowanym i niezaszyfrowanym) zawierającym potencjalnie niebezpieczny kod,
	4. z załącznikiem w postaci dokumentu Word lub Excel zawierającym potencjalnie niebezpieczny kod.
	5. W przypadku, gdy użytkownik pozwoli się oszukać, platforma musi posiadać możliwość automatycznego skierowania takiego użytkownika na dodatkowe szkolenie lub ponowne wykonanie jednego z wcześniej ukończonych szkoleń.
3. dedykowaną platformę dostarczającą raporty obejmujące minimum:
	1. status wykonania szkoleń przez użytkowników, z podziałem na grupy i uwzględnieniem terminu wykonania szkoleń oraz wyniku quizów i testów,
	2. status kampanii, wraz z raportem o liczbie wysłanych e-maili oraz szczegółach zwierających informację: kto otworzył wiadomość, kto i kiedy pozwolił się oszukać, kto otworzył załącznik, jaka była platforma z jakiej wykonał tę akację oraz szczegółowe daty wykonania tych operacji.

W ramach świadczonej usługi usługodawca musi:* przygotować platformę do świadczenia usługi, założyć konta dla użytkowników oraz sprawdzić techniczne elementy związane z zapewnieniem dostarczenia wiadomości phishingowych z platformy do użytkowników,
* zaproponować do akceptacji Zamawiającego szczegółowy harmonogram szkoleń dopasowany do okresu świadczenia usługi,
* zaplanować na podstawie harmonogramu całą kampanię szkoleniową i dostarczyć ją użytkownikom za pośrednictwem dedykowanych wiadomości e-mail,
* dostarczać pełny raport z realizacji szkoleń dla użytkowników oraz przeprowadzonych kampanii po zakończeniu każdego modułu szkoleniowego oraz zbiorcze raporty końcowe,
* wprowadzić zmiany w harmonogramie i zakresie szkoleń w przypadku potrzeby modyfikacji, zmian kolejności szkoleń lub liczby użytkowników (nie więcej niż 5 zmian w okresie trwania usługi).
 |  |
| Wymagania dodatkowe | Usługa ma być świadczona z centrum danych znajdującym się na terenie Unii Europejskiej. Dostawca platformy musi zapewnić całkowite usunięcie danych użytkowników po zakończeniu realizacji usługi. Wszystkie moduły (platforma szkoleniowa, platforma phishingowa i moduł raportowania) muszą pochodzić od jednego producenta.Dla zapewnienia wysokiego poziomu usług, podmiot świadczący usługę musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług. Zgłoszenia i komunikacja z usługodawcą będą przyjmowane w języku polskim w trybie 8x5, przez dedykowany portal serwisowy dostępny w sieci internet oraz infolinię w języku polskim 8x5. Czas reakcji usługodawcy nie może być dłuższy niż 1 godzina – reakcja w postaci połączenia telefonicznego lub odpowiedzi w portalu serwisowym. |  |
|  |  |

UWAGA:
Wypełnioną i podpisaną tabelę należy złożyć wraz z ofertą.

\*Prawą stronę tabeli należy wypełnić stosując słowa „spełnia” lub „nie spełnia”, zaś w przypadku żądania wykazania wpisu określonych parametrów, należy wpisać oferowane konkretne, rzeczowe wartości. W przypadku, gdy Wykonawca, w którejkolwiek z pozycji wpisze słowa „nie spełnia” lub zaoferuje niższe wartości, oferta zostanie odrzucona, gdyż jej treść nie odpowiada treści SWZ