Opis przedmiotu zamówienia

**CYKL SZKOLEŃ Z CYBERBEZPIECZEŃSTWA x 3**

**I.**        **Szkolenie:**

1. Szkolenia będą odbywać się w formie stacjonarnej w siedzibie zamawiającego na ul. Ogrodowa 10, 88-300 Mogilno.
2. Szkolenia będą dedykowane tematycznie dla działu: kadry zarządzającej 16 os., działu IT 2 os. oraz pracowników 65 os. (w podziale na dwie grupy).
3. Szkolenie musi składać się z teorii oraz prezentacji przykładów praktycznych.
4. Zamawiający zapewnia dostęp do sali szkoleniowej oraz rzutnika.
5. Ramowy program szkolenia:
6. Podstawy bezpieczeństwa w sieci;
7. Typy ataków np. kody QR, linki, Phishing, Typosquatting, ataki socjotechniczne;
8. Hasła i polityka haseł;
9. Zasady ochrony poczty elektronicznej;
10. Ochrona danych osobowych, wycieki danych;
11. Poprawne reagowanie na cyberataki;
12. Bezpieczeństwo fizyczne i zasady używania nośników danych;
13. Bezpieczeństwo w mediach społecznościowych;
14. Praca zdalna i jej bezpieczeństwo;
15. Kopie zapasowe i kopie bezpieczeństwa.

***Wymagania wobec Wykonawcy:***

1.    Wykonawca zobowiązany jest do zapewnienia:

a.    Trenera prowadzącego posiadającego co najmniej 2-letnie doświadczenie w zakresie prowadzenia szkoleń dotyczących zagadnień cyberbezpieczeństwa lub pokrewnych.

b.     Zamawiający zapewnia książeczki instruktażowe w wersji papierowej i elektronicznej. Oznakowania materiałów szkoleniowych logotypami programu zgodnie z wytycznymi programu Cyberbezpieczny Samorząd.

2.    Szkolenia będą prowadzone w godzinach pracy Zamawiającego.

3.    Harmonogram szkoleń:

I szkolenie – marzec/kwiecień 2025 r.

II szkolenie – wrzesień 2025 r.

III szkolenie – luty/marzec 2026 r.

**Cz. II: Przeprowadzenie testów socjotechnicznych**

1. Przedmiotem zamówienia jest przeprowadzenie podwójnych testów socjotechnicznych na pracownikach polegających na wykonaniu rekonesansu organizacji, kampanii phishingowej, kampanii vishingowej i testów w kontakcie bezpośrednim. Drugi test przeprowadzony zostanie w przeciągu kilku miesięcy po pierwszym teście, aby potwierdzić/sprawdzić odporność jednostki na cyberataki.
2. Zakresem testów socjotechnicznych będzie:
3. W ramach rekonesansu organizacji Wykonawca przeprowadzi wywiad polegający na gromadzeniu oraz analizie informacji na temat pracowników i struktury organizacji i pozyska informacje z ogólnodostępnych źródeł.
4. W ramach kampanii phishingowej Wykonawca opracuje co najmniej 2 scenariusze kampanii phishingowej i wykona symulację ataku polegającą w szczególności na wysłaniu maili nakłaniających do podania hasła dostępowego do jednego z systemów Zamawiającego i/lub nakłaniających do zainstalowania złośliwego oprogramowania.
5. W ramach kampanii vishingowej Wykonawca opracuje co najmniej 1 scenariusz kampanii vishingowej i wykona symulację ataku polegającą w szczególności na wykonaniu telefonów do wybranych pracowników nakłaniających do przekazania dostępu do komputera/telefonu służbowego lub informacji wrażliwych.
6. W ramach kontaktu bezpośredniego Wykonawca opracuje co najmniej 1 scenariusz kontaktu bezpośredniego i wykona próbę fizycznego, nieautoryzowanego wejścia do pomieszczeń Zamawiającego oraz co najmniej 5 prób nakłaniania pracowników do przekazania dostępu do komputera/telefonu służbowego, uruchomienia oprogramowania dostarczonego na nośniku zewnętrznym lub przekazania innych informacji wrażliwych.
7. Wykonawca po wykonanych testach opracuje dokumentację – raport z przeprowadzonych testów. Dokumentacja musi zawierać co najmniej:
8. Opis opracowanych scenariuszy kampanii phishingowej, kampanii vishingowej i prób kontaktu bezpośredniego.
9. Rezultaty przeprowadzonych symulacji i prób w podziale na scenariusze ze statystykami osiągniętych celów i oszacowaniem ryzyka czynnika ludzkiego dla organizacji.
10. Podsumowanie wyników i analiz dla Kierownictwa.

Wykonawca zaprezentuje raport z omówieniem Kierownictwu oraz dostarczy raport z przeprowadzonych testów w wersji elektronicznej w formacie pdf.