”Cyberbezpieczny Samorząd” - Zadanie 2 - Obszar kompetencyjny

1. Szkolenia dla pracowników z cyberbezpieczeństwa:

Szkolenia te są istotne dla pracowników Jednostki nadrzędnej oraz w Jednostkach Podległych, łącznie 7 Jednostek, ponieważ pomagają zwiększyć świadomość i umiejętności w dziedzinie cyberbezpieczeństwa, co z kolei przyczynia się do zwiększenia bezpieczeństwa organizacji przed atakami internetowymi:

Proponowany obszar szkoleń:

1. Świadomość cyberbezpieczeństwa - podstawowe zasady ochrony danych osobowych i informacji w sieci.
2. Identifikacja zagrożeń cybernetycznych - nauka rozpoznawania ataków phishingowych, malware'u i innych form ataków internetowych.
3. Zapobieganie atakom cybernetycznym - jak chronić swoje urządzenia i systemy przed atakami z zewnątrz.
4. Reagowanie na incydenty cybernetyczne - kroki do podjęcia w przypadku wykrycia ataku cybernetycznego oraz procedury raportowania incydentów.
5. Zasady korzystania z internetu i mediów społecznościowych - bezpieczne praktyki przeglądania internetu oraz komunikacji online.
6. Istotność bezpiecznego hasła - jak tworzyć i przechowywać silne hasła do swoich kont online.
7. Kultura cyberbezpieczeństwa - promowanie odpowiedzialnego zachowania pracowników w zakresie ochrony danych i informacji firmowych.

Po każdym szkoleniu możliwość szkoleń online dla danej grupy w Jednostkach wykonawca przeprowadzi symulacje phisingu kontrolowanego, po przeprowadzeniu ataku przekaże wyniki w postaci naruszenia cyberbezpieczentwa wraz z danymi użytkownika, który nie odrzucił i odczytał zainfekowaną wiadomość.

Dzięki przeprowadzeniu symulacji phisingu kontrolowanego, wykonawca może zidentyfikować potencjalne luki w cyberbezpieczeństwie danej grupy oraz dostarczyć konkretnych danych na temat tego, jakie konsekwencje mogą wyniknąć z odczytania zainfekowanej wiadomości. Dzięki temu użytkownicy będą bardziej świadomi zagrożeń i będą bardziej ostrożni w swoich działaniach online. W ten sposób szkolenia mogą przyczynić się do zwiększenia ogólnego poziomu cyberbezpieczeństwa w danej organizacji.

Dla wszystkich uczestników zostaną przesłane materiały szkoleniowe z przeprowadzonych szkoleń.

Czas na przeprowadzenie szkoleń do 04.2026r. dla wszystkich 7 jednostek łącznie ok. 600 osób Zamawiający po wyborze oferty przekaże nazwy i adresy jednostek.

2. Specjalistyczne Certyfikowane Szkolenia dla pracowników IT

Wykonawca wybrany w postępowaniu oferuje Certyfikowane Szkolenia dla 3 pracowników IT tj. specjalistyczne szkolenia dla pracowników IT z zakresu cyberbezpieczeństwa oraz specjalistycznych urządzeń zapory sieciowej typu UTM.

Podczas certyfikowanych szkoleń powinny zostać przedstawione praktycznie m.in.

1. Analiza ryzyka cybernetycznego i strategie zarządzania ryzykiem
2. Wykrywanie i reagowanie na incydenty bezpieczeństwa
3. Ochrona sieci przed atakami typu phishing, ransomware i malware
4. Monitoring ruchu sieciowego oraz analiza logów zdarzeń
5. Konfiguracja i zarządzanie urządzeniami UTM: nauka konfiguracji firewalla, filtrów URL oraz innych funkcji bezpieczeństwa UTM.
6. Wykrywanie i zapobieganie atakom złośliwego oprogramowania: nauka sposobów identyfikacji i neutralizacji różnych rodzajów szkodliwego oprogramowania.
7. Skanowanie ruchu sieciowego: poznanie metod skanowania ruchu sieciowego w celu wykrywania potencjalnych zagrożeń.
8. Ochrona przed atakami DDoS: nauka strategii i narzędzi do efektywnej obrony przed atakami DDoS.
9. Monitorowanie i analiza ruchu sieciowego: praktyczne szkolenia z analizy danych dotyczących ruchu sieciowego w celu wykrywania podejrzanych aktywności.
10. Zarządzanie incydentami bezpieczeństwa: nauka procedur i praktycznych technik radzenia sobie z incydentami bezpieczeństwa.
11. Aktualizacje i utrzymanie systemów UTM: zapoznanie się z procedurami aktualizacji oprogramowania oraz zapewnienie ciągłości działania systemów UTM.

Czas na przeprowadzenie szkoleń od dnia zawarcia umowy do 04.2026r.

Powyższe zapisy maja na celu **oszacować kwotę** jaką Zamawiający poniesie na realizacje w/w zadań. Po oszacowaniu kwoty Zamawiający ogłosi zapytanie właściwe celem wybrania Wykonawcy do realizacji Zadania 2.