Znak: ITI.271.3.2026

Załącznik nr 4
do zapytania ofertowego ITI.271.3.2026 z dnia 01.07.2026 r.

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

do **ZAPYTANIA OFERTOWEGO z dnia 01.07.2026 r.**

dla zamówienia, którego wartość nie przekracza 170 000 zł bez podatku od towarów i usług.

Postępowanie o udzielenie zamówienia publicznego na zadanie
pn. **„Realizacja usług doradczych, konsultingowych oraz szkoleniowych w zakresie bezpieczeństwa informacji oraz cyberbezpieczeństwa w ramach projektu »Wzmocnienie systemu cyberbezpieczeństwa Gminy Raków - Cyberbezpieczny Samorząd« - Zadanie 1 - Obszar organizacyjny – pkt 1 oraz Zadanie 2 - Obszar kompetencyjny – pkt 1, pkt 2, pkt 3”**
(numer referencyjny postepowania: ITI.271.3.2026).

Ze względu na różne zakresy usług, a co za tym idzie z uwagi na chęć poszerzenia kręgu ewentualnych wykonawców Zamawiający dzieli zamówienie na 4 części, których przedmiotem są:

1.1.1. **Część I: Realizacja usług doradczych i konsultingowych:**
- 1.1.1.1. Wykonanie przeglądu i aktualizacji dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji w tym wykonaniu analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podjęcie działań minimalizujących to ryzyko.

1.1.2. **Część II: Realizacja usług szkoleniowych – rodzaj 1:**
- 1.1.2.1. Wykonanie szkolenia specjalistycznego dla kadry informatycznej JST w zakresie cyberbezpieczeństwa.

1.1.3. **Część III: Realizacja usług szkoleniowych – rodzaj 2:**
- 1.1.3.1. Wykonanie szkolenia z zakresu cyberbezpieczeństwa dla wybranych przedstawicieli kadry JST, istotnych z punktu widzenia systemu zarządzania bezpieczeństwem informacji.
- 1.1.3.2. Wykonanie szkolenia dla pracowników JST budujące świadomość cyberzagrożeń i przedstawiające sposoby ochrony przed nimi.

Wymienione wyżej usługi muszą zostać wykonane dla 2 jednostek Gminy Raków tj. Urzędu Gminy w Rakowie oraz Gminnego Ośrodka Pomocy Społecznej w Rakowie.

1. WYMAGANIA DLA POSZCZEGÓLNYCH CZĘŚCI.

1.1. Część I. Realizacja usług doradczych i konsultingowych.

1.1.1. Wykonanie przeglądu i aktualizacji dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji w tym wykonanie analizy ryzyka utraty integralności, dostępności lub poufności informacji oraz wskazanie działań minimalizujących to ryzyko – na rzecz Urzędu Gminy w Rakowie. **– 1 szt.**

1.1.2. Wykonanie przeglądu i aktualizacji dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji w tym wykonanie analizy ryzyka utraty integralności, dostępności lub poufności informacji oraz wskazanie działań minimalizujących to ryzyko – na rzecz Gminnego Ośrodka Pomocy Społecznej w Rakowie – **1 szt.**

Kod CPV: 79417000-0 – Usługi doradcze w zakresie bezpieczeństwa.

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

I. Wymagania ogólne.

Usługi, o których mowa wyżej muszą zostać wykonane dla dwóch jednostek organizacyjnych Gminy Raków:

1. Urzędu Gminy w Rakowie (z siedzibą przy ul. Ogrodowej 1, 26-035 Raków);
2. Gminnego Ośrodka Pomocy Społecznej w Rakowie (z siedzibą przy ul. Jana Sienieńskiego 19, 26-035 Raków).

Jednostki te posiadają wdrożony Systemu Zarządzania Bezpieczeństwem Informacji (**dalej SZBI**).
Dokumentacja, jak również wszelkie inne materiały i informacje związane z SZBI ww. jednostek mogą zostać udostępniona do analizy i uzgodnień wyłącznie w siedzibach tych jednostek (lub dla obu jednostek jednocześnie w siedzibie Urzędu Gminy w Rakowie) dla Wykonawcy wybranemu w niniejszym postępowaniu, z którym zostanie podpisana stosowna umowa zapewniająca zachowania bezpieczeństwa i poufności.
Ze względu na newralgiczny charakter informacji związanych z infrastrukturą teleinformatyczną i techniczną jednostek, informacji o ryzykach oraz środkach ochrony zasobów jednostek Zmawiający nie dopuszcza możliwości wzajemnego przekazywania tychże danych za pomocą środków komunikacji elektronicznej, gdyż zwiększa to ryzyko nieuprawnionego do nich dostępu. Zamawiający dopuszcza przetwarzanie ww. danych w infrastrukturze Wykonawcy wyłącznie na czas opracowywania aktualizacji SZBI, pod warunkiem zapewnienia przez Wykonawcę adekwatnych środków bezpieczeństwa, w tym w szczególności szyfrowania nośników danych, na których przetwarzane są te dane. Po zakończeniu usługi potwierdzonym protokołem odbioru Wykonawca zobowiązany będzie do usunięcia ze swoich zasobów wszelkich danych związanych z przygotowaną przez niego dokumentacją.

II. Aktualizacja SZBI.

Zamawiający wymaga przeprowadzenia analizy obecnie funkcjonującego SZBI i jego ewentualnego dostosowania do obowiązujących standardów bezpieczeństwa informacji - w szczególności w zakresie wymagań stawionych przez Ustawę z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U.2026.20 t.j. ze zm.) oraz zgodności z wymaganiami normy PN-ISO/IEC 27001.
Przez dostosowanie Zamawiający rozumie aktualizację lub przygotowanie nowych/brakujących procedur, a nie ich realizację (przykład: wykonanie analizy polityki kopii zapasowych, na jej podstawie przygotowanie przez Wykonawcę ewentualnych rekomendacji i finalnej procedury odpowiadającej obowiązującym standardom w tym zakresie, a nie wykonanie kopii).
W szczególności Zamawiający kładzie nacisk na aktualizację procedur związanych z zarządzeniem ryzykiem oraz ciągłością działania jednostek.

III. Wymagane kwalifikacje.

Zamawiający wymaga, aby usługa wykonana została profesjonalnie, rzetelnie, z należytą starannością i z najlepszą wiedzą przez Wykonawcę.
Wobec powyższego Zamawiający wymaga posiadania przez Wykonawcę lub pracownika/ów Wykonawcy odpowiedzialnego/ych za bezpośrednie wykonanie usługi obowiązującego certyfikatu PN-ISO/IEC 27001 lub równoważnego, którego autentyczność można zweryfikować za pomocą strony www organizacji wystawiającej certyfikat. **Certyfikat należy dołączyć do oferty celem potwierdzenia**.

IV. Termin wykonania usługi.

Zamawiający wymaga, aby usługa wykonana została od **29 lipca 2026 r.** do **7 sierpnia 2026 r.** (daty włącznie). Wskazany okres jest okresem maksymalnym, w którym usługa musi zostać zrealizowana, jednak Wykonawca nie musi jej realizować w pełnym wymiarze tego okresu – jeżeli uzna, iż wykonał usługę w pełni może zgłosić gotowość do odbioru usługi w dowolnym momencie tego okresu.
Przy czym należy wskazać, że komunikacja pomiędzy Zamawiającym a Wykonawcą i dostępność personelu Zamawiającego obowiązuje w dni robocze w godzinach pracy jednostek tj. dla Urzędu Gminy w Rakowie - poniedziałek, środa, czwartek, piątek: od godz. 7:30 do 15:00, wtorek: od godz. 7:30 do 17:30; dla Gminnego Ośrodka Pomocy Społecznej w Rakowie - poniedziałek, środa, czwartek, piątek: od godz. 7:30 do 15:30, wtorek: od godz. 7:30 do 16:30.

V. Przekazanie ostatecznej dokumentacji Zamawiającemu i praw do niej.

Zamawiający wymaga, aby wszelka dokumentacja przygotowana w ramach realizacji usługi przekazana została Zamawiającemu w 2 egz. w formie wydruku podpisanego przez Wykonawcę oraz w formie elektronicznej edytowalnej (plik DOCX lub ODT) oraz w formacie PDF (forma elektroniczna podpisana kwalifikowanym podpisem elektronicznym) na trwałym nośniku danych, pozbawionym wad fizycznych, prawnych oraz znanych podatności/zagrożeń teleinformatycznych.

Ponadto Zamawiający wymaga, aby Wykonawca przeniósł na Zmawiającego z dniem ich udostępnienia majątkowe prawa autorskie do każdej dokumentacji wytworzonej w trakcie współpracy dotyczącej przedmiotu umowy w rozumieniu ustawy o prawie autorskim i prawach pokrewnych w związku z wykonywaniem umowy.
Przeniesienie majątkowych praw autorskich obejmuje następujące pola eksploatacji:

1. posiadanie, korzystanie, przenoszenie, prezentowanie, publikowanie, rozpowszechnianie utworu – w celach niekomercyjnych na potrzeby własne;
2. powielanie całości lub części utworu dowolną techniką, w tym w formie papierowej, elektronicznej, wizualnej lub fonograficznej – w celach niekomercyjnych na potrzeby własne,
3. przetwarzanie/zmiana całości lub części utworu w celu sporządzenia własnych materiałów, prezentacji, programów szkoleniowych, opracowań, raportów, zestawień, informacji – w celach niekomercyjnych na potrzeby własne.

Wraz z przeniesieniem majątkowych praw autorskich, w ramach wynagrodzenia za wykonaną usługę Zamawiający wymaga, aby Wykonawca zezwalał Zamawiającemu na wykonywanie autorskich praw zależnych do tych utworów oraz przenosi na Zamawiającego prawo własności nośników utworów.

Przygotowane w ramach usługi dokumenty (w formie papierowej jaki i elektronicznej) muszą być czytelne i uporządkowane, tak aby Zamawiający mógł w łatwy sposób z nich korzystać i je modyfikować w razie potrzeb.

Informacja: Koniec opisu Części I.

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

2.1. Część II. Realizacja usług szkoleniowych – rodzaj 1:

2.1.1. Wykonanie szkolenia specjalistycznego dla kadry informatycznej JST w zakresie cyberbezpieczeństwa – na rzecz Urzędu Gminy w Rakowie. **– 1 szt.**

Kod CPV: 80550000-4 – Usługi szkolenia w dziedzinie bezpieczeństwa.

I. Wymagania ogólne.

Zamawiający wymaga przeszkolenia **1** osoby (pracownika Urzędu Gminy w Rakowie) w zakresie podstawowych i zaawansowanych wdrożeń otwarto źródłowego systemu do monitorowania cyberbezpieczeństwa klasy SIEM/XDR – **WAZUH**.

II. Zakres szkolenia.

Minimalna liczba godzin szkolenia: 32 godziny zegarowe.
Minimalny zakres merytoryczny szkolenia:
Szkolenie powinno obejmować zagadnienia teoretyczne oraz praktyczne warsztaty dotyczące wdrażania, konfiguracji, administracji i wykorzystania systemu Wazuh jako platformy SIEM/XDR oraz monitorowania bezpieczeństwa infrastruktury IT.

1. Wprowadzenie do Wazuh
- architektura i komponenty systemu Wazuh,
- możliwości platformy w zakresie SIEM, XDR, HIDS i monitorowania zgodności,
- omówienie scenariuszy zastosowań w środowiskach produkcyjnych.

2. Instalacja i wdrożenie
- wymagania sprzętowe i systemowe,
- instalacja serwera Wazuh,
- konfiguracja środowiska,
- instalacja i konfiguracja agentów dla systemów Linux i Windows,
- konfiguracja monitorowania urządzeń bezagentowych (Agentless, Syslog, SSH).

3. Administracja i konfiguracja
- zarządzanie konfiguracją serwera i agentów,
- zarządzanie regułami detekcji oraz dekoderami,
- tworzenie i modyfikacja własnych reguł,
- konfiguracja polityk bezpieczeństwa,
- diagnostyka i rozwiązywanie problemów (troubleshooting).

4. Monitorowanie bezpieczeństwa
- analiza logów i zdarzeń bezpieczeństwa,
- monitorowanie integralności plików (File Integrity Monitoring),
- wykrywanie podatności i monitorowanie konfiguracji systemów,
- monitorowanie zgodności z wymaganiami bezpieczeństwa (Compliance),
- analiza alertów i korelacja zdarzeń.

5. Reagowanie na incydenty
- identyfikacja i analiza incydentów bezpieczeństwa,
- automatyzacja reakcji na zdarzenia,
- wykorzystanie mechanizmów Active Response,
- praktyczne scenariusze obsługi incydentów.

6. Zarządzanie środowiskiem Wazuh
- zabezpieczanie infrastruktury Wazuh,
- zarządzanie użytkownikami i uprawnieniami,

- konfiguracja klastra Wazuh,
- skalowanie środowiska i zapewnienie wysokiej dostępności.

7. Konfiguracje zaawansowane

- optymalizacja wydajności systemu,
- dostrajanie reguł detekcji,
- ograniczanie liczby fałszywych alarmów,
- tworzenie własnych mechanizmów detekcji.

8. Integracje

- integracja z systemami Windows i Linux,
- integracja z urządzeniami sieciowymi oraz źródłami logów,
- integracja z narzędziami bezpieczeństwa i orkiestracji (SOAR),
- wykorzystanie zewnętrznych źródeł Threat Intelligence.

9. Warsztaty praktyczne – do samodzielnej realizacji

Szkolenie powinno obejmować ćwiczenia praktyczne polegające na:

- instalacji i konfiguracji środowiska,
- podłączaniu agentów,
- tworzeniu reguł i dekoderów,
- analizie logów,
- wykrywaniu podatności,
- obsłudze incydentów,
- integracji z wybranymi systemami,
- samodzielnym rozwiązywaniu typowych problemów administracyjnych.

Wymagania organizacyjne

- szkolenie prowadzone przez trenera posiadającego praktyczne doświadczenie we wdrażaniu systemu Wazuh,
- zapewnienie materiałów szkoleniowych w formie elektronicznej,
- udostępnienie scenariuszy ćwiczeń praktycznych,
- wydanie imiennych certyfikatów ukończenia szkolenia.

III. Termin i miejsce wykonania usługi.

Zamawiający wymaga, aby usługa wykonana została od **15 lipca 2026 r.** do **31 sierpnia 2026 r.** (daty włącznie).

Wskazany okres jest okresem maksymalnym, w którym usługa musi zostać zrealizowana, jednak Wykonawca nie musi jej realizować w pełnym wymiarze tego okresu – jeżeli uzna, iż wykonał usługę w pełni może zgłosić gotowość do odbioru usługi w dowolnym momencie tego okresu.

Zamawiający dopuszcza możliwość wykonania usługi w trybie online.

Informacja: Koniec opisu Części II.

3.1. Część III. Realizacja usług szkoleniowych – rodzaj 2.

3.1. Wykonanie szkolenia z zakresu cyberbezpieczeństwa dla wybranych przedstawicieli kadry JST, istotnych z punktu widzenia systemu zarządzania bezpieczeństwem informacji – na rzecz Urzędu Gminy w Rakowie oraz Gminnego Ośrodka Pomocy Społecznej w Rakowie. – **1 szt.**

3.2. Wykonanie szkolenia dla pracowników JST budującego świadomość cyberzagrożeń i przedstawiającego sposoby ochrony przed nimi – na rzecz Urzędu Gminy w Rakowie oraz Gminnego Ośrodka Pomocy Społecznej w Rakowie. – **1 szt.**

Kod CPV: 80550000-4 – Usługi szkolenia w dziedzinie bezpieczeństwa.

I. Wymagania dla pkt. 3.1.

1. Zamawiający wymaga przeszkolenia **8 osób** z zakresu cyberbezpieczeństwa dla wybranych przedstawicieli kadry JST, istotnych z punktu widzenia systemu zarządzania bezpieczeństwem informacji – na rzecz Urzędu Gminy w Rakowie oraz Gminnego Ośrodka Pomocy Społecznej w Rakowie.
2. Zamawiający wymaga potwierdzenia przeszkolenia osób (certyfikaty imienne).
3. Miejsce, termin i czas szkolenia: siedziba Urzędu Gminy w Rakowie, ul. Ogrodowa 1, 26-035 Raków, termin: **30 lipca 2026 r.** od. godz. 8.00. **Czas szkolenia – min. 4 godziny zegarowe + 15 minutowe przerwy po każdej godzinie zegarowej.**
4. Zamawiający zapewnia pomieszczenie do przeprowadzenia szkolenia oraz urządzenie multimedialne do wyświetlania materiałów edukacyjnych.
5. **Szczegółowy zakres szkolenia teoretycznego powinien obejmować co najmniej następujące zagadnienia:**
   a. **Najważniejsze wymagania wprowadzone przez Ustawę z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa** (Dz.U.2026.20 t.j. ze zm.).
   b. **Standardy dobrych praktyk bezpieczeństwa informacji i cyberbezpieczeństwa:**
      i. **ISO 27001, NIS 2 i ich odniesienie do pracy jednostki samorządu terytorialnego**: Kluczowe standardy bezpieczeństwa informacji: ISO 27001 i NIS 2 - jak te standardy mogą być wdrażane w jednostkach samorządu terytorialnego. Praktyczne przykłady implementacji oraz korzyści wynikające z przestrzegania tych standardów.
      ii. **Odpowiedzialność najwyższego kierownictwa w zakresie bezpieczeństwa cyfrowego**: Obowiązki spoczywające na najwyższym kierownictwie organizacji w zakresie zapewnienia bezpieczeństwa cyfrowego, w tym m.in. konieczność tworzenia strategii, monitorowania przestrzegania procedur oraz reagowania na incydenty.
   c. **Co robić, gdy systemy IT przestają działać - jak przygotować się na sytuacje kryzysowe:**
      i. **Systemy zarządzania ciągłością działania**: Znaczenie systemów zarządzania ciągłością działania (BCM) w kontekście zapewnienia nieprzerwanego funkcjonowania organizacji w przypadku awarii systemów IT. Opis powinien zawierać elementy takie jak identyfikacja kluczowych zasobów, planowanie awaryjne oraz procedury odtwarzania systemów po incydencie.
      ii. **Planowanie, przygotowanie, regularne testowanie strategii i procedur**: Jak organizacja może skutecznie planować i przygotowywać się na sytuacje kryzysowe, w tym regularne testowanie planów i procedur awaryjnych, organizowanie szkoleń dla pracowników oraz przeprowadzanie symulacji incydentów.

d. **Cyfrowe bezpieczeństwo fizyczne:**
   i. **Dostęp do obiektu instytucji administracji publicznej i samorządowej**: Jak zabezpieczyć fizyczny dostęp do obiektów, w których przechowywane są wrażliwe dane cyfrowe, przed atakami hackerskimi i innymi formami zagrożeń fizycznych - kontrola dostępu, monitoring oraz zabezpieczenia przed włamaniami.
   ii. **Zapewnienie bezpieczeństwa fizycznego dla dokumentów**: Należy przedstawić metody zabezpieczania dokumentów, które są przechowywane w budynkach instytucji, przed nieautoryzowanym dostępem lub kradzieżą. Szkolenie powinno obejmować procedury przechowywania, kontrolę dostępu oraz systemy zabezpieczające.
   iii. **Dostęp fizyczny do sprzętu i oprogramowania IT**: Należy omówić, jak organizacja może chronić swój sprzęt i oprogramowanie IT przed fizycznym dostępem osób niepowołanych, co może prowadzić do poważnych naruszeń bezpieczeństwa cyfrowego.

e. **Bezpieczeństwo cyfrowe organizacji:**
   i. **Omówienie zakresu obszarów bezpieczeństwa cyfrowego w organizacji**: W tym punkcie należy przedstawić kompleksowe podejście do zarządzania bezpieczeństwem cyfrowym, obejmujące procesy wewnętrzne organizacji, infrastrukturę IT oraz fizyczne zabezpieczenia obiektu. Opis powinien uwzględniać, jak te obszary współdziałają w celu ochrony danych, systemów i zasobów przed różnorodnymi zagrożeniami cyfrowymi oraz jakie standardy i procedury są wdrażane, aby zapewnić ciągłość działania organizacji.
   ii. **Omówienie niebezpieczeństw cybernetycznych dla instytucji administracji publicznej**: Ten podpunkt powinien zawierać analizę najczęstszych cyber zagrożeń, z jakimi spotykają się instytucje administracji publicznej. Należy omówić konkretne przypadki, takie jak ataki phishingowe, ransomware, czy DDoS, oraz przedstawić skutki takich incydentów. Ważnym elementem będzie również omówienie, które części infrastruktury są najbardziej narażone i jakie działania prewencyjne mogą zostać podjęte.
   iii. **Przegląd najczęstszych form ataków i metod zmniejszania ryzyka**: należy przedstawić szczegółowy opis typowych form ataków, takich jak malware, phishing, ransomware, oraz omówić ich potencjalne konsekwencje dla instytucji publicznych. Szkolenie powinno również obejmować strategie i narzędzia stosowane do zmniejszania ryzyka, takie jak regularne aktualizacje systemów, szkolenia pracowników, implementacja zaawansowanych systemów zabezpieczeń oraz monitorowanie aktywności sieciowej.

f. **Szpiegostwo informacyjno-cyfrowe - insider threat:**
   i. **Zagrożenia administracji samorządowej działaniami hybrydowymi**: W tym punkcie należy szczegółowo omówić specyfikę zagrożeń hybrydowych, które mogą łączyć elementy cybernetyczne, informacyjne oraz fizyczne, ukierunkowane na destabilizację funkcjonowania administracji samorządowej. Należy przedstawić przykłady takich działań oraz metody obrony przed nimi.
   ii. **Wywiad gospodarczy a szpiegostwo przemysłowe**: Należy rozróżnić wywiad gospodarczy od szpiegostwa przemysłowego, wskazując na różnice w metodach pozyskiwania informacji oraz na możliwe cele tych działań. Opis powinien zawierać przykłady technik, takich jak podsłuchy, infiltracja, phishing ukierunkowany, oraz omówienie, jak takie działania mogą zagrażać bezpieczeństwu cyfrowemu organizacji.

iii. **Działania sabotażowe i dywersyjne**: W tej części należy omówić, jak działania sabotażowe i dywersyjne mogą wpłynąć na cyfrowe bezpieczeństwo organizacji. Należy przedstawić przykłady takich działań, jak uszkodzenie infrastruktury IT, złośliwe wprowadzenie wirusów czy manipulacja danymi, oraz omówić środki zapobiegawcze, które mogą minimalizować ryzyko takich ataków.

iv. **Metody i formy prowadzenia wrogiego rekonesansu**: Szkolenie powinno zawierać przegląd technik rekonesansu stosowanych przez atakujących w celu zdobycia informacji o organizacji, które mogą być później wykorzystane do przeprowadzenia skutecznego ataku. Należy omówić techniki, takie jak analiza ruchu sieciowego, inżynieria społeczna, OSINT (Open Source Intelligence), oraz ich znaczenie w kontekście przygotowania do ataku.

v. **HUMINT i OSINT w zdobywaniu wiedzy**: Należy omówić, jak metody HUMINT (Human Intelligence) i OSINT są wykorzystywane do zdobywania informacji na temat organizacji, które mogą zostać użyte do szpiegostwa lub sabotażu. Należy uwzględnić przykłady działań takich jak zbieranie danych od wewnętrznych informatorów, analiza publicznie dostępnych źródeł informacji oraz wpływ takich działań na bezpieczeństwo cyfrowe organizacji.

vi. **Radykalizacja pracowników i petentów**: Opis powinien skupić się na zagrożeniach wynikających z radykalizacji pracowników oraz petentów, które mogą prowadzić do działań szkodliwych dla organizacji, takich jak sabotaż, przecieki informacji, czy ataki fizyczne. Należy również omówić, jak organizacja może monitorować i przeciwdziałać takim zagrożeniom.

vii. **Polityka zabezpieczenia obiektu**: W tym podpunkcie należy omówić zasady i procedury mające na celu zabezpieczenie obiektu przed nieuprawnionym dostępem oraz ingerencją ze strony osób trzecich. Zakres powinien obejmować zabezpieczenia fizyczne, takie jak kontrola dostępu, monitoring, jak również aspekty związane z ochroną danych cyfrowych znajdujących się w obiekcie.

viii. **Procesy typowania, opracowania i pozyskania do współpracy insidera**: Należy omówić, jak przestępcy mogą typować i pozyskiwać insiderów w organizacji, jakie metody stosują do ich przekonania do współpracy oraz jakie kroki organizacja może podjąć, aby zidentyfikować i zapobiec takim działaniom.

ix. **Metody pozyskiwania insidera przez stronę trzecią**: Należy omówić metody, jakimi strony trzecie mogą próbować pozyskiwać insiderów w organizacji, takie jak szantaż, przekupstwo czy manipulacja emocjonalna. Należy również omówić sposoby minimalizowania ryzyka takich działań.

x. **Przykłady ataków inicjowanych przez insidera**: Należy przedstawić przykłady rzeczywistych ataków, które zostały zainicjowane przez insiderów, wskazując na ich skutki oraz na błędy organizacyjne, które umożliwiły przeprowadzenie tych ataków.

xi. **Najczęstsze błędy w zarządzaniu organizacją**: Należy omówić najczęstsze błędy w zarządzaniu, które mogą prowadzić do zwiększenia ryzyka skutecznych ataków przez insiderów, takie jak brak odpowiednich procedur bezpieczeństwa, niewystarczające szkolenia pracowników czy zaniedbania w zakresie monitorowania i audytów.

xii. **Socjotechnika, deepfake, spoofing i dezinformacja jako narzędzia ataku**: Zakres powinien obejmować szczegółowe omówienie nowoczesnych technik socjotechnicznych, takich jak deepfake, spoofing i dezinformacja, które są wykorzystywane do manipulowania i wprowadzania w błąd pracowników organizacji w celu przeprowadzenia ataku.

xiii. **Narzędzia i czynniki umożliwiające zminimalizowanie zagrożeń**: Należy przedstawić narzędzia i strategie, które organizacja może wdrożyć, aby minimalizować ryzyko wystąpienia zagrożeń, takie jak wdrożenie zaawansowanych systemów monitorowania, regularne audyty bezpieczeństwa czy programy szkoleniowe dla pracowników.

xiv. **Procesy wykrywania działań insidera**: Opis powinien obejmować omówienie procesów i narzędzi, które mogą być użyte do wykrywania działań insidera w organizacji, takich jak analiza anomalii w systemach IT, monitorowanie działań pracowników oraz techniki identyfikacji zagrożeń.

g. **Podróże służbowe, sympozja, konferencje – biznesowa rzeczywistość a wysokie ryzyko pozyskania danych:**

i. **Czynniki stanowiące realne zagrożenie poza siedzibą organizacji**: Należy omówić specyficzne zagrożenia, na jakie narażeni są pracownicy podczas podróży służbowych, konferencji i sympozjów, takie jak przechwycenie danych, podsłuchy, kradzież urządzeń mobilnych, czy inżynieria społeczna.

ii. **Właściwe przygotowanie podróży**: Najlepsze praktyki w zakresie przygotowania się do podróży służbowej z punktu widzenia bezpieczeństwa, w tym zabezpieczenie urządzeń, przygotowanie planu reagowania na incydenty oraz zapoznanie się z lokalnymi zagrożeniami cyfrowymi.

iii. **Zachowanie podczas wyjazdu**: Należy omówić, jak pracownicy powinni postępować podczas wyjazdów, aby minimalizować ryzyko utraty danych, w tym bezpieczne korzystanie z urządzeń elektronicznych, unikanie publicznych sieci Wi-Fi oraz zachowanie ostrożności w miejscach publicznych.

iv. **Najlepsze praktyki zmniejszające ryzyko**: Najlepsze praktyki, które mogą znacząco zmniejszyć ryzyko narażenia organizacji na zagrożenia podczas wyjazdów służbowych, takie jak stosowanie VPN, szyfrowanie danych, regularne aktualizacje oprogramowania oraz świadomość zagrożeń.

v. **Katalog podmiotów i organizacji podejrzewanych o niejawne zbieranie danych**

vi. **Scenariusze i narzędzia służące przejęciu danych**: Omówienie scenariuszy, które mogą prowadzić do przejęcia danych podczas podróży służbowych, takie jak ataki man-in-the-middle, kradzież urządzeń, czy podstępne zdobywanie informacji przez osoby trzecie.

vii. **Cyfrowe aspekty w polityce bezpieczeństwa wyjazdów służbowych**: Należy omówić, jak organizacje mogą włączyć aspekty cyfrowego bezpieczeństwa do polityki dotyczącej wyjazdów służbowych, w tym zarządzanie urządzeniami mobilnymi, monitorowanie działań pracowników oraz zapewnienie wsparcia technicznego podczas wyjazdów.

II. Wymagania dla pkt. 3.2.

1. Zamawiający wymaga przeszkolenia **31 osób (podzielonych na 2 grupy) -** pracowników JST - w zakresie budowania świadomości cyberzagrożeń i przedstawienia sposobów ochrony przed nimi – na rzecz Urzędu Gminy w Rakowie oraz Gminnego Ośrodka Pomocy Społecznej w Rakowie.
2. Zamawiający wymaga potwierdzenia przeszkolenia osób (certyfikaty imienne).
3. Miejsce, termin i czas szkolenia: siedziba Urzędu Gminy w Rakowie, ul. Ogrodowa 1, 26-035 Raków, termin: **2 dni szkoleniowe – 1 dzień na 1 grupę - (14 lipca 2026 r.,** oraz **11 sierpnia 2026 r.)** każdy od. godz. 8.00. **Czas szkolenia w każdym z dni – min. 4 godziny zegarowe + 15 minutowe przerwy po każdej godzinie zegarowej.**

4. Zamawiający zapewnia pomieszczenie do przeprowadzenia szkolenia oraz urządzenie multimedialne do wyświetlania materiałów edukacyjnych.
5. **Szczegółowy zakres szkolenia teoretycznego powinien obejmować co najmniej następujące zagadnienia:**
   a. **Wprowadzenie do bezpieczeństwa cyfrowego w organizacji**
      i. Omówienie zakresu niebezpieczeństw cybernetycznych, którym najczęściej poddane są instytucje administracji publicznej i samorządowej.
      ii. Przegląd najczęstszych form ataków i ich konsekwencji dla instytucji administracji publicznej, w tym samorządowej oraz metod zmniejszania potencjalnego ryzyka w realizacji bieżących zadań - na przykładach z ostatnich 6 m-cy.
   b. **Cyfrowe bezpieczeństwo fizyczne. Podstawowe zasady bezpieczeństwa fizycznego w kontekście możliwych ataków cyfrowych:**
      i. Dostęp do obiektu instytucji administracji publicznej i samorządowej (ataki hackerskie typu "tailgating" i inne formy wejść i zagrożeń fizycznych).
      ii. Zapewnienie bezpieczeństwa fizycznego dla dokumentów fizycznie umieszczonych w budynku instytucji.
      iii. Dostęp fizyczny do sprzętu i oprogramowania IT w Urzędzie, w tym zewnętrzne nośniki pamięci cyfrowej.
   c. **Cyberbezpieczeństwo:**
      i. Podstawowe zasady higieny i bezpieczeństwa cyfrowego w jednostce administracji publicznej i samorządowej na przykładach: ataki wykorzystujące inżynierię społeczną, ataki złośliwym oprogramowaniem, próby wyłudzenia danych.
      ii. Korzystanie z poczty elektronicznej - szyfrowanie danych, budowanie bezpiecznych haseł, zagrożenie przejęcia poczty służbowej i prywatnej, możliwe symptomy infekcji komputera.
      iii. Uwierzytelnianie dwuskładnikowe - powody, metody, narzędzia.
      iv. Metody zmniejszania potencjalnego ryzyka w realizacji bieżących zadań.
      v. Komunikacja kryzysowa – co należy zrobić w przypadku wystąpienia incydentu.
   d. **Bezpieczeństwo danych instytucji administracji publicznej i samorządowej – czynnik ludzki:**
      i. Rozmowy o pracy w miejscach publicznych – zasady bezpiecznych rozmów, czego unikać, jak ograniczyć ryzyko.
      ii. Udostępnianie zewnętrzne – zasady kwalifikacji, przesyłanie danych e-mailem, przenoszenie na pendrive, korzystanie z nośników reklamowych, wykorzystanie folderów współdzielonych i tymczasowych, szyfrowanie.
      iii. Makra – wykorzystanie do ataków, kiedy włączać makra, jak unikać zagrożeń.
      iv. Usuwanie danych – jak zadbać o dane, jak przechowywać dane, miejsca przechowywania danych.
      v. RODO – podstawowe wymagania, jak działać zgodnie z RODO, na co zwracać uwagę w codziennej pracy.
   e. **Bezpieczna praca z przeglądarką:**
      i. Strony szyfrowane – jak rozpoznać strony szyfrowane i nieszyfrowane, co mówi nam oznaczenie https i kłódka, jak sprawdzić, czy strona jest bezpieczna, pułapki https, nowe oznaczenia szyfrowania.
      ii. Certyfikaty – co oznacza SSL, jak sprawdzić certyfikat strony, na co zwrócić uwagę.
   f. **Prywatne działania w sieci i ekspozycja na zagrożenia cyfrowe instytucji publicznej i samorządowej:**
      i. Zagrożenia związane z używaniem poczty prywatnej do celów służbowych.

ii. Potencjalne konsekwencje dla Urzędu wynikające z przejęcia prywatnego konta pracownika na portalu społecznościowym.
iii. Zagrożenia wykorzystywania służbowych urządzeń mobilnych do celów prywatnych.
iv. Bezpieczeństwo psychiczne w używaniu portali społecznościowych.
v. Wykorzystanie sztucznej inteligencji do ataków socjotechnicznych.

g. **Sprzęt służbowy, praca zdalna:**
   i. Na co warto zwrócić uwagę w kontekście bezpieczeństwa, pracując z domu lub w podróży.

Informacja: Koniec opisu Części III.

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską