*Załącznik nr 2 do zapytania ofertowego*

ZAMAWIAJĄCY:

Gmina Brześć Kujawski

pl. Władysława Łokietka 1

87-880 Brześć Kujawski

e-mail: urzad@brzesckujawski.pl

Nr referencyjny BI.II.271.10.2025.NŻ

**OPIS PRZEDMIOTU ZAMÓWIENIA**

1. **Przedmiotem zamówienia jest wykonanie usług szkoleniowych oraz audytów cyberbezpieczeństwa dla Urzędu Miejskiego w Brześciu Kujawskim oraz jednostek podległych w ramach Konkursu Grantowego „Cyberbezpieczny Samorząd”, Priorytet II: Zaawansowane usługi cyfrowe, działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa,   
   w ramach Funduszy Europejskich na rozwój cyfrowy 2021-2027 (FERC) ramach projektu grantowego „Cyberbezpieczny Samorząd”, który jest podzielony na dwie części:**

**Część 1: Szkolenia w zakresie cyberbezpieczeństwa dla pracowników i kadry kierowniczej oraz dostęp do platformy szkoleniowej** **dla pracowników Urzędu Miejskiego w Brześciu Kujawskim   
i jednostek podległych**

**Część 2: Audyty cyberbezpieczeństwa dla Urzędu Miejskiego oraz jednostek podległych**

**Opis zasad warunków równoważności:**

* Za równoważne do wyspecyfikowanego rozwiązania Zamawiający uzna rozwiązanie o tym samym przeznaczeniu, cechach technicznych, jakościowych i funkcjonalnych odpowiadających cechom technicznym, jakościowym i funkcjonalnym wskazanych w opisie przedmiotu zamówienia, lub lepszych, oznaczonych innym znakiem towarowym, patentem lub pochodzeniem.
* Rozwiązanie równoważne musi pozwalać na zrealizowanie zakładanego przez Zamawiającego celu poprzez parametry wydajnościowe i funkcjonalne, mające wpływ na skuteczność działania, takie same lub lepsze od wskazanych wymagań minimalnych.
* Użycie w opisie przedmiotu zamówienia nazw rozwiązań, materiałów i urządzeń służy ustaleniu minimalnego standardu wykonania i określenia właściwości i wymogów technicznych założonych w dokumentacji technicznej dla projektowanych rozwiązań.
* Wykonawca zobligowany jest do wykazania, że oferowane rozwiązania równoważne spełnią zakładane wymagania minimalne.
* Brak określenia „minimum” oznacza wymaganie na poziomie minimalnym, a Wykonawca może zaoferować rozwiązanie o lepszych parametrach.
* W celu zachowania zasad neutralności technologicznej i konkurencyjności dopuszcza się rozwiązania równoważne do wyspecyfikowanych, przy czym za rozwiązanie równoważne uważa się takie rozwiązanie, które pod względem technologii, wydajności i funkcjonalności nie odbiega lub jest lepsze od technologii funkcjonalności i wydajności wyszczególnionych w rozwiązaniu wyspecyfikowanym.
* Nie podlegają porównaniu cechy rozwiązania właściwe wyłącznie dla rozwiązania wyspecyfikowanego, takie jak: zastrzeżone patenty, własnościowe rozwiązania technologiczne, własnościowe protokoły itp., a jedynie te, które stanowią o istocie całości zakładanych rozwiązań technologicznych i posiadają odniesienie w rozwiązaniu równoważnym. W związku z tym, Wykonawca może zaproponować rozwiązania, które realizują takie same funkcjonalności wyspecyfikowane przez Zamawiającego w inny, niż podany sposób.
* Przez bardzo zbliżoną (podobną) wartość użytkową rozumie się podobne, z dopuszczeniem nieznacznych różnic nie wpływających w żadnym stopniu na całokształt systemu, zachowanie oraz realizowanie podobnych funkcjonalności w danych warunkach, dla których to warunków rozwiązania te są dedykowane. Rozwiązanie równoważne musi zawierać dokumentację potwierdzającą, że spełnia wymagania funkcjonalne Zamawiającego, w tym wyniki porównań, testów czy możliwości oferowanych przez to rozwiązanie w odniesieniu do rozwiązania wyspecyfikowanego. W tym przypadku należy do postępowania dołączyć wszelkie dowody wskazujące na spełnienie niniejszych wymagań.

1. **Część I: Szkolenie z zakresu cyberbezpieczeństwa dla pracowników oraz kadry kierowniczej oraz dostęp do platformy szkoleniowej dla pracowników Urzędu Miejskiego w Brześciu Kujawskim   
   i jednostek podległych**

**Etap I: Dostęp do platformy szkoleniowej dla pracowników Urzędu Miejskiego w Brześciu Kujawskim i jednostek podległych**

Zamówienie obejmuje dostęp do materiałów szkoleniowych z zakresu cyberbezpieczeństwa w ramach zakupu dostępu do platformy szkoleniowej, na której pracownicy urzędu i jednostek podległych będą mogli na bieżąco szkolić się z zakresu cyberbezpieczeństwa. Materiały szkoleniowe muszą być przez Wykonawcę na bieżąco uzupełniane i aktualizowane, w związku z pojawieniem się nowych zagrożeń i podatności, nowych metod ochrony informacji i narzędzi do tego wykorzystywanych oraz zmieniającej się sytuacji geopolitycznej.

**Materiały tematyczne powinny obejmować zagadnienia związane m.in. z:**

* podstawy cyberbezpieczeństwa (podstawowe pojęcia i zasady działania),
* cyberbezpieczeństwo w codziennej pracy urzędu,
* standardy i najlepsze praktyki postępowania w celu zapewnienia cyberbezpieczeństwa w urzędzie, cyberhigiena,
* bezpieczeństwo urządzeń i bezpieczeństwo fizyczne, bezpieczne hasła, zarządzanie hasłami, uwierzytelnienie wieloskładnikowe, klucze sprzętowe,
* przegląd i rozpoznawanie najpopularniejszych zagrożeń (w tym rodzaje ataków, ransomware i malware, phishing, fake newsy, atak telefoniczny, spoofing), sposoby unikania zagrożeń, zasady bezpiecznego korzystania z Internetu,
* ochrona informacji i prywatność w Internecie,
* jak bezpiecznie korzystać z narzędzi teleinformatycznych w urzędzie – przykłady stosowania zabezpieczeń,
* reagowanie na incydenty bezpieczeństwa (w tym zasady postępowania w razie podejrzenia naruszenia bezpieczeństwa/ataku),
* procedury zgłaszania incydentów (w tym zgłaszanie incydentów do CSIRT NASK),
* socjotechnika, przykłady zastosowania.
  + - 1. Dostęp do platformy szkoleniowej obejmuje od dnia zawarcia umowy do 30.06.2026 r.

Ilość przyznanych dostępów do materiałów szkoleniowych: 340 osób

**Platforma szkoleniowa powinna zapewnić:**

- możliwość generowania imiennych certyfikatów po ukończeniu szkolenia

- elastyczny dostęp do aktualnych szkoleń w dogodnym dla nich czasie przez cały okres dostępu do platformy

- udostępniane kursy i materiały szkoleniowe powinny być na bieżąco uzupełniane i aktualizowane, w związku z pojawieniem się nowych zagrożeń i podatności, nowych metod ochrony informacji i narzędzi do tego wykorzystywanych

- interfejs w języku polskim

- możliwość sprawdzenia nabytej wiedzy poprzez testy na końcu kursu

- widoczność, na jakim etapie jest realizowany dany kurs (informacja, ile zostało mu do końca szkolenia, np. slajd 7/30, pytanie 4 z 30, ect.)

- materiały szkoleniowej muszą być wzbogacone o materiały multimedialne pod postacią filmów poglądowych, animacje, itp.

- generowanie raportów zbiorczych dla każdego użytkownika, każdego szkolenia oraz dla wszystkich użytkowników wraz ze szczegółami dotyczącymi postępów i wyników testów,

- dostęp do panelu administracyjnego, w którym uprawniony użytkownik może przeglądać postępy indywidualne każdego z pozostałych,

Udostępnienie platformy obejmuje jej utrzymanie oraz serwisowanie w przypadku awarii. Czas reakcji na zgłoszenia dotyczące **błędów krytycznych**, które uniemożliwiają korzystanie z platformy, wynosi **maksymalnie 12h**, a czas na usunięcie błędu – **maksymalnie 48h**

Czas reakcji na zgłoszenia dotyczące **pozostałych błędów** (niekrytycznych) wynosi maksymalnie 2 dni, a czas na ich usunięcie wynosi do 7 dni roboczych.

Czas jest liczony od momentu zgłoszenia w przypadku gdy zgłoszenie ma miejscu podczas czasu pracy/dostępności serwisu lub od czasu rozpoczęcia pracy serwisu w kolejnym dniu roboczym następującym po dniu zgłoszenia.

Termin udostępnienia platformy wraz z całością materiałów szkoleniowych – najpóźniej 30 dni po podpisaniu umowy.

**Wykonawca zobowiązany jest do realizacji zamówienia zgodnie z wymogami określonymi poniżej:**

1. Wykonawca zapewni:
   1. osobę prowadzącą szkolenie, która posiada wiedzę, doświadczenie i umiejętności adekwatne do rodzaju i zakresu merytorycznego szkolenia, zdolną do pełnej realizacji wymogów związanych z prowadzeniem szkolenia;
   2. wydanie uczestnikom szkolenia po jego zakończeniu zaświadczenia/certyfikatu o ukończeniu szkolenia;
   3. prowadzenie dokumentacji szkolenia, na którą składa się lista uczestników szkolenia, którym wydano zaświadczenia/certyfikaty o ukończeniu szkolenia;
   4. oznakowanie w odpowiedni sposób wszelkiej dokumentacji szkolenia, zgodnie z zasadami oznakowania projektu grantowego pn.: „Cyberbezpieczny Samorząd”;
2. **Etap II: Szkolenie z zakresu cyberbezpieczeństwa dla pracowników oraz kadry kierowniczej**

**Minimalny zakres tematyczny szkolenia:**

* + 1. Co nam zagraża? Co dzieje się obecnie w Polsce i na świecie? Przykłady ataków.
    2. Kradzieże i wyłudzenia informacji – przykłady z życia urzędów
    3. Kultura ochrony informacji, dojrzałość organizacji.
    4. Straty wynikające z udanego ataku na firmę – omówienie i przykłady.
    5. Bezpieczeństwo w organizacji. Obowiązki jednostek publicznych wynikające z aktualnego stanu prawnego w obszarze bezpieczeństwa informacji - KRI – Krajowe Ramy Interoperacyjności.
    6. Składowe systemu zarządzania bezpieczeństwem informacji.
    7. Socjotechniki, przykłady zastosowania.
    8. Metody codziennej ochrony informacji - praca z danymi osobowymi w urzędzie i poza nim, fizyczne bezpieczeństwo miejsca pracy, dobre praktyki.
    9. Rodzaje ataków:
       - poczta elektroniczna;
       - ataki BPC, BEC, APT;
       - komunikatory;
       - programy biurowe (MS Office);
       - ataki pasożytnicze;
       - ataki ransomware i jak z nimi sobie radzić.
    10. Cyberbezpieczeństwo w pracy zdalnej – omówienie, dobre praktyki/wskazówki.
    11. Szyfrowanie dokumentów w ramach dostępnych funkcji w pakiecie Office.
    12. Szyfrowanie dowolnego pliku programem zewnętrznym.
    13. Bezpieczeństwo urządzeń mobilnych.
    14. Fake news - jak je identyfikować i walka z fałszywymi wiadomościami.
    15. OSINT (biały wywiad) przykłady i zastosowanie w Urzędzie.
    16. Sesja pytań i odpowiedzi.

**W przypadku szkoleń dla kadry kierowniczej, tematyka podanych zagadnień powinna także uwzględniać obowiązki ciążące na kadrze kierowniczej oraz zawierać dodatkowe tematy:**

* + 1. Rola i obowiązki kadry kierowniczej w zakresie cyberbezpieczeństwa wynikające z aktów prawnych i wdrożonych polityk.
    2. Organy i instytucje zwalczające zagrożenia w cyberprzestrzeni.
    3. Charakterystyka stopni alarmowych CRP – zagrożenia i obowiązki.

**Wymagania dotyczące organizacji szkoleń:**

**Szkolenie z zakresu cyberbezpieczeństwa dla pracowników Urzędu Miejskiego w Brześciu Kujawskim**

* + 1. szkolenie odbędzie się w trybie stacjonarnym:
* dla pracowników Urzędu Miejskiego w Brześciu Kujawskim na terenie Urzędu Miasta, adres   
  pl. Władysława Łokietka 1, 87-880 Brześć Kujawski w terminie do 30 września 2025 r.
  + 1. Wykonawca przeprowadzi szkolenie w 3 grupach, przy czym szkolenia tych grup nie mogą trwać jednocześnie, aby nie powodować utrudnień w ciągłości pracy danej Jednostki;
    2. w szkoleniu udział będzie brało 66 pracowników (podzielonych na 3 grup);
    3. szkolenie dla jednej grupy powinno trwać minimum 3 godziny zegarowe (łącznie z przerwami);
    4. szkolenie powinno odbyć się w dni robocze, w godzinach pracy Urzędu Zamawiającego;
    5. szkolenie musi być prowadzone w języku polskim;

**Szkolenie z zakresu cyberbezpieczeństwa dla kadry kierowniczej – Urzędu Miejskiego w Brześciu Kujawskim, istotnych z punktu widzenia polityki bezpieczeństwa informacji i systemu zarządzania bezpieczeństwem informacji.**

* + 1. szkolenie odbędzie się w trybie stacjonarnym:
* dla pracowników Urzędu Miejskiego w Brześciu Kujawskim na terenie Urzędu Miasta, adres   
  pl. Władysława Łokietka 1, 87-880 Brześć Kujawski w terminie do 30 września 2025 r.
  + 1. Wykonawca przeprowadzi szkolenie w 2 grupach, przy czym szkolenia tych grup nie mogą trwać jednocześnie, aby nie powodować utrudnień w ciągłości pracy danej Jednostki;
    2. w szkoleniu udział będzie brało 11 pracowników (podzielonych na 2 grupy);
    3. Szkolenie dla jednej grupy powinno trwać minimum 3 godziny zegarowe (łącznie z przerwami);
    4. Szkolenie powinno odbyć się w dni robocze, w godzinach pracy Urzędu Zamawiającego;
    5. Szkolenie musi być prowadzone w języku polskim;

**Wykonawca zobowiązany jest do realizacji zamówienia zgodnie z wymogami określonymi poniżej:**

* 1. Wykonawca zapewni:
     1. osobę prowadzącą szkolenie, która posiada wiedzę, doświadczenie i umiejętności adekwatne do rodzaju i zakresu merytorycznego szkolenia, zdolną do pełnej realizacji wymogów związanych z prowadzeniem szkolenia;
     2. wydanie uczestnikom szkolenia po jego zakończeniu zaświadczenia/certyfikatu o ukończeniu szkolenia;
     3. prowadzenie dokumentacji szkolenia, na którą składają się:
        1. lista obecności uczestników szkolenia,
        2. lista uczestników szkolenia, którym wydano zaświadczenia/certyfikaty o ukończeniu szkolenia;
     4. oznakowanie w odpowiedni sposób wszelkiej dokumentacji szkolenia, zgodnie z zasadami oznakowania projektu grantowego pn.: „Cyberbezpieczny Samorząd”;
  2. Wykonawca zobowiązany jest po przeprowadzeniu szkolenia do przekazania dokumentacji szkolenia zamawiającemu w wersji papierowej;
  3. Wykonawca pokrywa wszelkie koszty związane z wykonaniem przedmiotu zamówienia, w tym koszty swojego ewentualnego zakwaterowania, dojazdu, wyżywienia, przygotowania materiałów szkoleniowych (druku itp.).

1. **Część II: Przeprowadzenie audytów KRI dla Urzędu Miejskiego w Brześciu Kujawskim oraz jednostek podległych**

Zakres i przedmiot audytu KRI obejmuje przegląd systemów pod kątem zarządzania bezpieczeństwem informacji, umożliwiających realizację i egzekwowanie działań:

* 1. zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia;
  2. utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację;
  3. przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy;
  4. podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji;
  5. bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4;
  6. zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak:
     1. zagrożenia bezpieczeństwa informacji,
     2. skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna,
     3. stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich;
  7. zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez:
     1. monitorowanie dostępu do informacji,
     2. czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,
     3. zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji;
  8. ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość;
  9. zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie;
  10. zawierania w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji;
  11. ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych;
  12. zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na:
      1. dbałości o aktualizację oprogramowania,
      2. minimalizowaniu ryzyka utraty informacji w wyniku awarii,
      3. ochronie przed błędami, utratą, nieuprawnioną modyfikacją,
      4. stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa,
      5. zapewnieniu bezpieczeństwa plików systemowych,
      6. redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,
      7. niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,
      8. kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa;
  13. bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących;
  14. zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.
  15. rozliczalność w systemach teleinformatycznych podlega wiarygodnemu dokumentowaniu w postaci elektronicznych zapisów w dziennikach systemów (logach).

**Harmonogram poszczególnych audytów:**

* + 1. Audyt dla Urzędu Miejskiego w Brześciu Kujawskim
       1. Audyt KRI nr 1 – do 31 czerwca 2025 r.
       2. Audyt KRI nr 2 – do 30 grudnia 2025 r.
       3. Audyt KRI nr 3 – na zakończenie projektu „Cyberbezpieczny Samorząd” przez Zamawiającego, jednak nie później niż do 20.06.2026 r.
    2. Audyt dla jednostek podległych
       1. Ilość jednostek podległych: 10
       2. Audyt KRI – na zakończenie projektu „Cyberbezpieczny Samorząd” przez Zamawiającego, jednak nie później niż do 20.06.2026 r.

**W ramach realizacji przedmiotu zamówienia Wykonawca zobowiązany będzie do:**

1. dokonania oceny zgodności funkcjonujących zasad i procedur dotyczących zarządzania bezpieczeństwem informacji, w tym przetwarzania danych osobowych, zgodnie z § 19 rozporządzeniem Rady Ministrów z dnia 21 maja 2024r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. poz. 773),
2. opracowania dokumentacji poaudytowej – raportu z wytycznymi do doskonalenia i rekomendacjami. Dokumentacja poaudytowa (raport) ma być przygotowana zgodnie z zasadami dostępności cyfrowej dokumentów tekstowych opisanymi na stronie https://www.gov.pl/web/dostepnosc-cyfrowa/jak-zwiekszyc-dostepnosc-cyfrowa-dokumentow-tekstowych oraz oznaczona pełnokolorowym znakiem Funduszy Europejskich, znakiem barw RP i znakiem UE lub znakiem monochromatycznym (zgodnie z Podręcznikiem wnioskodawcy i beneficjenta Funduszy Europejskich na lata 2021-2027 w zakresie informacji i promocji).

**Szczegółowe parametry zamówienia:**

1. **Urząd Miejski w Brześciu Kujawskim**
   1. Ilość pracowników: 89
   2. Ilość lokalizacji: 5
   3. Ilość serwerów fizycznych: 1
   4. Ilość serwerów wirtualnych: 4
   5. Ilość stacji komputerowych: 82
2. **Centrum Usług Wspólnych w Brześciu Kujawskim**
   1. Ilość pracowników: 13
   2. Ilość lokalizacji: 1
   3. Ilość serwerów fizycznych: 0
   4. Ilość serwerów wirtualnych: 0
   5. Ilość stacji komputerowych: 9
3. **Brzeski Ośrodek Pomocy Społecznej w Brześciu Kujawskim**
   1. Ilość pracowników: 32
   2. Ilość lokalizacji: 1
   3. Ilość serwerów fizycznych: 2
   4. Ilość serwerów wirtualnych: 0
   5. Ilość stacji komputerowych: 41
4. **Szkoła Podstawowa Nr 1 w Brześciu Kujawskim**
   1. Ilość pracowników: 94
   2. Ilość lokalizacji: 1
   3. Ilość serwerów fizycznych: 0
   4. Ilość serwerów wirtualnych: 0
   5. Ilość stacji komputerowych: 183
5. **Zespół Szkół Nr 2 w Brześciu Kujawskim**
   1. Ilość pracowników: 33
   2. Ilość lokalizacji: 1
   3. Ilość serwerów fizycznych: 0
   4. Ilość serwerów wirtualnych: 0
   5. Ilość stacji komputerowych: 42
6. **Szkoła Podstawowa w Brzeziu**
   1. Ilość pracowników: 32
   2. Ilość lokalizacji: 1
   3. Ilość serwerów fizycznych: 0
   4. Ilość serwerów wirtualnych: 0
   5. Ilość stacji komputerowych: 70
7. **Szkoła Podstawowa im. K. Makuszyńskiego w Wieńcu**
   1. Ilość pracowników: 53
   2. Ilość lokalizacji: 1
   3. Ilość serwerów fizycznych: 0
   4. Ilość serwerów wirtualnych: 0
   5. Ilość stacji komputerowych: 51
8. **Przedszkole Publiczne nr 1 w Brześciu Kujawskim „Kraina Bajek”**
   1. Ilość pracowników: 28
   2. Ilość lokalizacji: 1
   3. Ilość serwerów fizycznych: 0
   4. Ilość serwerów wirtualnych: 0
   5. Ilość stacji komputerowych: 10
9. **Żłobek Brzeskie Skrzaty w Brześciu Kujawskim**
   1. Ilość pracowników: 11
   2. Ilość lokalizacji: 1
   3. Ilość serwerów fizycznych: 0
   4. Ilość serwerów wirtualnych: 0
   5. Ilość stacji komputerowych: 4
10. **Żłobek Wieniecka Kraina Malucha**
    1. Ilość pracowników: 9
    2. Ilość lokalizacji: 1
    3. Ilość serwerów fizycznych: 0
    4. Ilość serwerów wirtualnych: 0
    5. Ilość stacji komputerowych: 3