

---

### Pytanie 1

---

Szanowni Państwo,

Zwracamy się z prośbą o udział w badaniu dotyczącym cyberbezpieczeństwa w jednostkach samorządu terytorialnego. Zespół badawczy tworzą: [REDACTED] z Katedry Finansów Publicznych Uniwersytetu Ekonomicznego w Poznaniu (UEP).

Badanie ma formę ankiety, której wypełnienie zajmie około 10 minut.

Dane z ankiet zostaną zakodowane i wykorzystane w celach naukowych, a wyniki służyć będą rozwojowi obszaru zapewnienia bezpieczeństwa informacji w sektorze samorządowym.

---

- przystępuję do badania
  - **rezygnuję z wypełnienia ankiety**
- 

### Pytanie 2

---

Województwo

---

- warmińsko-mazurskie
  - wielkopolskie
  - dolnośląskie
  - kujawsko-pomorskie
  - lubelskie
  - lubuskie
  - łódzkie
  - małopolskie
  - mazowieckie
  - opolskie
  - podkarpackie
  - podlaskie
  - pomorskie
  - śląskie
  - świętokrzyskie
  - zachodniopomorskie
- 

### Pytanie 3

---

Typ gminy

---

- 
- gmina miejska
  - gmina wiejska
  - gmina miejsko-wiejska
  - miasto na prawach powiatu
- 

Pytanie 4

---

Liczba mieszkańców (2019)

---

- do 10.000
  - 10.000-20.000
  - 20.000-30.000
  - 30.000-40.000
  - 40.000-50.000
  - 50.000-100.000
  - pow. 100.000
- 

Pytanie 5

---

Wielkość bieżących dochodów budżetowych na mieszkańca (2018)

---

- poniżej 3.000
  - 3.000-3.500
  - 3.500-4.000
  - 4.000-4.500
  - 4.500-5.000
  - powyżej 5.000
- 

Pytanie 6

---

Czy gmina została uznana za operatora usługi kluczowej?

---

- tak
  - nie
- 

Pytanie 7

---

Kto został wyznaczony do utrzymywania kontaktów z podmiotami krajowego systemu bezpieczeństwa?

---

- 
- wójt (burmistrz, prezydent) lub zastępca
  - sekretarz gminy
  - pracownik zatrudniony na stanowisku do spraw informatyki
  - inna osoba zatrudniona na stanowisku ... (proszę podać nazwę stanowiska)
- 

Pytanie 8

---

Czy w urzędzie wdrożono system zarządzania bezpieczeństwem informacji?

---

- Tak
  - Nie
- 

Pytanie 9

---

Czy wdrożony system zarządzania bezpieczeństwem informacji posiada akredytację zgodności z normą PN-ISO/IEC 27001:2014?

---

- Tak
  - Nie
- 

Pytanie 10

---

Dlaczego w gminie nie wdrożono systemu zarządzania bezpieczeństwem informacji?

---

- nie było takiego obowiązku
  - nie mamy specjalisty z zakresu informatyki
  - nie mamy elektronicznego obiegu dokumentów
  - nie widzimy potrzeby
  - nie mamy wystarczających środków finansowych
  - z innego powodu (jakiego?)
- 

Pytanie 11

---

Gmina wdroży system zarządzania bezpieczeństwem informacji, jeżeli:

---

- organy administracji rządowej przekażą na ten cel dodatkowe środki w formie dotacji
  - otrzymamy dofinansowanie ze środków unijnych
  - podpiszemy porozumienie z sąsiednimi gminami w sprawie wspólnego wdrożenia takiego systemu
  - wprowadzimy elektroniczny obieg dokumentów
  - w innych przypadkach (jakich?)
- 

Pytanie 12

---

Czy w Pani/Pana opinii cyberprzestępczość stanowi zagrożenie dla urzędu?

---

- nie wiem
- nie stanowi zagrożenia
- stanowi minimalne zagrożenie
- stanowi średnie zagrożenie
- stanowi duże zagrożenie
- stanowi bardzo duże zagrożenie

---

Pytanie 13

---

Czy w urzędzie przeprowadzana jest okresowa analiza ryzyka utraty integralności, poufności i dostępności informacji?

- 
- Tak
  - Nie

---

Pytanie 14

---

Dlaczego w urzędzie nie jest przeprowadzana analiza ryzyka utraty integralności, poufności i dostępności informacji?

- 
- nie było takiej potrzeby
  - brak środków finansowych
  - nieprzypisanie obowiązków z tego zakresu do żadnego stanowiska pracy
  - brak osób z odpowiednimi kompetencjami
  - inne powody (jakie?)

---

Pytanie 15

---

Czy w urzędzie prowadzona jest aktualna i kompletna elektroniczna ewidencja sprzętu informatycznego?

- 
- Tak
  - Nie

---

Pytanie 16

---

Czy w urzędzie przeprowadzany jest corocznie audyt wewnętrzny bezpieczeństwa informacji?

- 
- nie
  - tak, przez zatrudnionego audytora wewnętrznego
  - tak, przez usługodawcę zewnętrznego

---

Pytanie 17

---

Dlaczego w urzędzie nie przeprowadzono audytu wewnętrznego z zakresu bezpieczeństwa informacji?

---

- nie było takiej potrzeby
  - brak środków finansowych
  - inne powody (jakie?)
- 

#### Pytanie 18

---

Proszę wskazać elementy urzędu, w którym Pani/Pan pracuje szczególnie podatne na cyberprzestępczość?  
(możliwość zaznaczenia kilku odpowiedzi)

---

- infrastruktura krytyczna
  - infrastruktura w chmurze
  - dane osobowe
  - usługi on-line/aplikacje webowe/strony internetowe
  - systemy płatności
  - pracownicy
  - stacje robocze (sprzęt pracowników)
  - inne (jakie?)
- 

#### Pytanie 19

---

Czy w latach 2017-2019 wystąpiły w urzędzie incydenty związane z naruszeniem bezpieczeństwa informacji?

---

- nie
  - tak – do 5 incydentów
  - tak – do 10 incydentów
  - tak – do 20 incydentów
  - tak – powyżej 20 incydentów
- 

#### Pytanie 20

---

Czy zgłoszono wystąpienie incydentu związanego z naruszeniem bezpieczeństwa informacji?  
(możliwość zaznaczenia kilku odpowiedzi)

---

- nie
  - tak – na policję
  - tak – na cert.pl lub cert.gov.pl
  - tak – inne (gdzie?)
-

---

**Pytanie 21**

---

Proszę zaznaczyć przykłady działalności cyberprzestępczej, które wystąpiły w urzędzie.  
(możliwość zaznaczenia kilku odpowiedzi)

---

- phishing
  - spam
  - wyciek informacji
  - botnet
  - złośliwe oprogramowanie
  - wstrzyknięcie kodu
  - kradzież danych (ujawnienie poufnych informacji)
  - rogueware/ransomware/scareware
  - exploit drive-by-download na zainfekowanej stronie
  - inne (jakie?)
- 

**Pytanie 22**

---

Które z rozwiązań są stosowane w urzędzie? (możliwość zaznaczenia kilku odpowiedzi)

---

- firewall
  - antywirusy
  - skanery podatności
  - blokady i filtry spamu
  - szyfrowanie danych
  - systemy wczesnego ostrzegania
  - szyfrowanie VOIP
  - dedykowane zasoby VPN
  - SIEM (Security Information and Event Management)
  - systemy IDS/IPS (wykrywanie intruzów)
  - systemy DLP (ochrona przed wyciekiem danych)
  - inne (jakie?)
- 

**Pytanie 23**

---

W jaki sposób zarządza się cyberbezpieczeństwem w urzędzie?  
(możliwość zaznaczenia kilku odpowiedzi)

---

- 
- wewnątrznie (pracownik/pracownicy odpowiedzialni za politykę bezpieczeństwa)
  - przez dostawcę Internetu (IPS)
  - outsourcing – specjalista/firma zewnętrzna
  - inne (jakie?)
- 

Pytanie 24

---

Czy w latach 2017-2019 zorganizowano dla pracowników urzędu szkolenie z zakresu cyberbezpieczeństwa?

---

- nie
  - tak, dla kadry kierowniczej
  - tak, dla wszystkich pracowników
- 

Pytanie 25

---

Dlaczego szkolenia z zakresu cyberbezpieczeństwa nie odbyły się?

---

- nie było takiej potrzeby
  - brak środków finansowych
  - inne powody (jakie?)
- 

Pytanie 26

---

Czy gmina jest ubezpieczona od ryzyka cyberataku?

---

- tak, nasza polisa obejmuje to ryzyko
  - nie, ale planujemy rozszerzenie zakresu ubezpieczenia
  - nie, nie widzimy takiej potrzeby
- 

Pytanie 27

---

Dziękujemy za udział w badaniu

---