Samorządy w cyfrowym świecie: w poszukiwaniu sensu

Warszawa || 26-27 czerwca 2019

23.kmwi.pl

Dominika Lisiak-Felicka

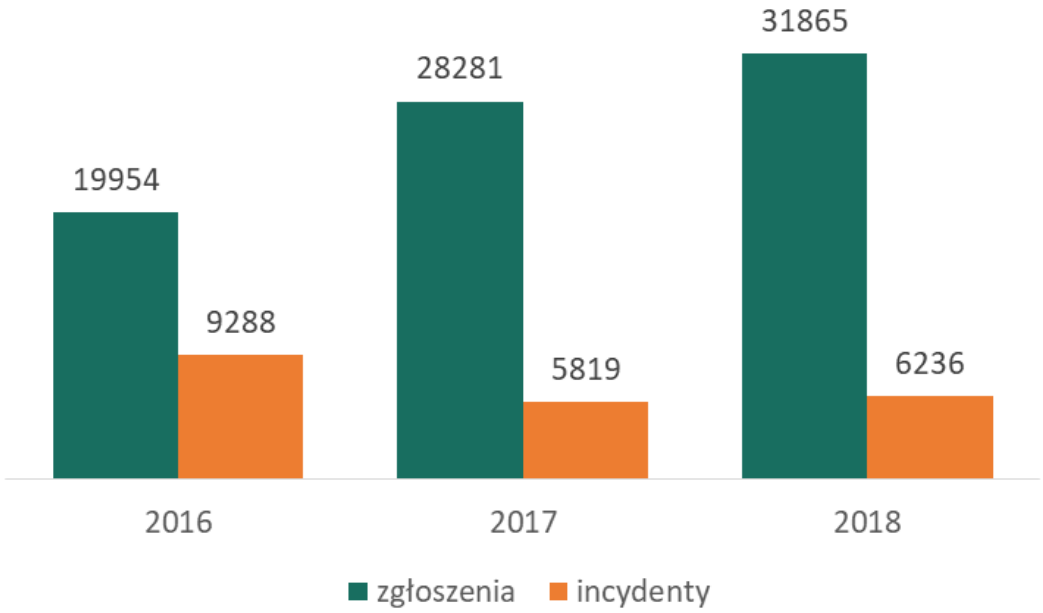
Cyberbezpieczeństwo urzędów administracji samorządowej - wyniki badań

Plan prezentacji

- Dane statystyczne o incydentach
- Przykłady incydentów
- Wyniki kontroli NIK
- Wyniki wcześniejszych badań własnych
- Badanie „Cyberbezpieczeństwo urzędów administracji samorządowej”
- Wnioski

Dane statystyczne

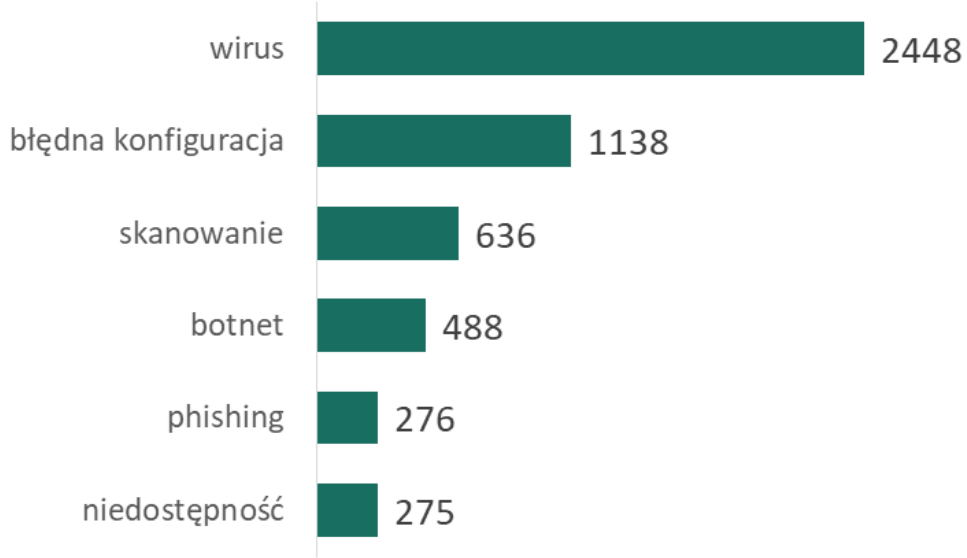
- Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2018 roku.



Źródło: csirt.gov.pl

Dane statystyczne

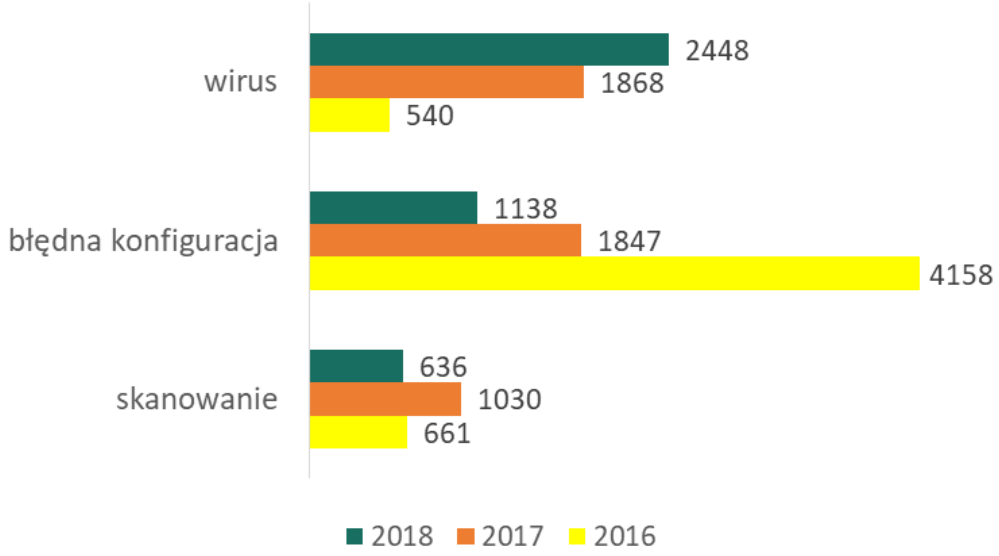
- Klasyfikacja najczęstszych incydentów zgłoszonych do CSIRT GOV w 2018 r.



Źródło: csirt.gov.pl

Dane statystyczne

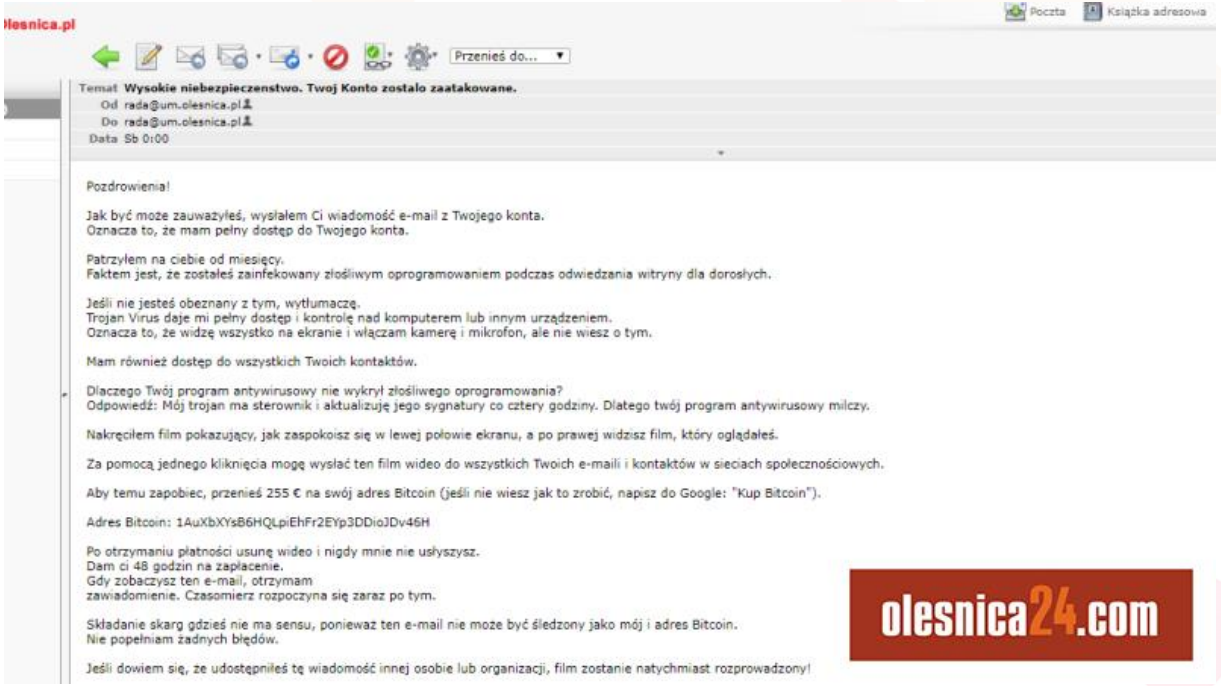
- Klasyfikacja najczęstszych incydentów zgłoszonych do CSIRT GOV w latach 2016- 2018.



Źródło: csirt.gov.pl

Przykłady incydentów

- 19.01.2019 r. - atak cyberprzestępców na służbowe skrzynki radnych Rady Miasta Oleśnicy.



lesnica.pl

Poczta Książka adresowa

Przenieś do...

Temat **Wysokie niebezpieczenstwo. Twoj Konto zostalo zaatakowane.**
Od rada@um.olesnica.pl
Do rada@um.olesnica.pl
Data Sb 0:00

Pozdrowienia!

Jak być może zauważyłeś, wysłałem Ci wiadomość e-mail z Twojego konta.
Oznacza to, że mam pełny dostęp do Twojego konta.

Patrzyłem na ciebie od miesięcy.
Faktem jest, że zostałeś zainfekowany złośliwym oprogramowaniem podczas odwiedzania witryny dla dorosłych.

Jeśli nie jesteś obeznany z tym, wytłumaczę.
Trojan Virus daje mi pełny dostęp i kontrolę nad komputerem lub innym urządzeniem.
Oznacza to, że widzę wszystko na ekranie i włączam kamerę i mikrofon, ale nie wiesz o tym.

Mam również dostęp do wszystkich Twoich kontaktów.

Dlaczego Twój program antywirusowy nie wykrył złośliwego oprogramowania?
Odpowiedź: Mój trojan ma sterownik i aktualizuję jego sygnatury co cztery godziny. Dlatego twój program antywirusowy milczy.

Nakręciłem film pokazujący, jak zaspokoisz się w lewej połowie ekranu, a po prawej widzisz film, który oglądałeś.

Za pomocą jednego kliknięcia mogę wysłać ten film wideo do wszystkich Twoich e-maili i kontaktów w sieciach społecznościowych.

Aby temu zapobiec, przenieś 255 € na swój adres Bitcoin (jeśli nie wiesz jak to zrobić, napisz do Google: "Kup Bitcoin").

Adres Bitcoin: 1AuXbXYsB6HQLpiEhFr2EYp3DDioJDv46H

Po otrzymaniu płatności usunę wideo i nigdy mnie nie usłyszysz.
Dam ci 48 godzin na zapłacenie.
Gdy zobaczysz ten e-mail, otrzymam
zawiadomienie. Czasomierz rozpoczyna się zaraz po tym.

Składanie skarg gdzieś nie ma sensu, ponieważ ten e-mail nie może być śledzony jako mój i adres Bitcoin.
Nie popełniam żadnych błędów.

Jeśli dowiem się, że udostępniłeś tę wiadomość innej osobie lub organizacji, film zostanie natychmiast rozprowadzony!

olesnica24.com

Źródło: https://www.olesnica24.com/wiadomosci/1206,nasz-news-atak-hakerow-na-skrzynki-radnych

Przykłady incydentów

- 25.02.2019 r. - w wyniku ataku utrudniona była bieżąca praca Wydziału Geodezji i Nieruchomości i obsługa osób w Urzędzie Miasta Tarnowa.

Źródło: http://www.kt24.pl/tarnow-hakerzy-zaatakowali-urzad-miasta/

Przykłady incydentów

- 02.05.2019 r. - zmasowany atak cyberprzestępców z Afryki Północnej na raciborskie Biuletyny Informacji Publicznej.

Źródło: https://raciborz.com.pl/2019/05/02/atak-hakerow-na-raciborskie-biuletyny-informacji-publicznej.html

Przykłady incydentów

- 10.05.2019 r. - przez trzy dni Urząd Gminy Rudnik nie miał dostępu do danych osobowych na serwerze, bo zostały zaszyfrowane przez cyberprzestępców, którzy żądali okupu w bitcoinach.

Źródło: https://www.supertydzien.pl/wiadomosci/6419,atak-hakerow-na-rudnik-super-tydzien

Przykłady incydentów

- 20-21.06.2019 r. - atak na wiele serwisów internetowych. Pojawił się na nich fałszywy komunikat o ewakuacji Polaków przez żandarmerię i wojska USA.


epoznan.pl WIADOMOŚCI SPORT KULTURA I ROZRYWKA KORKI TURYSTYKA OGŁOSZENIA KATALOG

Udostępnij

Lubię to! 3

ZGŁOŚ BŁĄD

WYŚLIJ ZDJĘCIE

PILNE

Zgodnie z planem ćwiczeń pk. "Dragon '19" na terenie Rzeczypospolitej Polskiej odbędzie się epizod praktyczny tych manewrów międzynarodowych.

Związany on będzie z ewakuacją ludności z obszarów zagrożonych działaniami militarnymi na terenie województwa.
W związku z tym KAŻDY obywatel jest ZOBOWIĄZANY do przybycia pod siedzibę Urzędu **21 czerwca przed godz.16**. Należy mieć przy sobie tylko niezbędne rzeczy i dokumenty. Ewakuacja zostanie przeprowadzona siłami Żandarmerii Wojskowej.
Cały epizod praktyczny manewrów potrwa 5 dni, w ciągu których każda ewakuowana osoba będzie miała zapewnione 4 posiłki dziennie, wodę pitną, indywidualne miejsce odpoczynku w 20-to osobowym namiocie, niezbędną pomoc medyczną i inne wygody dla pobytu w łagru na wyznaczony termin.
Według przepisów Rozporządzenia Rady Ministrów w sprawie wprowadzenia obowiązkowych ćwiczeń wojskowych (z dnia 24 marca 2015 r.) w mieszkaniach obywateli mogą być rozlokowani żołnierzy USA na termin przeprowadzenia ww. epizodu praktycznego.
Zgodnie z ww. aktem prawnym odmowa wykonania polecenia Ministerstwa Obrony Narodowej może być podstawą dla wysiedlenia przy użyciu sił Military Police wojsk USA.
Urząd przeprasza za czasowe niewygody i zapewnia, iż nie istnieje zagrożenia dla bezpieczeństwa społeczeństwa.

Źródło: https://niebezpiecznik.pl/post/niezalezna-pl-i-inne-serwisy-w-polsce-zhackowane-rozsiewaly-plotki-o-ewakuacji-polakow-przez-zandarmerie-i-wojska-usa/

Wyniki kontroli NIK

- Informacja o wynikach kontroli: „Zarządzanie bezpieczeństwem informacji w jednostkach samorządu terytorialnego”,
- Od 4 czerwca 2018 r. do 12 października 2018 r.,
- 23 jednostki z obszaru pięciu województw (mazowieckiego, podlaskiego, łódzkiego, małopolskiego i dolnośląskiego), w tym:
  - dziewięć starostw powiatowych;
  - 14 urzędów miast/miast i gmin/gmin.

Źródło: https://www.nik.gov.pl/plik/id,20027,v,artykul_19054.pdf

Wyniki kontroli NIK

- Ocena ogólna - rodzaje ocen kontrolowanej działalności wykonywanej w badanych j.s.t. [%]

Źródło: https://www.nik.gov.pl/plik/id,20028,v,artykul_19054.pdf

Wyniki kontroli NIK

„NIK negatywnie oceniła wykonywanie przez blisko 70% skontrolowanych urzędów jednostek samorządu terytorialnego zadań związanych z zapewnieniem bezpieczeństwa przetwarzania informacji w okresie objętym kontrolą. W 61% kontrolowanych urzędów brak było systemowego podejścia do zapewnienia bezpieczeństwa informacji.

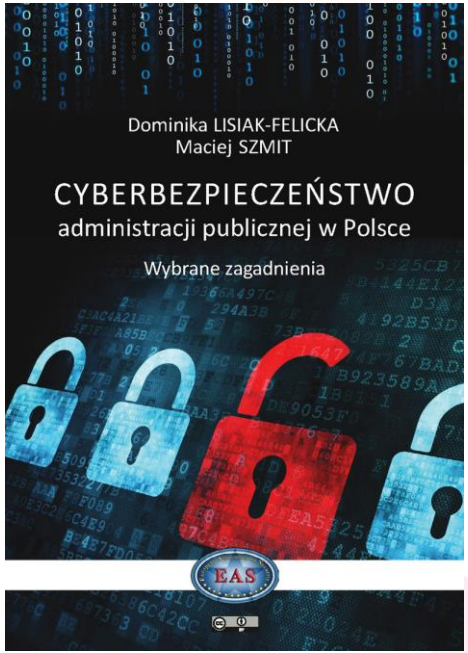
W wielu kontrolowanych urzędach j.s.t. nie dostrzegano występujących zagrożeń. W 48% jednostek nie dokonywano analiz ryzyka, a w 70% nie przeprowadzono obowiązkowego corocznego audytu z zakresu bezpieczeństwa informacji. Brak cyklicznych analiz ryzyka i nieprowadzenie audytów bezpieczeństwa nie pozwalał na identyfikację istotnych ryzyk w zakresie bezpieczeństwa informacji. **Kontrola wykazała, że w wielu urzędach j.s.t. zasady mające na celu zwiększenie bezpieczeństwa przetwarzania danych nie były przestrzegane,** w szczególności w ponad 80% kontrolowanych urzędów wystąpiły nieprawidłowości w zarządzaniu uprawnieniami użytkowników w systemach informatycznych.

Wyniki kontroli wskazują, że o ile w urzędach j.s.t. w większości podjęto działania w celu dostosowania do RODO, to w dalszym ciągu często nie są przestrzegane wymogi dotyczące bezpieczeństwa informacji wynikające z obowiązującego od 2012 r. rozporządzenia KRI.”

Źródło: https://www.nik.gov.pl/plik/id,20028,v,artykul_19054.pdf

Wyniki wcześniejszych badań własnych

- stan wdrożenia systemów zarządzania bezpieczeństwem informacji;
- zarządzanie incydentami związanymi z bezpieczeństwem informacji;
- czynniki sukcesu wdrożenia systemu zarządzania bezpieczeństwem informacji;
- przeglądy systemów zarządzania bezpieczeństwem informacji;
- dokumentacja bezpieczeństwa informacji;



Źródło:
https://www.researchgate.net/publication/301204372_Cyberbezpieczenstwo_administracji_publicznej_w_Polsce_Wybrane_zagadnienia

Wyniki wcześniejszych badań własnych

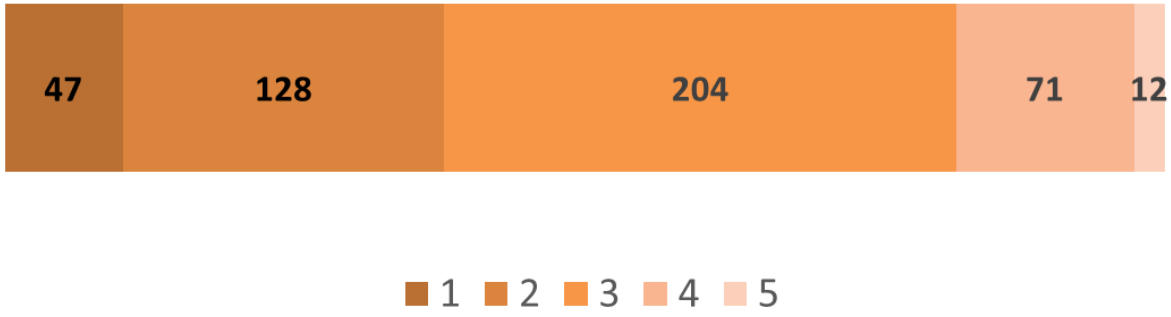
- Najważniejsze wyniki:
  - Brak systemowego podejścia do zagadnień bezpieczeństwa informacji (spośród 293 urzędów, 151 posiadało wdrożony System Zarządzania Bezpieczeństwem Informacji, w 21 przypadkach system ten był certyfikowany),
  - Problemy z zarządzaniem incydentami związanymi z bezpieczeństwem informacji (tylko 47 urzędów rejestrowało incydenty),
  - Niejednorodne formy dokumentacji.

Wyniki wcześniejszych badań własnych

- Cel badania: **określenie stopnia przygotowania urzędów administracji samorządowej w Polsce do wdrożenia zmian wynikających z RODO**,
- 462 wypełnionych kwestionariuszy ankiety,
- Najważniejsze wyniki:
  - Tylko 96 (21%) urzędów formalnie zdefiniowało strategię wdrożenia RODO (cele, terminy, osoby odpowiedzialne, procedury);
  - Jedynie 32 urzędy zdefiniowały mierniki gotowości/dojrzałości wdrożenia RODO;

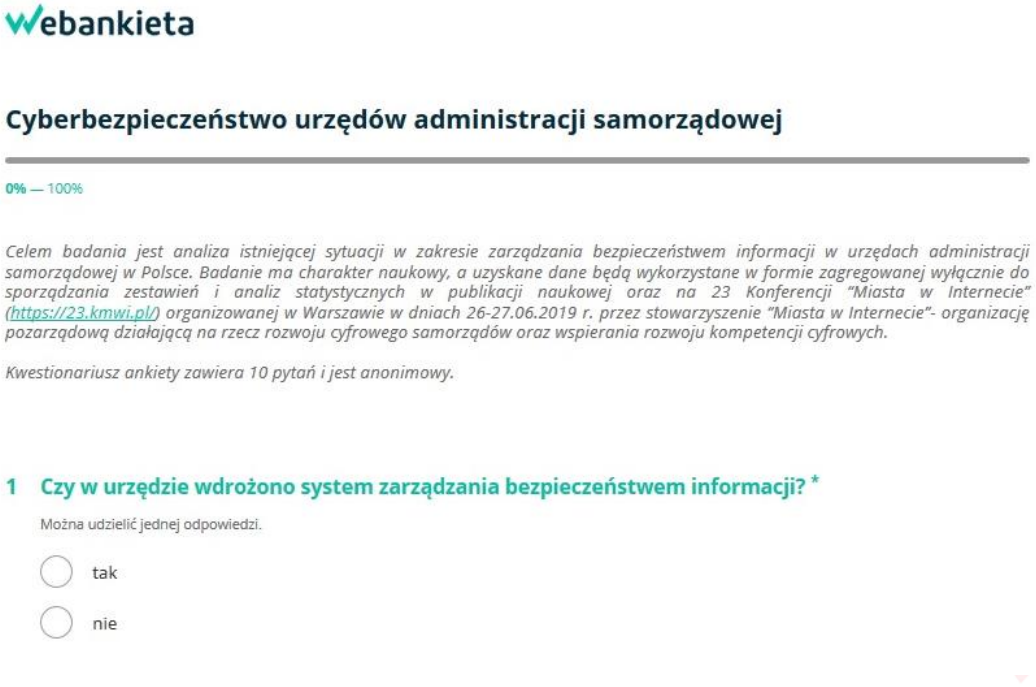
Wyniki wcześniejszych badań własnych

- Ewaluacja procesu wdrożenia RODO prowadzona w 139 urzędach;
- Ocena stopnia przygotowania urzędu do wprowadzenia zmian wynikających z RODO według opinii urzędników (gdzie 1 – brak wdrożenia, a 5 – wdrożenie wszystkich wymagań RODO).



Wyniki badania „Cyberbezpieczeństwo urzędów administracji samorządowej”

- Cel badania: analiza istniejącej sytuacji w zakresie zarządzania bezpieczeństwem informacji w urzędach administracji samorządowej w Polsce.



Webankieta

Cyberbezpieczeństwo urzędów administracji samorządowej

0% — 100%

Celem badania jest analiza istniejącej sytuacji w zakresie zarządzania bezpieczeństwem informacji w urzędach administracji samorządowej w Polsce. Badanie ma charakter naukowy, a uzyskane dane będą wykorzystane w formie zagregowanej wyłącznie do sporządzania zestawień i analiz statystycznych w publikacji naukowej oraz na 23 Konferencji "Miasta w Internecie" (https://23.kmwi.pl/) organizowanej w Warszawie w dniach 26-27.06.2019 r. przez stowarzyszenie "Miasta w Internecie"- organizację pozarządową działającą na rzecz rozwoju cyfrowego samorządów oraz wspierania rozwoju kompetencji cyfrowych.

Kwestionariusz ankiety zawiera 10 pytań i jest anonimowy.

1 Czy w urzędzie wdrożono system zarządzania bezpieczeństwem informacji? *

Można udzielić jednej odpowiedzi.

- tak
- nie

Wyniki badania „Cyberbezpieczeństwo urzędów administracji samorządowej”

- 543 odpowiedzi

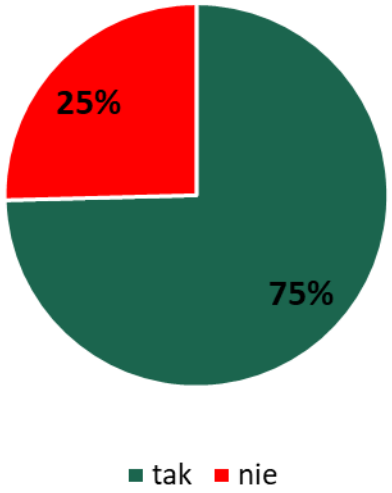
Typ urzędu	*%*	*Liczba odp.*
urząd marszałkowski	2%	10
starostwo powiatowe	12%	64
urząd gminy/miasta	86%	469
	Razem:	**543**

Województwo	Liczba odp.
mazowieckie	57
warmińsko-mazurskie	47
wielkopolskie	46
małopolskie	45
śląskie	44
lubelskie	40
dolnośląskie	37
kujawsko-pomorskie	37
łódzkie	32
podkarpackie	32
pomorskie	28
podlaskie	27
świętokrzyskie	19
zachodniopomorskie	16
opolskie	14
lubuskie	12
Suma	**533**

Wizualizacja nie zawiera danych o urzędach marszałkowskich ze względu na możliwość identyfikacji urzędów.

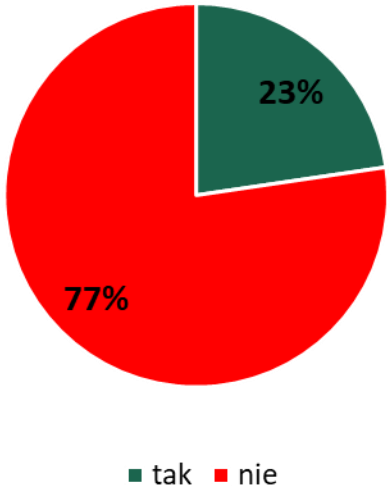
Wyniki badania „Cyberbezpieczeństwo urzędów administracji samorządowej”

- Czy w urzędzie wdrożono system zarządzania bezpieczeństwem informacji?



Wyniki badania „Cyberbezpieczeństwo urzędów administracji samorządowej”

- Czy system ten jest certyfikowany na zgodność z wymaganiami normy ISO/IEC 27001?

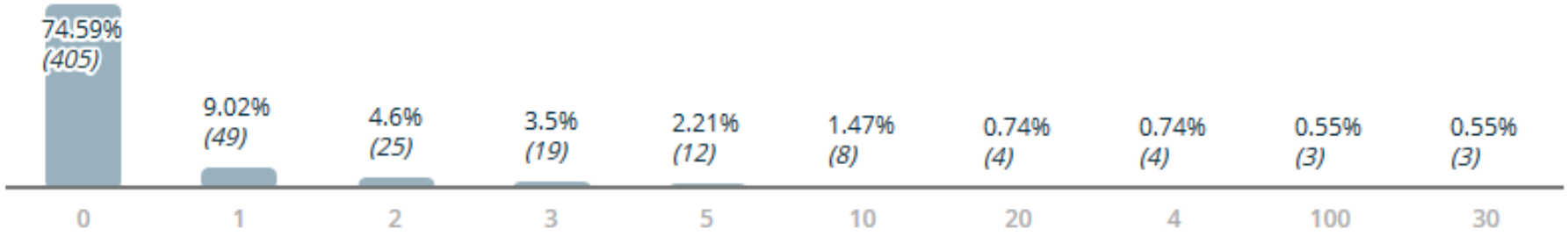


Wyniki badania „Cyberbezpieczeństwo urzędów administracji samorządowej”

- Które z poniższych elementów w urzędzie uważa Pani/Pan za najbardziej podatne na ataki cyberprzestępców?

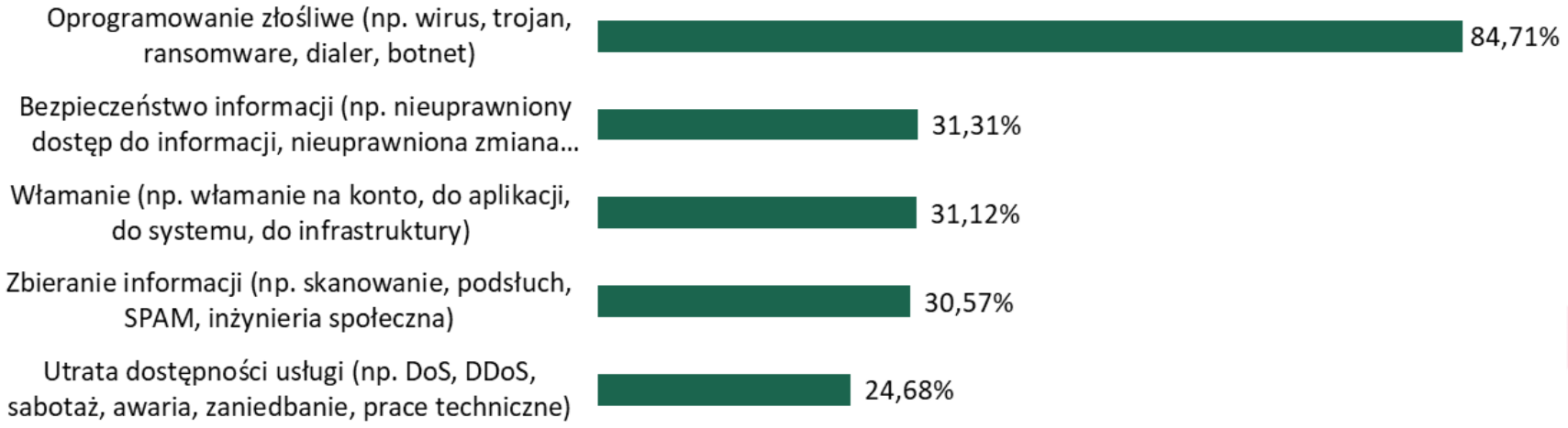
Wyniki badania „Cyberbezpieczeństwo urzędów administracji samorządowej”

- Ile incydentów związanych z bezpieczeństwem informacji zostało zarejestrowanych w urzędzie w ciągu ostatnich 12 miesięcy.



Wyniki badania „Cyberbezpieczeństwo urzędów administracji samorządowej”

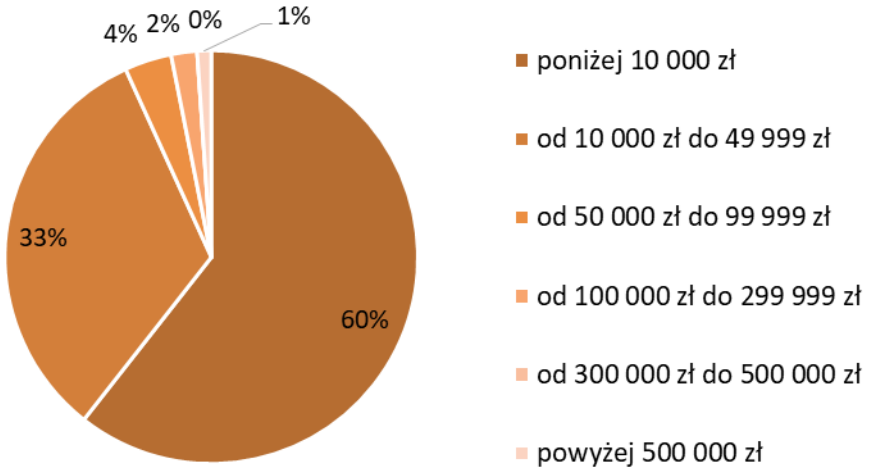
- Które z kategorii incydentów według Pani/Pana opinii stanowią największe zagrożenie dla urzędu? (kategorie zgodne z CSIRT GOV)



Wyniki badania „Cyberbezpieczeństwo urzędów administracji samorządowej”

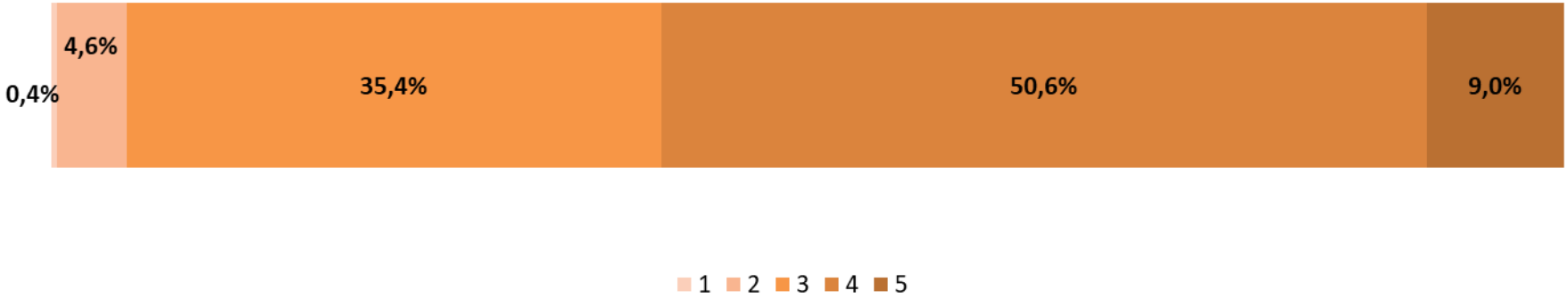
- Jaki jest orientacyjny roczny budżet urzędu przeznaczany na bezpieczeństwo informacji?

Odpowiedź	*%*	*Liczba odp.*
poniżej 10 000 zł	60,59%	329
od 10 000 zł do 49 999 zł	32,60%	177
od 50 000 zł do 99 999 zł	3,68%	20
od 100 000 zł do 299 999 zł	2,03%	11
od 300 000 zł do 500 000 zł	0,00%	0
powyżej 500 000 zł	1,10%	6



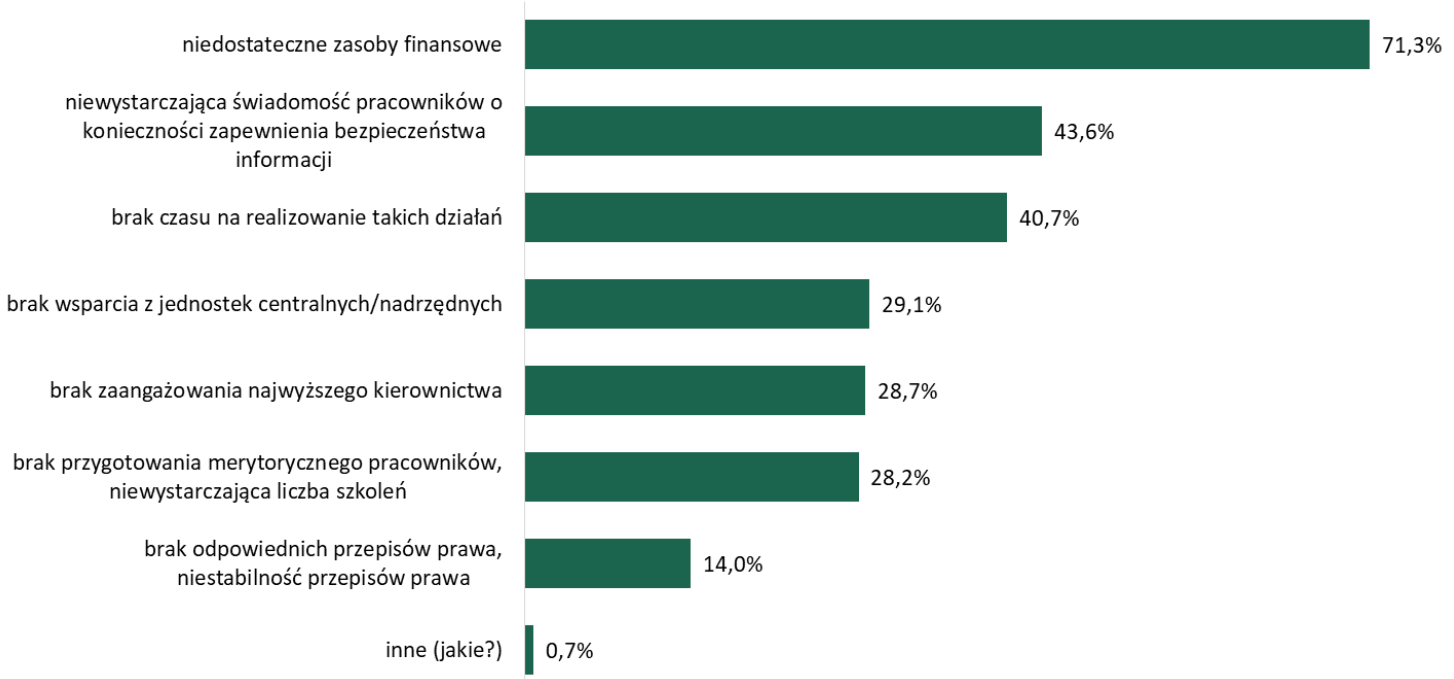
Wyniki badania „Cyberbezpieczeństwo urzędów administracji samorządowej”

- W skali od 1 do 5 jak ocenia Pan/Pani poziom bezpieczeństwa informacji w urzędzie?



Wyniki badania „Cyberbezpieczeństwo urzędów administracji samorządowej”

- Co według Pani/Pana opinii jest największym problemem w zapewnieniu odpowiedniego poziomu bezpieczeństwa informacji w urzędzie?



Wnioski

- Wzrasta liczba urzędów posiadających wdrożony system zarządzania bezpieczeństwem informacji;
- Tylko w 23% przypadków system ten jest certyfikowany;
- Identyfikacja elementów, które są najbardziej podatne na ataki cyberprzestępców;
- Największe zagrożenie dla urzędów stanowi oprogramowanie złośliwe;

Wnioski

- Kwestia zarządzania incydentami związanymi z bezpieczeństwem informacji - brak incydentów?
- Bardzo niskie finansowanie bezpieczeństwa informacji;
- Niedostateczne zasoby finansowe najczęściej wskazanym problemem w zapewnieniu bezpieczeństwa informacji;
- Optymizm urzędników w ocenie poziomu bezpieczeństwa.

Dziękuję za uwagę.

Dominika Lisiak-Felicka
dominika.lisiak@gmail.com