JOURNAL OF MODERN SCIENCE

1/65/2026

www.jomswsge.com

DOI: 10.13166/jms/218199

Mariusz Czternastek
University of the National Education Commission, Krakow, Poland
ORCID iD: 0000-0002-0396-9904

Zbigniew Ciekanowski
War Studies University, Poland
ORCID iD: 0000-0002-0549-894X

Sławomir Żurawski
Andrzej Frycz Modrzewski University in Krakow, Poland
ORCID iD: 0000-0001-9527-3391

Henryk Wyrębek
University of Siedlce, Poland
ORCID iD: 0000-0001-9801-6905

ZARZĄDZANIE INCYDENTAMI CYBERBEZPIECZEŃSTWA W JEDNOSTKACH SAMORZĄDU TERYTORIALNEGO

CYBERSECURITY INCIDENT MANAGEMENT IN LOCAL GOVERNMENT UNITS

Abstract

The aim of this article is to identify key organizational and procedural barriers to cybersecurity incident management in local government units and to synthetically systematize findings derived from available empirical analyses. The study is based on a qualitative secondary analysis of the 2025 report of the Supreme Audit Office, data published by CERT Poland, and selected case studies of ransomware incidents affecting Polish local governments. An exploratory and comparative approach was applied to identify recurring organizational response patterns and systemic weaknesses. The findings indicate a widespread lack of business continuity plans, insufficient backup protection, unclear responsibility allocation, and a low level of information security culture within local governments. The article concludes with practical recommendations focused on implementing a cybersecurity incident management lifecycle and strengthening the digital resilience of local government units.

Keywords: *incident management, information security, local government units, cyber threats*

Streszczenie

Celem artykułu jest identyfikacja kluczowych barier organizacyjnych i proceduralnych w zarządzaniu incydentami cyberbezpieczeństwa w jednostkach samorządu terytorialnego oraz syntetyczne ujęcie wniosków płynących z dostępnych analiz empirycznych. Badanie oparto na jakościowej analizie wtórnej raportu Najwyższej Izby Kontroli z 2025 r., danych CERT Polska oraz wybranych studiów przypadków incydentów ransomware w polskich JST. Wyniki wskazują na powszechny brak planów ciągłości działania, niedostateczne zabezpieczenie kopii zapasowych, niejednoznaczny podział odpowiedzialności oraz niski poziom kultury bezpieczeństwa informacji w JST. Artykuł formułuje wnioski praktyczne w postaci rekomendacji dotyczących wdrażania cyklu zarządzania incydentem bezpieczeństwa oraz wzmacniania odporności cyfrowej samorządu.

Słowa kluczowe: *zarządzanie incydentami, bezpieczeństwo informacji, jednostki samorządu terytorialnego, cyberzagrożenia*

Wprowadzenie

Współczesne jednostki samorządu terytorialnego (JST) stanowią istotny filar systemu administracji publicznej, odpowiedzialny za realizację zadań publicznych najbliżej obywateli. Zakres ich kompetencji obejmuje szerokie spektrum działań – od zapewnienia porządku publicznego i bezpieczeństwa mieszkańców po organizację usług komunalnych, edukacyjnych i społecznych. W kontekście dynamicznych zmian cywilizacyjnych oraz wzrastającego poziomu zagrożeń – zarówno naturalnych, technologicznych, jak i wywołanych działalnością człowieka – JST muszą nieustannie adaptować się do nowych realiów zarządzania ryzykiem i sytuacjami kryzysowymi. Skuteczność tych działań w dużej mierze zależy od zdolności jednostek samorządowych do reagowania na incydenty bezpieczeństwa, które mogą zakłócić ciągłość funkcjonowania urzędów, naruszyć infrastrukturę krytyczną, a także wpłynąć na życie i zdrowie obywateli.

W dobie cyfryzacji oraz postępującej integracji systemów informacyjnych coraz większą rolę w krajobrazie zagrożeń odgrywają incydenty o charakterze teleinformatycznym – ataki hakerskie, wycieki danych, awarie systemów zarządzania kryzysowego czy zakłócenia w funkcjonowaniu e-usług (Hoffman, Cseh, 2020). Jednocześnie JST muszą mierzyć się z tradycyjnymi rodzajami incydentów, takimi jak pożary, powodzie, skażenia chemiczne, akty wandalizmu czy lokalne konflikty społeczne. Skuteczne zarządzanie tego rodzaju zdarzeniami wymaga nie tylko sprawnych struktur organizacyjnych i technicznego przygotowania, lecz także zbudowania kultury bezpieczeństwa wśród pracowników administracji oraz mieszkańców.

Niezbędne staje się opracowanie procedur i mechanizmów, które umożliwiają szybkie rozpoznanie incydentu, ocenę jego charakteru i skali, a także skuteczną reakcję i usunięcie skutków. Odpowiedzialność za te działania spoczywa w dużej mierze na władzach lokalnych, które odgrywają kluczową rolę w systemie zarządzania kryzysowego, będąc pierwszym ogniwem reagującym na sytuacje nadzwyczajne. W tym kontekście zarządzanie incydentami nie może być traktowane jedynie jako techniczne działanie reagujące na zdarzenia po ich wystąpieniu, lecz jako strategiczny, wieloetapowy proces zapobiegania, planowania, reagowania i odbudowy. Obejmuje on współdziałanie różnych

struktur administracyjnych, służb ratowniczych, jednostek organizacyjnych samorządu oraz partnerów zewnętrznych, w tym sektora prywatnego i organizacji pozarządowych.

Metody badawcze

Badanie ma charakter jakościowej analizy zastanych danych. Materiał badawczy obejmował raport Najwyższej Izby Kontroli z 2025 r., roczne raporty CERT Polska (Computer Emergency Response Team Polska) oraz opisy wybranych incydentów ransomware w jednostkach samorządu terytorialnego. Dobór studiów przypadków miał charakter celowy i obejmował incydenty, które skutkowały zakłóceniem ciągłości działania urzędów. Analiza polegała na wyodrębnieniu wspólnych kategorii problemowych (m.in. ciągłość działania, zabezpieczenie kopii zapasowych, struktura odpowiedzialności, komunikacja kryzysowa), a następnie ich porównaniu w celu identyfikacji powtarzalnych schematów organizacyjnych i systemowych.

W artykule zastosowano odpowiednie metody badawcze – analizę literatury przedmiotu oraz studium przypadku, które wspólnie umożliwiły zbudowanie pogłębionej i wieloaspektowej diagnozy stanu zarządzania incydentami bezpieczeństwa w jednostkach samorządu terytorialnego.

Analiza literatury obejmowała przegląd publikacji naukowych z zakresu bezpieczeństwa informacji, zarządzania kryzysowego, administracji publicznej i cyberbezpieczeństwa, a także dokumentów normatywnych (takich jak ustawa o Krajowym Systemie Cyberbezpieczeństwa, RODO (ogólne rozporządzenie o ochronie danych), rozporządzenie KRI (Standardy Krajowych Ram Interoperacyjności) oraz raportów instytucji publicznych – w szczególności kompleksowego raportu Najwyższej Izby Kontroli z 2025 r. dotyczącego stanu zabezpieczenia systemów informatycznych w JST. Analiza ta pozwoliła uchwycić standardy organizacyjne, obowiązujące przepisy oraz istniejące rekomendacje w zakresie reagowania na incydenty, a także zidentyfikować luki i niespójności w obowiązujących rozwiązaniach.

Uzupełnieniem tej analizy było zastosowanie metody studium przypadku (*case study*), w ramach którego przeanalizowano wybrane incydenty bezpieczeństwa, które wystąpiły w różnych jednostkach samorządu w Polsce.

Przykłady ataków ransomware w Kościerzynie, Otwocku, Tucznej, Krakowie i Oświęcimiu pozwoliły prześledzić realny przebieg zdarzeń, zakres ich skutków, działania naprawcze oraz skalę organizacyjnych trudności, z jakimi borykały się zaatakowane urzędy. Studium przypadku ujawniło powtarzające się wzorce błędów, takie jak brak planów ciągłości działania, niedostateczna ochrona kopii zapasowych, niewyznaczenie koordynatora kryzysowego czy brak procedur komunikacji z mieszkańcami i partnerami zewnętrznymi.

Zestawienie wyników obu metod pozwoliło nie tylko skonfrontować modelowe założenia z praktyką funkcjonowania JST, ale również sformułować rekomendacje odnoszące się do wdrażania strategii odporności cyfrowej, budowy struktur reagowania kryzysowego oraz konieczności rozwoju kompetencji kadrowych w administracji lokalnej. Dzięki temu artykuł łączy walor analityczny z praktycznym i może stanowić punkt wyjścia dla dalszych badań oraz działań usprawniających system zarządzania incydentami w samorządach.

Rola jednostek samorządu terytorialnego w systemie bezpieczeństwa lokalnego

Incydent bezpieczeństwa rozumiany jest jako zdarzenie naruszające poufność, integralność lub dostępność zasobów informacyjnych bądź organizacyjnych, które nie osiąga jeszcze progu sytuacji kryzysowej, lecz wymaga skoordynowanej reakcji organizacyjnej. Zarządzanie incydentami należy traktować jako proces cyklicznyobejmujący etapy: identyfikacji, klasyfikacji, reakcji, odtworzenia oraz wyciągania wniosków (ang. *incident management lifecycle*). Podejście to jest zgodne z międzynarodowymi standardami, takimi jak ISO/IEC 27035, ISO 22301 oraz wytycznymi NIST (National Institute of Standards and Technology) i ENISA (European Union Agency for Cybersecurity).

W kontekście JST zarządzanie incydentami stanowi istotny element budowania odporności cyfrowej samorządu oraz kształtowania kultury bezpieczeństwa informacji.

Współczesne jednostki samorządu terytorialnego odgrywają kluczową rolę w kształtowaniu bezpieczeństwa publicznego na poziomie lokalnym, będąc jednocześnie podstawowym ogniwem administracji publicznej w Polsce. Ich usytuowanie w strukturze państwa sprawia, że są najbliżej obywatela – zarówno

w sensie geograficznym, jak i organizacyjnym – co przekłada się na bezpośrednią odpowiedzialność za realizację zadań związanych z ochroną życia, zdrowia, mienia oraz środowiska. Bezpieczeństwo lokalne, rozumiane jako stan wolny od zagrożeń zakłócających codzienne funkcjonowanie społeczności lokalnej, staje się jednym z fundamentalnych obszarów aktywności samorządu. Stan ten w odniesieniu do społeczności lokalnych determinowany jest cechami charakterystycznymi dla tejże społeczności. Należą do nich:

- większa autonomia;
- własne normy społeczne regulujące działania danej społeczności;
- silne więzi kulturowe i międzyludzkie;
- zamieszkiwanie wyodrębnionego, stosunkowo niewielkiego terytorium;
- poczucie zakorzenienia i przynależności do zamieszkiwanego miejsca (Rozwadowski, 2014, s. 248).

Bezpieczeństwo społeczności lokalnych to zarówno niwelowanie zagrożeń, jak i szacowanie ryzyka ich wystąpienia (Mickiewicz, 2020, s. 5). W tym kontekście JST nie tylko wykonują zadania zlecone przez administrację rządową, ale również projektują i realizują własne strategie bezpieczeństwa, uwzględniając lokalną specyfikę, strukturę społeczną, geograficzne uwarunkowania i potencjalne zagrożenia. Zakres kompetencji JST w obszarze bezpieczeństwa obejmuje m.in.:

- utrzymanie porządku publicznego;
- przeciwdziałanie sytuacjom kryzysowym;
- wspieranie działań służb ratowniczych;
- organizację systemu ostrzegania ludności;
- zabezpieczenie imprez masowych;
- przeciwdziałanie skutkom klęsk żywiołowych i katastrof technicznych.

Gminy i powiaty są odpowiedzialne za prowadzenie analiz ryzyka, tworzenie planów zarządzania kryzysowego, szkolenie personelu oraz zapewnienie zasobów i infrastruktury niezbędnych do efektywnego reagowania. Co więcej, JST pełnią funkcję koordynatorów działań podejmowanych przez różne instytucje – od policji, przez Państwową Straż Pożarną, po lokalne podmioty gospodarcze i organizacje pozarządowe (Klonowska, Hytrek, 2008, s. 20).

Ten wielowymiarowy charakter działań sprawia, że skuteczność zarządzania bezpieczeństwem w dużej mierze zależy od sprawności organizacyjnej, kompetencji kadry urzędniczej oraz umiejętności współpracy międzysektorowej.

Dynamiczne zmiany społeczne, urbanizacyjne i technologiczne, a także nowe typy zagrożeń, w tym cyberataki, zagrożenia hybrydowe, migracje przymusowe czy ekstremalne zjawiska pogodowe, znacząco poszerzają zakres odpowiedzialności samorządów. W związku z tym powstaje pytanie o zakres obowiązków, odpowiedzialności, a także kompetencji (Jańczuk, 2015, s. 325).

W warunkach ciągłego ryzyka i niepewności JST muszą wykazywać się odpornością organizacyjną, zdolnością szybkiego reagowania oraz elastycznością proceduralną. To z kolei wymaga ciągłego doskonalenia systemów zarządzania bezpieczeństwem – nie tylko w wymiarze formalnym, ale również poprzez rozwijanie partnerstw lokalnych, wzmacnianie partycypacji społecznej i budowanie zaufania obywateli do instytucji publicznych.

Warto również zaznaczyć, że JST pełnią nie tylko funkcję wykonawczą, lecz także edukacyjną i prewencyjną. Poprzez działania informacyjne, kampanie społeczne, ćwiczenia ewakuacyjne czy wspieranie lokalnych programów bezpieczeństwa publicznego samorządy przyczyniają się do kształtowania świadomości zagrożeń oraz promowania odpowiedzialnych postaw obywatelskich. Ich rola w zakresie integracji społeczności lokalnej wokół idei wspólnego bezpieczeństwa jest nie do przecenienia.

W konsekwencji rola jednostek samorządu terytorialnego w systemie bezpieczeństwa lokalnego nie ogranicza się do realizacji procedur administracyjnych, lecz staje się dynamicznym, wielowymiarowym procesem zarządzania ryzykiem i budowania odporności lokalnych społeczności na różnego rodzaju zagrożenia.

Charakterystyka współczesnych zagrożeń i incydentów bezpieczeństwa

Szybki rozwój nowoczesnych technologii sprawił, że internet stał się dostępny prawie dla każdego (Nowicka i in., 2023, s. 425). Jednostki samorządu terytorialnego (JST), pełniąc funkcję organizatora życia społecznego i gospodarczego na poziomie lokalnym, stają przed koniecznością mierzenia się z coraz bardziej zróżnicowanym i nieprzewidywalnym katalogiem zagrożeń

(Gerwatowski, 2019, s. 89–90). Ewolucja współczesnych zagrożeń – zarówno pod względem ich charakteru, jak i skali oddziaływania – wpływa bezpośrednio na sposób organizacji i funkcjonowania struktur odpowiedzialnych za bezpieczeństwo publiczne. Transformacja technologiczna, urbanizacja, zmiany klimatyczne, zjawiska społeczne o wysokiej dynamice (jak migracje czy radykalizacja postaw), a także rosnąca liczba incydentów o charakterze cybernetycznym wymagają od JST przedefiniowania tradycyjnych modeli zarządzania bezpieczeństwem.

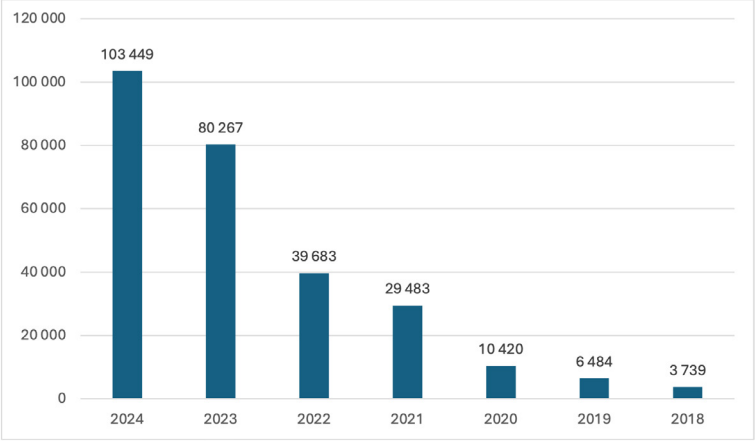
Z roku na rok z powodu wielu czynników stopień wykorzystywania przez JST usług e-administracji rośnie (Włodyka, 2022, s. 206). W pierwszej kolejności należy zwrócić uwagę na rosnącą skalę i złożoność zagrożeń teleinformatycznych (Żurawski, Ciekanowski, 2023, s. 10). Samorządy lokalne, będące operatorem szerokiego spektrum usług elektronicznych – od rejestrów mieszkańców, przez systemy podatkowe, po zdalne kanały obsługi interesantów – stają się coraz częstszym celem ataków hakerskich, kampanii phishingowych, ataków typu DDoS oraz incydentów związanych z nieuprawnionym dostępem do danych osobowych. W wielu przypadkach cyberincydenty nie tylko paraliżują bieżące funkcjonowanie urzędów, ale mogą prowadzić do naruszenia przepisów RODO, utraty zaufania społecznego oraz strat finansowych wynikających z przestojów i konieczności odbudowy systemów (Ciekanowski i in., 2023, s. 783). Na wykresie 1 przedstawiono liczbę obsłużonych przez CERT Polska incydentów w latach 2018–2024.

Najwięcej incydentów odnotowano w administracji publicznej – 1911 przypadków (Raport roczny 2024 z działalności CERT Polska). Pomimo dynamicznego rozwoju usług cyfrowych w administracji publicznej, wiele JST nie dysponuje wystarczającymi zasobami technologicznymi ani kadrowymi do wdrażania zaawansowanych systemów bezpieczeństwa informacyjnego. Brakuje także spójnych procedur reagowania na incydenty oraz standardów wymiany informacji z innymi podmiotami – zarówno pionowo (z administracją rządową), jak i horyzontalnie (z innymi JST czy partnerami prywatnymi).

JST, odpowiadając za infrastrukturę drogową, energetyczną, wodociągową i kanalizacyjną, muszą nie tylko szybko reagować na skutki tych incydentów, ale też prowadzić działania prewencyjne, inwestycyjne oraz edukacyjne, ograniczające prawdopodobieństwo ich wystąpienia i zasięg. Nie można pominąć także

incydentów o charakterze społecznym i kryminalnym (Kwiecińska i in., 2023). Na poziomie lokalnym JST coraz częściej są zaangażowane w zarządzanie sytuacjami konfliktowymi związanymi z dużymi skupiskami ludzi – protestami, demonstracjami, konfliktami wokół inwestycji infrastrukturalnych czy kontrowersji światopoglądowych.

Wykres 1. *Zestawienie liczby obsłużonych przez CERT Polska incydentów w latach 2018–2024*



Źródło: Raport roczny 2024 z działalności CERT Polska, s. 90.

Wyzwaniem staje się także integracja systemu zarządzania kryzysowego z rosnącą liczbą zewnętrznych interesariuszy, w tym firm infrastrukturalnych (energetyka, gazownictwo, telekomunikacja), operatorów usług transportowych czy organizacji społecznych. W sytuacji wystąpienia incydentu, który ma charakter wielowymiarowy i przekracza kompetencje jednego podmiotu, kluczowe znaczenie mają ustalone kanały komunikacji, wspólne procedury oraz przećwiczone scenariusze działania. Braki w tych obszarach skutkują chaosem organizacyjnym, opóźnieniami decyzyjnymi oraz wzrostem strat materialnych i społecznych.

Kolejną kategorią zagrożeń są zdarzenia o charakterze hybrydowym, których skutki mogą być trudne do jednoznacznego przypisania sprawcy, a przebieg łączy elementy działań fizycznych i cyfrowych. Mowa tu m.in. o sabotażu infrastruktury krytycznej, celowym szerzeniu dezinformacji,

próbach zakłócenia wyborów lokalnych czy kampaniach mających na celu destabilizację społeczną. JST, jako podmioty odpowiedzialne za przygotowanie procesów wyborczych, rejestrację obywateli czy zarządzanie informacją, stają się potencjalnym celem takich działań, nawet jeśli są one prowadzone przez podmioty spoza granic państwa. Odporność informacyjna samorządu, rozumiana jako zdolność do przeciwdziałania dezinformacji i zachowania ciągłości działania w warunkach presji psychologicznej, staje się zatem nowym elementem systemu bezpieczeństwa lokalnego.

W literaturze przedmiotu przyjmuje się, że skuteczne zarządzanie bezpieczeństwem lokalnym wymaga przede wszystkim prawidłowego rozpoznania i klasyfikacji możliwych incydentów (Żurawski, Ciekanowski, 2022, s. 367).

W coraz większym stopniu na zagrożenia należy także patrzeć przez pryzmat interdyscyplinarności – granice między incydentami środowiskowymi, cyfrowymi a społecznymi coraz bardziej się zacierają. Na przykład silne burze mogą uszkodzić infrastrukturę energetyczną, co z kolei prowadzi do przerwy w działaniu systemów teleinformatycznych JST, uniemożliwiając pracę urzędów oraz systemów alarmowych. W takich warunkach obywatele mogą zacząć działać spontanicznie, co może przerodzić się w chaos komunikacyjny, panikę, a w skrajnych przypadkach – w akty agresji lub przemoc. Oznacza to, że przygotowanie JST do reagowania na incydenty nie może być już domeną jedynie urzędów i struktur obrony cywilnej – konieczna jest koordynacja z mieszkańcami i lokalnymi liderami opinii.

W tym kontekście coraz częściej mówi się o potrzebie budowania lokalnej odporności systemowej (ang. *local resilience*), rozumianej jako zdolność wspólnot lokalnych do adaptacji, przetrwania i odbudowy po zdarzeniach kryzysowych (Shaw, Maythorne, 2012). Obejmuje to nie tylko inwestycje w infrastrukturę czy sprzęt ratowniczy, lecz także tworzenie mechanizmów komunikacji kryzysowej, edukację mieszkańców w zakresie reagowania na zagrożenia, rozwój wolontariatu kryzysowego czy budowanie zaufania do instytucji publicznych. W związku z poprawą odporności systemów informatycznych administracji publicznej, w tym również JST, oraz budowaniem zdolności do skutecznego zapobiegania incydentom i reagowania na nie, zgodnie z zapisami strategii konieczne jest ustanowienie Narodowych Standardów

Cyberbezpieczeństwa jako zbioru wymagań organizacyjnych i technicznych dotyczących w pierwszej kolejności bezpieczeństwa:

- aplikacji,
- urządzeń mobilnych,
- stacji roboczych,
- serwerów i sieci,
- modeli chmury obliczeniowej (Karpiuk, 2021, s. 48).

W Polsce, choć w niektórych gminach i miastach pojawiają się dobre praktyki (np. systemy ostrzegania SMS, aplikacje mobilne ds. bezpieczeństwa, lokalne grupy ratownicze), wciąż brakuje jednolitej strategii wzmacniania odporności JST na poziomie krajowym.

W kontekście globalnych trendów coraz częściej analizuje się również zjawisko tzw. przeciążenia informacyjnego (ang. *information overload*) jako nowej formy zagrożenia dla JST. Podczas incydentu, zwłaszcza nagłego, jednostki samorządu są zalewane ogromną ilością informacji pochodzących z różnych źródeł: od służb ratunkowych, przez media, aż po media społecznościowe i samych obywateli. Brak narzędzi do skutecznej filtracji, weryfikacji i przekazywania informacji może prowadzić do błędnych decyzji, opóźnień i eskalacji kryzysu. Właściwe zarządzanie informacją, jej centralizacja i automatyzacja analizy (np. z wykorzystaniem sztucznej inteligencji lub systemów klasy PSIM (*Physical Security Information Management*) mogą stać się w niedalekiej przyszłości standardem w dużych JST.

W celu lepszego zrozumienia skali oraz charakteru wyzwań, z jakimi mierzą się jednostki samorządu terytorialnego, warto przywołać konkretne przypadki incydentów bezpieczeństwa, które miały miejsce na poziomie lokalnym w Polsce w ostatnich latach. Przykładem może być cyberatak w województwie podkarpackim na jeden z urzędów, a dokładnie na Urząd Miasta i Gminy Nowa Sarzyna. Naruszono bezpieczeństwo danych znajdujących się bazach. W oficjalnym komunikacie do sprawy wskazano, że osoby z zewnątrz włamały się na serwery i zaszyfrowały bazy danych za pomocą oprogramowania ransomware. Z wydanego zawiadomienia wynika, że mowa m.in. o imionach i nazwiskach, adresach zamieszkania, numerach PESEL, dowodach osobistych / paszportach czy stanie cywilnym (Atak hakerski na polski urząd, Cyberdefence, 2025).

Innym przykładem jest atak typu ransomware w Kościerzynie, w którym złośliwe oprogramowanie z rodziny Mapo doprowadziło do zaszyfrowania danych urzędowych i sparaliżowało działanie systemów informatycznych, co unaocznia skalę zagrożeń dla administracji lokalnej. Dzięki zaangażowaniu specjalistów udało się opracować narzędzie umożliwiające odszyfrowanie plików i przywrócenie dostępu do informacji, co podkreśla znaczenie posiadania procedur awaryjnych i współpracy z ekspertami w dziedzinie cyberbezpieczeństwa (Gmina Kościerzyna skutecznie odszyfrowała swoje dane po ataku ransomware, Sekurak, 2019).

W Otwocku doszło do innego incydentu, w wyniku którego cyberprzestępcy uzyskali dostęp do serwerów Urzędu Miasta i zaszyfrowali dane, zakłócając funkcjonowanie kluczowych usług publicznych – w tym obsługi kart metropolitalnych, programów wsparcia dla rodzin wielodzietnych, a także systemów podatkowych i gospodarki odpadami. Zdarzenie to wpłynęło bezpośrednio na jakość i ciągłość realizacji zadań administracyjnych (Serwis Samorządowy PAP, 2025).

Ofiarą ataków ransomware padło również wiele innych jednostek samorządu terytorialnego. W Urzędzie Gminy Tuczna cyberprzestępcy zaszyfrowali m.in. dane księgowe, informacje podatkowe, dane osobowe oraz numery kont bankowych, domagając się okupu (Atak hakerski na Urząd Gminy Tuczna, RadioBiper, 2021).

Podobne incydenty miały miejsce w Urzędzie Marszałkowskim Województwa Małopolskiego w Krakowie (Zhakowano Urząd Marszałkowski w Krakowie, Cyberdefence24, 2021) oraz w Starostwie Powiatowym w Oświęcimiu (Atak hakerów w Starostwie Powiatowym w Oświęcimiu, InfoOswiecim.pl, 2025) gdzie zaatakowane zostały podsystemy informatyczne. Wszystkie te przypadki wskazują na pilną potrzebę wzmacniania odporności cyfrowej samorządów oraz wdrażania skutecznych środków zapobiegawczych i reagowania na cyberzagrożenia.

Te zdarzenia pokazują, że JST muszą być przygotowane także na incydenty wykraczające poza klasyczne schematy zagrożeń – takie, które mają charakter społeczno-komunikacyjny i wymagają odpowiednich narzędzi zarządzania dialogiem oraz narracją publiczną, dlatego rola jednostek samorządu terytorialnego w realizacji zadań z zakresu zapewnienia bezpieczeństwa społeczności

lokalnych nie powinna się sprowadzać tylko do realizacji ustawowych zobowiązań (Mróz, 2017, s. 123).

Analiza studiów przypadków ujawniła powtarzalne schematy reakcji organizacyjnych JST na incydenty cyberbezpieczeństwa. Do najczęściej identyfikowanych problemów należały: brak aktualnych planów ciągłości działania, niewłaściwe zabezpieczenie kopii zapasowych, niejednoznaczny podział odpowiedzialności w sytuacjach kryzysowych oraz opóźniona lub niespójna komunikacja z mieszkańcami. Jednocześnie przypadki, w których uruchomiono procedury awaryjne i zaangażowano zewnętrznych ekspertów, wskazują na znaczenie wcześniejszego przygotowania organizacyjnego i testowania procedur reagowania.

Znaczenie i istota zarządzania incydentami w jednostkach samorządu terytorialnego – wnioski z analizy raportu Najwyższej Izby Kontroli

Cyberbezpieczeństwo postrzegane jest dziś jako jedno z kluczowych wyzwań o charakterze społeczno-technologicznym, przed którymi stoją instytucje sektora publicznego. Coraz częściej podkreśla się potrzebę jego zapewnienia w funkcjonowaniu administracji publicznej, w tym również w strukturach samorządu terytorialnego. Zagadnienie to znajduje coraz szersze odzwierciedlenie zarówno w literaturze naukowej, jak i w strategiach rządowych oraz raportach opracowywanych przez niezależne ośrodki analityczne (Chodakowska i in., 2022, s. 133).

Zarządzanie incydentami bezpieczeństwa w jednostkach samorządu terytorialnego wymaga systemowego i strategicznego podejścia, które wykracza poza działania o charakterze techniczno-administracyjnym. W świetle wyników kontroli Najwyższej Izby Kontroli z 2025 r., przeprowadzonej w 24 urzędach JST, uwidacznia się poważna luka organizacyjna i proceduralna w zakresie przygotowania do reagowania na incydenty i zapewniania ciągłości działania. Aż 71% kontrolowanych jednostek nie miało polityki ciągłości działania, a połowa z nich nie wdrożyła planów odtworzeniowych (Raport NIK, 2025).

Co więcej, tam, gdzie dokumentacja formalnie istniała, najczęściej nie była testowana, co uniemożliwiało realną weryfikację skuteczności przyjętych rozwiązań.

Raport NIK wskazuje, że zarządzanie incydentami musi być rozumiane jako cykliczny i wieloetapowy proces obejmujący planowanie, zapobieganie, reagowanie i odbudowę. W wielu JST brakuje systemów zarządzania bezpieczeństwem informacji (SZBI), które pozwalałyby na identyfikację aktywów informacyjnych, ocenę ryzyka oraz wdrażanie adekwatnych środków ochrony. W jednej trzeciej urzędów taki system w ogóle nie funkcjonował, a w pozostałych przypadkach nie był przeglądany lub aktualizowany. Problemem jest także fakt, że ochrona informacji często ogranicza się wyłącznie do danych osobowych, pomijając inne kluczowe zasoby, takie jak informacje finansowe, dane z rejestrów podatkowych czy informacje o infrastrukturze krytycznej.

Niepokojące są również ustalenia dotyczące braku jednoznacznego przypisania odpowiedzialności za działania w sytuacjach incydentalnych. Choć w większości urzędów wyznaczono osoby do kontaktu z krajowym systemem cyberbezpieczeństwa, w praktyce ich działania były fragmentaryczne, a obowiązki realizowane często z opóźnieniem lub niezgodnie z przepisami. W wielu przypadkach funkcja inspektora ochrony danych była łączona z obowiązkami audytorskimi, co prowadziło do konfliktu interesów i naruszało zasadę niezależności wymaganą przez normy ISO oraz przepisy RODO.

Zarządzanie incydentami bezpieczeństwa nie może ograniczać się do reakcji na zdarzenia. Równie ważne są działania prewencyjne, takie jak szkolenia, audyty wewnętrzne oraz analizy ryzyka. Tymczasem NIK wykazała, że 42% urzędów nie zapewniało pracownikom szkoleń z zakresu bezpieczeństwa informacji, a w 37% nie przeprowadzano corocznych audytów lub realizowano je nierzetelnie. Brakuje też mechanizmów umożliwiających uczenie się na błędach – procedury reagowania nie były aktualizowane zgodnie z doświadczeniami z wcześniejszych incydentów, a wiedza operacyjna nie była systematyzowana i wykorzystywana w doskonaleniu procedur. Na wykresie w przestawiono najczęściej stwierdzane nieprawidłowości w kontrolowanych jednostkach przez NIK.

Wykres 2. *Najczęściej stwierdzane nieprawidłowości w kontrolowanych przez NIK jednostkach*

Źródło: Zapewnienie bezpieczeństwa informacji oraz ciągłości działania systemów informatycznych w jednostkach samorządu terytorialnego, Raport NIK, Warszawa 2025.

Z raportu wynika również, że wiele JST nie zabezpiecza należycie relacji z partnerami zewnętrznymi. W jednej trzeciej analizowanych umów z dostawcami usług informatycznych brakowało kluczowych zapisów dotyczących poufności danych i procedur postępowania w sytuacjach zagrożenia. Z kolei w połowie urzędów nieprawidłowo przechowywano kopie zapasowe danych – w miejscach narażonych na te same czynniki ryzyka, co systemy źródłowe, np. w tej samej serwerowni, co naruszało podstawowe zasady bezpieczeństwa fizycznego.

Braki organizacyjne, niska świadomość kierownictwa JST, niedobory kadrowe w działach IT oraz ograniczenia finansowe prowadzą do stanu, w którym wiele samorządów jest nieprzygotowanych na skuteczne reagowanie na incydenty bezpieczeństwa. Wprowadzenie zintegrowanych, formalnych systemów zarządzania ryzykiem oraz procedur ciągłości działania – zgodnie z normami ISO 27001 i ISO 22301 – powinno stać się priorytetem każdej jednostki samorządu terytorialnego. Zarządzanie incydentami nie jest wyłącznie zadaniem informatyka czy inspektora danych osobowych – to kompetencja strategiczna, która wymaga zaangażowania całej organizacji, od najwyższego kierownictwa po pracowników operacyjnych.

Wnioski płynące z raportu NIK jasno pokazują, że zarządzanie incydentami w samorządzie musi być oparte na planowości, odpowiedzialności, testowalności i przejrzystości. Odpowiednio zaprojektowany i wdrożony system może nie tylko ograniczyć straty wynikające z incydentów, ale także wzmocnić zaufanie obywateli do instytucji publicznych oraz zwiększyć odporność JST na zagrożenia współczesnego świata. Wnioski płynące z analizy studium przypadków oraz analizy raportu NIK pozwalają wskazać najczęstsze błędy organizacyjne popełniane przez JST w kontekście zarządzania incydentami bezpieczeństwa. Do najważniejszych należą:

- brak aktualnych planów reagowania kryzysowego, często niedostosowanych do realnych zagrożeń lub niekompatybilnych z planami powiatowymi i wojewódzkimi;
- niedostateczne przygotowanie kadry administracyjnej – w wielu JST osoby odpowiedzialne za zarządzanie kryzysowe nie mają specjalistycznych szkoleń ani doświadczenia w koordynowaniu działań w warunkach zagrożenia;
- brak mechanizmów komunikacji z mieszkańcami – w tym brak nowoczesnych systemów alarmowania, stron internetowych o charakterze kryzysowym czy narzędzi dwustronnej komunikacji;
- fragmentaryczność współpracy międzysektorowej – ograniczona współpraca z sektorem prywatnym, organizacjami pozarządowymi czy społecznościami lokalnymi;
- słaba kultura ćwiczeń i testowania procedur – wiele JST nie przeprowadza regularnych symulacji sytuacji kryzysowych z udziałem mieszkańców i służb zewnętrznych.

W związku z powyższym niniejszy artykuł postuluje szereg praktycznych rekomendacji, które mogą przyczynić się do zwiększenia skuteczności JST w zakresie zarządzania incydentami bezpieczeństwa:

- wprowadzenie obowiązkowych audytów bezpieczeństwa w JST, obejmujących analizę ryzyka, ocenę planów zarządzania kryzysowego oraz gotowość kadrową;
- rozwój lokalnych centrów zarządzania kryzysowego jako stałych struktur koordynacyjnych, wyposażonych w zaplecze techniczne i kompetencyjne;

- budowa zintegrowanych systemów komunikacji kryzysowej – w tym alertów mobilnych, platform informacyjnych, integracji z mediami społecznościowymi oraz kanałów kontaktu z grupami szczególnego ryzyka;
- wsparcie dla edukacji i treningów – w tym organizacja regularnych szkoleń dla urzędników, ćwiczeń symulacyjnych z udziałem społeczności oraz tworzenie lokalnych sieci wolontariatu kryzysowego;
- tworzenie strategii odporności lokalnej, która uwzględnia nie tylko aspekty infrastrukturalne, ale również społeczne, informacyjne i organizacyjne.

Zarządzanie incydentami bezpieczeństwa w jednostkach samorządu terytorialnego nie jest wyłącznie zadaniem techniczno-administracyjnym. To proces złożony, wymagający interdyscyplinarnego podejścia, integracji struktur lokalnych oraz aktywnego włączenia społeczności. Tylko budowanie odporności instytucjonalnej, organizacyjnej i społecznej może zagwarantować skuteczność reagowania na współczesne, często niestandardowe i hybrydowe zagrożenia, z jakimi mierzy się samorząd w XXI w.

Dyskusja

Uzyskane wyniki analizy potwierdzają, że problematyka zarządzania incydentami cyberbezpieczeństwa w jednostkach samorządu terytorialnego powinna mieć charakter systemowy i strukturalny, a nie incydentalny czy wyłącznie techniczny. Wnioski płynące z analizy raportu Najwyższej Izby Kontroli, danych CERT Polska oraz studiów przypadków JST wpisują się w szerszy nurt badań nad bezpieczeństwem administracji publicznej, które wskazują na deficyty organizacyjne, proceduralne i kompetencyjne jako główne źródła podatności na incydenty bezpieczeństwa. Jednocześnie analiza pozwala zauważyć, że w polskich JST problemy te mają swoją specyfikę wynikającą z ograniczeń zasobowych, rozproszenia kompetencji oraz niedostatecznej integracji zarządzania bezpieczeństwem z ogólnym systemem zarządzania jednostką.

W kontekście międzynarodowych standardów zarządzania incydentami, takich jak ISO/IEC 27035 czy NIST SP 800-61, widoczna jest istotna luka pomiędzy deklarowanymi obowiązkami a faktycznym poziomem dojrzałości organizacyjnej JST. Standardy te jednoznacznie wskazują, że skuteczne

zarządzanie incydentami powinno być procesem cyklicznym, obejmującym nie tylko reakcję na zdarzenie, lecz także fazy przygotowania, testowania, odtwarzania oraz systematycznego uczenia się na podstawie wcześniejszych doświadczeń. Tymczasem analiza wykazała, że w wielu JST działania ograniczają się do doraźnego reagowania po wystąpieniu incydentu, bez wdrożonych mechanizmów formalnej ewaluacji i aktualizacji procedur. W rezultacie każdorazowe zdarzenie traktowane jest jako sytuacja wyjątkowa, a nie jako element powtarzalnego cyklu zarządzania ryzykiem.

Istotnym elementem wymagającym dyskusji jest również relacja pomiędzy zarządzaniem incydentami a ciągłością działania JST. Zgodnie z założeniami normy ISO 22301 planowanie ciągłości działania powinno stanowić integralny komponent zarządzania organizacją, a nie wyłącznie techniczny dodatek do systemów informatycznych (Sitek M. 2023, s. 130). Wyniki analizy wskazują jednak, że w praktyce JST często nie mają spójnych i testowanych planów ciągłości działania, a jeśli dokumenty takie istnieją, mają charakter formalny i nie są wykorzystywane operacyjnie. Prowadzi to do sytuacji, w której incydenty cyberbezpieczeństwa skutkują paraliżem funkcjonowania urzędu, zakłóceniem realizacji usług publicznych oraz eskalacją kryzysu w wymiarach społecznym i komunikacyjnym.

Wyniki studiów przypadków pozwalają również na pogłębioną refleksję nad rolą czynnika ludzkiego i kultury bezpieczeństwa informacji w JST. Analiza potwierdza ustalenia wcześniejszych badań, zgodnie z którymi niski poziom świadomości pracowników administracji publicznej, brak regularnych szkoleń oraz marginalizowanie zagadnień bezpieczeństwa w codziennej praktyce organizacyjnej znacząco zwiększają ryzyko skutecznych ataków cybernetycznych. W tym kontekście zarządzanie incydentami nie powinno być postrzegane wyłącznie jako domena działów IT czy inspektorów ochrony danych, lecz jako element kultury organizacyjnej całej jednostki, wymagający zaangażowania kadry kierowniczej oraz jasnego przypisania odpowiedzialności.

Na uwagę zasługuje również problem fragmentaryczności współpracy międzyinstytucjonalnej. Analiza wskazuje, że JST często funkcjonują w izolacji, a wymiana informacji o incydentach, dobrych praktykach czy błędach organizacyjnych ma charakter ograniczony i niesformalizowany. Tymczasem rekomendacje ENISA oraz doświadczenia innych państw UE podkreślają

znaczenie sieciowego podejścia do zarządzania incydentami, opartego na współdzieleniu wiedzy, standaryzacji procedur oraz interoperacyjności systemów reagowania. Brak takich mechanizmów w polskich JST prowadzi do powielania tych samych błędów organizacyjnych i ogranicza możliwość budowania odporności systemowej na poziomie lokalnym i regionalnym.

Dyskusji wymaga także kwestia wykorzystania raportu NIK jako kluczowego źródła empirycznego. Z jednej strony raport ten dostarcza unikatowych, przekrojowych danych o stanie zabezpieczeń i praktykach organizacyjnych JST, z drugiej jednak nie może być traktowany jako substytut badań naukowych w ścisłym sensie metodologicznym. Przeprowadzona analiza pokazuje jednak, że poprzez rekontekstualizację ustaleń NIK w ramach teorii zarządzania incydentami oraz zestawienie ich z analizą studiów przypadków możliwe jest wygenerowanie wiedzy *ponadraportowej*, w postaci uogólnionych wzorców słabości systemowych i rekomendacji o charakterze strategicznym.

Ograniczeniem niniejszego artykułu jest jego wtórny charakter oraz oparcie na dostępnych źródłach instytucjonalnych i opisach przypadków, co nie pozwala na pełną weryfikację zależności przyczynowo-skutkowych ani ocenę poziomu dojrzałości zarządzania incydentami w całej populacji JST. Jednocześnie ograniczenie to wskazuje kierunki dalszych badań, w szczególności potrzebę realizacji badań empirycznych opartych na wywiadach pogłębionych, badaniach ankietowych oraz analizie dokumentów wewnętrznych JST według jednolitej procedury badawczej.

Podsumowując, wyniki analizy i ich interpretacja prowadzą do wniosku, że skuteczne zarządzanie incydentami cyberbezpieczeństwa w JST wymaga przejścia od podejścia reaktywnego do podejścia systemowego, opartego na cyklu zarządzania incydentem, integracji z planowaniem ciągłości działania oraz budowaniu odporności cyfrowej samorządu. Dyskusja ta wzmacnia tezę, że bez włączenia zarządzania incydentami w strategiczne ramy bezpieczeństwa lokalnego JST pozostaną podatne na powtarzalne zakłócenia funkcjonowania, niezależnie od postępu technologicznego czy formalnych obowiązków prawnych.

Wnioski

Przedstawione wnioski wynikają bezpośrednio z analizy raportu NIK, danych CERT Polska oraz syntetycznej analizy studiów przypadków incydentów cyberbezpieczeństwa w JST. Zarządzanie incydentami bezpieczeństwa w jednostkach samorządu terytorialnego stanowi dziś jedno z kluczowych wyzwań funkcjonalnych, organizacyjnych i strategicznych w ramach systemu bezpieczeństwa publicznego. W obliczu coraz bardziej złożonych zagrożeń – zarówno tradycyjnych (katastrofy naturalne, awarie infrastruktury), jak i nowoczesnych (cyberataki, dezinformacja, zagrożenia hybrydowe) – JST muszą rozwijać kompleksowe mechanizmy reagowania, planowania oraz odbudowy po kryzysie. Wnioski płynące z raportu NIK z 2025 r. jednoznacznie wskazują, że wiele samorządów nie ma niezbędnych polityk, procedur ani zdolności organizacyjnych do skutecznego zarządzania incydentami, co zwiększa ryzyko paraliżu funkcjonowania urzędów oraz utraty zaufania społecznego.

Skuteczne zarządzanie incydentami wymaga przede wszystkim wdrożenia podejścia systemowego, opartego na identyfikacji i klasyfikacji zagrożeń, planowaniu ciągłości działania, wyznaczeniu jednoznacznych ról i odpowiedzialności, a także integracji działań między różnymi podmiotami – zarówno wewnątrz JST, jak i z partnerami zewnętrznymi. Nieodzowne staje się także wzmacnianie kompetencji kadry, regularne szkolenia, przeprowadzanie testów planów awaryjnych oraz prowadzenie rzetelnych audytów bezpieczeństwa informacji.

Studia przypadków ataków ransomware, które dotknęły różne samorządy w Polsce, wskazują jednoznacznie na potrzebę budowania odporności cyfrowej. Brak procedur odtworzeniowych, nieaktualne kopie zapasowe, nieskuteczna komunikacja wewnętrzna czy niejasna struktura decyzyjna – to najczęściej powtarzające się słabości organizacyjne. Równocześnie tam, gdzie doszło do szybkiego zaangażowania ekspertów i uruchomienia planów awaryjnych, możliwe było ograniczenie strat i przywrócenie ciągłości działania.

Wnioskiem końcowym jest konieczność traktowania zarządzania incydentami nie jako epizodycznego działania technicznego, lecz jako integralnego komponentu strategii bezpieczeństwa lokalnego. JST, które świadomie rozwijają swoje zdolności w tym zakresie, nie tylko minimalizują ryzyko operacyjne, ale również budują zaufanie obywateli, wzmacniają odporność instytucjonalną

i przyczyniają się do podniesienia jakości usług publicznych. W dobie cyfrowej transformacji i złożonych zagrożeń bezpieczeństwa, kompetentne zarządzanie incydentami staje się podstawowym warunkiem trwałego i skutecznego funkcjonowania administracji samorządowej.

References

Jańczuk, L. (2015). *Samorząd terytorialny w systemie bezpieczeństwa publicznego*. W: E.M. Guzik-Makaruk, E.W. Pływaczewski (red.). *Współczesne oblicza bezpieczeństwa* (s. 325–335). Białystok: Wydawnictwo Temida 2.

Kwiecińska, M., Ordyniec, E., Żurawski, S. (2023). *Cyberzagrożenia jako główna determinanta bezpieczeństwa społecznego*. W: J. Wołejszo, K. Rejman, M. Wilczyńska (red.). *Bezpieczeństwo informacji wobec współczesnych zagrożeń* (s. 131–156). Kalisz: Kaliskie Towarzystwo Przyjaciół Nauk, Akademia Kaliska im. Prezydenta Stanisława Wojciechowskiego.

Mickiewicz, P. (2020). *Bezpieczeństwo społeczności lokalnych. Organizacja systemy i projektowanie działań*. Poznań: Wydawnictwo Naukowe FNCE.

Mróz, B. (2017). *Rola i zadania organów administracji samorządowej w systemie bezpieczeństwa publicznego*. W: M. Sitek, E. Feret, J. Dobkowski (red.). *Wydawanie aktów administracyjnych jako forma realizacji zadań samorządu terytorialnego* (s. 111–124). Józefów: Wyższa Szkoła Gospodarki Euroregionalnej im. Alcide De Gasperi.

Żurawski, S., Ciekanowski, Z. (2023). *Wpływ zagrożeń w cyberprzestrzeni na bezpieczeństwo państwa*. W: D. Brążkiewicz, J. Nowicka, Z. Ciekanowski, L. Elak (red.). *Współczesne wyzwania dla bezpieczeństwa państwa* (s. 9–27). Warszawa: Wydawnictwo im. Profesora Leszka Krzyżanowskiego Menedżerskiej Akademii Nauk Stosowanych w Warszawie.

Żurawski, S., Ciekanowski, Z. (2022). *Zarządzanie bezpieczeństwem informacyjnym w jednostkach samorządu terytorialnego*. W: J. Wołejszo, K. Rejman, M. Wilczyńska (red.). *Ryzyko i niepewność w bezpieczeństwie informacji* (s. 365–379). Kalisz: Kaliskie Towarzystwo Przyjaciół Nauk.

Artykuły

Cichonski, P., Millar, T., Grance, T., Scarfone, K. (2012). *Computer security incident handling guide* (NIST Special Publication 800-61 Rev. 2). National Institute of Standards and Technology.

Ciekanowski, M., Gruchelski, J., Nowicka, J., Żurawski, S., Pauliuchuk, Y. (2023). Cyberspace as a Source of New Threats to the Security of the European Union. *European Research Studies Journal*, 26(3), s. 782–797.

European Union Agency for Cybersecurity. (2023). *Good practices for incident management. ENISA*. Retrieved May 20, 2025.

Gerwatowski, J. (2019). Bezpieczeństwo informacyjne w jednostkach samorządu terytorialnego. *Studia Prawnoustrojowe*, 44, s. 89–106.

Hoffman, I. (2020). Cseh K.B. E-administration, cybersecurity and municipalities – the challenges of cybersecurity issues for the municipalities in Hungary.*Cybersecurity and Law*, 4(2), s. 199–211.

Karpiuk, M. (2021). Cybersecurity as an element in the planning activities of public administration. *Cybersecurity and Law*, 1, s. 45–52.

Klonowska, I., Hytrek, A. (2008). Policja a cyberprzestrzeń. *Kwartalnik Policyjny*, 2, s. 18–20.
Nowicka, J., Kopczewski, M., Ciekanowski, Z., Król A. (2023). Cyberspace and Related Threats. *European Research Studies Journal*, 2, s. 421–435.
Rozwadowski, M. (2014). Bezpieczeństwo społeczności lokalnych oraz działania zmierzające do jego poprawy. *Kultura Bezpieczeństwa. Nauka–Praktyka–Refleksje*, 15, s. 243–252.
Shaw, K., Maythorne, L. (2012). Managing for local resilience: towards a strategic approach. *Public Policy and Administration*, 28(1), s. 43–65.
Sitek, M. (2023). Konstytucyjne i ustawowe podstawy współpracy samorządów gminnych z organizacjami pozarządowymi w zakresie realizacji funkcji świadczącej wobec uchodźców wojennych z Ukrainy. *Przegląd Prawa Konstytucyjnego*, 4(74), s. 121–134.
Włodyka, E. (2022). Gotowi – do startu – start? Przyczynek do dyskusji nad gotowością jednostek samorządu terytorialnego do zapewniania cyberbezpieczeństwa. *Cybersecurity and Law*, 1(7), s. 202–219.

Akty prawne i inne dokumenty

International Organization for Standardization. (2016). ISO/IEC 27035-1:2016 Information technology – Security techniques – Information security incident management — Part 1: Principles of incident management. ISO.
International Organization for Standardization. (2019). ISO 22301:2019 Security and resilience – Business continuity management systems – Requirements. ISO.
Raport roczny 2024 z działalności CERT Polska.
Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych. Dz.U. z 2024 r., poz. 773.
Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych. Dz.U. z 2018 r., poz. 1000.
Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Dz.U. z 2018 r., poz. 1560.
Zapewnienie bezpieczeństwa informacji oraz ciągłości działania systemów informatycznych w jednostkach samorządu terytorialnego, Raport NIK, Warszawa 2025.

Źródła internetowe

Atak hakerów w Starostwie Powiatowym w Oświęcimiu, https://infooswiecim.pl/info-z-miasta/atak-hakerow-w-starostwie-powiatowym-w-oswiecimiu/ (dostęp: 20.05.2025).
Atak hakerski na polski urząd, https://cyberdefence24.pl/cyberbezpieczenstwo/atak-hakerski-na-polski-urzad (dostęp: 20.05.2025).

Atak hakerski na Urząd Gminy Tuczna. Gmina apeluje o zachowanie ostrożności, RadioBiper, https://radiobiper.info/2021/12/13/atak-hakerski-na-urzad-gminy--tuczna-gmina-apeluje-o-zachowanie-ostroznosci/ (dostęp: 20.05.2025).

Gmina Kościerzyna skutecznie odszyfrowała swoje dane po ataku ransomware!, https://sekurak.pl/gmina-koscierzyna-skutecznie-odszyfrowala-swoje-dane-po-ataku--ransomware/ (dostęp: 20.05.2025).

Urząd miejski w Otwocku padł ofiarą cyberataku, Serwis Samorządowy PAP, https://samorzad.pap.pl/kategoria/e-urzad/urzad-miejski-w-otwocku-padl-ofiara-cyberataku (dostęp: 20.05.2025).

Zhakowano Urząd Marszałkowski w Krakowie, https://cyberdefence24.pl/polityka-i--prawo/zhakowano-urzad-marszalkowski-w-krakowie (dostęp: 20.05.2025).