

Informujemy, iż w celu optymalizacji treści dostępnych w naszym serwisie i dostosowania ich do Państwa indywidualnych potrzeb korzystamy z informacji zapisanych za pomocą plików cookies na urządzeniach końcowych użytkowników. Pliki cookies użytkownik może kontrolować za pomocą ustawień swojej przeglądarki internetowej. Dalsze korzystanie z naszego serwisu internetowego bez zmiany ustawień przeglądarki internetowej oznacza, iż użytkownik akceptuje stosowanie plików cookies.

[Akceptuję pliki cookies](#)

MENU

[Instrukcja korzystania z BIP](#)

[Nabór](#)

[Zamówienia publiczne](#)

[Organizacja przyjmowania i załatwiania skarg i wniosków](#)

[Podstawa prawna powstania Centrum Usług Informatycznych w Białymstoku](#)

[Plan zamówień publicznych](#)

[Sprawozdania finansowe](#)

[Dostęp do informacji publicznej nieudostępnionej w BIP](#)

[Ochrona danych osobowych](#)

[Cyberbezpieczeństwo](#)

[Zarządzenia](#)

[Petycje](#)

[Sygnałista](#)

[Raport o stanie zapewnienia dostępności podmiotu publicznego
zgłoszeń naruszeń prawa](#)

Incydent cyberbezpieczeństwa w Urzędzie Miejskim w Wadowicach - analiza i wnioski

Opis zdarzenia

W dniu 5 października 2025 r. doszło do ataku typu ransomware na infrastrukturę IT Urzędu Miejskiego w Wadowicach. Celem ataku były m.in. bazy danych zawierające dane osobowe pracowników urzędu oraz mieszkańców gminy. Sprawcy najprawdopodobniej zaszyfrowali dane, a także – według wstępnych ustaleń – mogli wykraść część informacji, co stwarza ryzyko ich upublicznienia.

Działania podjęte po incydencie

- Urząd przeprowadził weryfikację wewnętrzną i poinformował o możliwym wycieku danych.
- Burmistrz Wadowic zapewnił, że urząd nie utracił danych, choć dostęp do nich został ograniczony ze względów bezpieczeństwa.
- Władze apelują do mieszkańców o zmianę haseł (szczególnie bankowych) i zachowanie ostrożności wobec nieznanych połączeń telefonicznych.
- Zgłoszono incydent do UODO, CSIRT, NASK oraz policji.
- Sprawą zajmuje się Centralne Biuro Zwalczania Cyberprzestępczości oraz CERT Polska, które zabezpieczyły ślady cyfrowe.

Skutki ataku

- Ryzyko kradzieży tożsamości – potencjalny wyciek danych osobowych może prowadzić do oszustw finansowych lub wykorzystania tożsamości mieszkańców do celów przestępczych.
- Częściowe ograniczenie działania urzędu – niektóre sprawy można obecnie załatwiać tylko osobiście; płatności odbywają się wyłącznie przelewem.

- Utrata zaufania społecznego i ryzyko reputacyjne dla administracji samorządowej.

Wnioski i rekomendacje

1. Potrzeba wzmocnienia bezpieczeństwa IT w administracji publicznej

Atak wykazał słabe punkty w zabezpieczeniach systemów samorządowych. Konieczne są:

- regularne audyty bezpieczeństwa,
- wdrożenie wielopoziomowego uwierzytelniania,
- szyfrowanie danych w spoczynku i w transzycie,
- tworzenie i testowanie kopii zapasowych offline.

2. Edukacja i świadomość pracowników oraz mieszkańców

- Pracownicy urzędów powinni być szkoleni w zakresie rozpoznawania potencjalnych zagrożeń.
- Mieszkańcy powinni otrzymać jasne instrukcje dot. ochrony danych i reagowania na próby oszustw (np. phishing, spoofing).

3. Sprawne procedury reagowania na incydenty

- Działania urzędu i służb były szybkie i zgodne z procedurami.
- Kluczowe jest dalsze rozwijanie współpracy z instytucjami takimi jak CERT Polska, CSIRT i CBZC.

4. Konieczność budowy zaufania po incydencie

- Transparentna komunikacja z mieszkańcami i informowanie o postępach w przywracaniu systemów oraz wynikach dochodzenia są niezbędne do odbudowy zaufania.

Podsumowanie:

Atak ransomware na urząd ujawnił poważne ryzyko związane z cyberbezpieczeństwem administracji lokalnej. Chociaż podjęto szybkie działania zaradcze, incydent ten pokazuje, jak ważne są inwestycje w zabezpieczenia IT, edukację i rozwój procedur kryzysowych. Mieszkańcy powinni pozostać czujni i zadbać o bezpieczeństwo swoich danych osobowych.

METRYKA STRONY

REJESTR ZMIAN