RAPORT Z OBSŁUGI INCYDENTU W JEDNOSTCE SAMORZĄDU TERYTORIALNEGO

Realizacja zadań podmiotu publicznego wg art. 21 i 22 Ustawy o KSC — Model In-house

Podmiot Publiczny:	Urząd Miejski w Starogrodzie	**Identyfikator:**	INC-JST-2026-114
System/Usługa:	E-Urząd & System Obsługi Mieszkańców (Baza danych)	**Krytyczność:**	ŚREDNIA / ISTOTNA (WYCIEK / NIEDOSTĘPNOŚĆ)
Klasyfikacja (KSC):	Incydent w podmiocie publicznym (Zgłoszenie CSIRT NASK)	**Model realizacji:**	Własny zespół (Wydział Informatyki / In-house)

Scenariusz: Atak BEC (Business Email Compromise) i nieautoryzowany eksport danych osobowych w Wydziale Gospodarki Nieruchomościami

W samorządach (JST), realizujących zadania podmiotu publicznego w myśl art. 21 Ustawy o KSC, procesy opierają się najczęściej na wewnętrznych, kilkuosobowych zespołach IT. Niniejszy przypadek opisuje przejęcie konta mailowego pracownika urzędu, wykorzystanie go do phishingu wewnętrznego oraz próbę eksportu bazy danych interesantów, obsłużoną w całości przez lokalnych administratorów.

Przebieg obsługi incydentu przez wewnętrzny zespół IT

Czas	Faza procesu	Opis działania technicznego (In-house)	Rola / Obsada
07:40:00	I: WYKRYWANIE	Pracownik Wydziału Finansowego zgłasza telefonicznie do lokalnego IT (Punkt Kontaktowy), że otrzymał od kierownika nieruchomości dziwny e-mail z linkiem do „pilnej korekty decyzji podatkowej”.	Pracownik Urzędu (Zgłoszenie)
07:55:00	II: ANALIZA	Lokalny administrator IT loguje się do konsoli serwera pocztowego (M365/Postfix). Analiza nagłówków: mail wysłany z autentycznego konta kierownika, ale logowanie nastąpiło z zagranicznego adresu IP (VPN/Tor). Wykryto	Starszy Informatyk / Administrator poczty

Czas	Faza procesu	Opis działania technicznego (In-house)	Rola / Obsada
		regułę ukrytą usuwającą wiadomości przychodzące.	
08:10:00	**III: POWSTRZYMANIE**	**Containment:** Natychmiastowe zresetowanie hasła skompromitowanego konta i unieważnienie wszystkich aktywnych sesji tokenów (Revoke sessions). Wstrzymanie ruchu wychodzącego z tego konta.	Informatyk Urzędu
08:30:00	**II: TRIAŻ I SKAN**	Weryfikacja logów systemów powiązanych. Wykryto, że przed zablokowaniem, z tego konta podjęto próbę pobrania załączników z bazy e-Urząd zawierających rejestry PESEL/adresy. Nastąpił częściowy eksport arkusza (ok. 120 rekordów).	ASI (Administrator Systemów Informatycznych)
10:00:00	**RAPORTOWANIE**	**Zgłoszenia ustawowe:** 1. Koordynator ds. cyberbezpieczeństwa JST zgłasza incydent do **CSIRT NASK** przez platformę S46 (wymóg KSC). 2. Powiadomienie IOD o naruszeniu ochrony danych osobowych pod kątem zgłoszenia do **UODO** (w ciągu 72h).	Koordynator ds. Cyberbezpieczeństwa / IOD
11:30:00	**III: ERADYKACJA**	Usunięcie złośliwych wiadomości phishingowych ze skrzynek innych pracowników urzędu z poziomu administracyjnego (Search-Mailbox & Delete). Pełne skanowanie stacji roboczej kierownika.	Wewnętrzny Zespół IT
13:00:00	**III: ODTWARZANIE**	Przywrócenie pełnej funkcjonalności konta po zmianie procedur dostępu. Wymuszenie fizycznego stawiennictwa pracownika w celu odebrania nowych poświadczeń i weryfikacji tożsamości.	Wydział Informatyki
15:15:00	**IV: ZAMKNIĘCIE**	Sprawdzenie logów pod kątem ponownych prób logowań z podejrzanych klas IP — brak. Zamknięcie incydentu w wewnętrznym arkuszu/ systemie ewidencji.	Kierownik Wydziału Informatyki

Specyfika Modelu In-house w Samorządzie

W modelach własnych JST wyzwaniem jest ograniczona liczba personelu. Kluczową rolę odegrała tutaj **czujność użytkownika** (Faza I) oraz szybka korelacja logów poczty z logami aplikacji dziedzinowej przez wewnętrznego administratora. Obowiązki KSC (zgłoszenie do NASK) oraz RODO (zgłoszenie do UODO) były realizowane równolegle przez wyznaczonych urzędników: IOD oraz wyznaczonego Koordynatora ds. Cyberbezpieczeństwa JST.

Działania poincydentalne (Faza IV — Wnioski i Post-Mortem)

Biorąc pod uwagę specyfikę struktury urzędu miejskiego, Kierownik Informatyki wdrożył następujący plan naprawczy o charakterze technicznym i organizacyjnym:

Wdrożone wnioski poincydentalne:

- **Techniczne (Polityka Kont):** Wdrożenie na serwerze pocztowym bezwzględnej blokady logowań spoza terytorium RP (Geofencing) dla wszystkich kont pracowniczych, o ile nie zgłoszono delegacji zagranicznej.
- **Edukacyjne:** Przeprowadzenie w trybie pilnym 15-minutowych szkoleń stanowiskowych dla pracowników Wydziału Nieruchomości oraz Finansowego z zakresu rozpoznawania ataków typu phishing i technik socjotechnicznych.
- **Organizacyjne:** Wpisanie do "Procedury zarządzania incydentami JST" obowiązku natychmiastowego powiadamiania Inspektora Ochrony Danych (IOD) w przypadku każdego incydentu dotykającego systemów przetwarzających rejestry mieszkańców.