I SAMORZĄDOWE FORUM OCHRONY LUDNOŚCI I ODPORNOŚCI SPOŁECZNEJ

Praktyczne rozwiązania dla samorządów we wdrażaniu ustawy o ochronie ludności i obronie cywilnej oraz zapewnienia ciągłości dostaw usług kluczowych i cyberbezpieczeństwa

Data: 5 czerwca 2025

Miejsce: Centrum Edukacyjno-Multimedialne, ul. Jana Pawła II 55, 05-500 Piaseczno

www.iccss.network

Międzynarodowe Centrum Bezpieczeństwa Obywatelskiego i Społecznego

RCB Rządowe Centrum Bezpieczeństwa

Podręcznik Ćwiczenia CYBRELIA 2025

Ćwiczenia z zarządzania kryzysowego oraz ochrony infrastruktury (przed, w trakcie i po) incydencie zapoczątkowanym przez cyberatak. Symulacja cyberataku na system wodociągowy Symulacja zarządzania kryzysowego
Metodologia Tabletop Exercise - Międzynarodowe Centrum Bezpieczeństwa Chemicznego (ICCSS)

Spis treści

www.iccss.network

1. Wprowadzenie do ćwiczenia CYBRELIA 2025

1.1 Koncepcja ćwiczenia

Ćwiczenie CYBRELIA 2025 to krótka, praktyczna symulacja zarządzania kryzysowego typu **Tabletop Exercise (TTX)**, przeprowadzana w ramach I Samorządowego Forum Ochrony Ludności i Odporności Społecznej. Ćwiczenie koncentruje się na zintegrowanym podejściu do cyberbezpieczeństwa i odporności w infrastrukturze krytycznej.

1.2 Kontekst wydarzenia

Ćwiczenie odbywa się podczas Forum w Piasecznie (5 czerwca 2025) jako praktyczny element wymiany doświadczeń dla przedstawicieli samorządów, służb ratowniczych i spółek komunalnych.

1.3 Czas trwania

Godzina 11:10 - 13:00 - ćwiczenie sztabowe
Sesja 3 (14:50 - 16:00) - raport i podsumowanie ćwiczenia

2. Cele i zakres ćwiczenia

2.1 Cele główne

1. **Zgranie zespołów reagowania** na złożony kryzys (cyber + infrastrukturalny)
2. **Przetestowanie komunikacji** między służbami i operatorami
3. **Ocena odporności** na dezinformację
4. **Sprawdzenie procedur** awaryjnego zaopatrzenia w wodę

2.2 Zakres tematyczny

- Cyberbezpieczeństwo systemów wodociągowych
- Zarządzanie kryzysowe na poziomie gminnym
- Komunikacja kryzysowa z mieszkańcami
- Ciągłość świadczenia usług kluczowych

3. Metodologia Tabletop Exercise

3.1 Charakterystyka TTX

- **Moderowana dyskusja** przy stole konferencyjnym
- **Scenariusz napędzany zdarzeniami** (inject-driven)
- **Fokus na procesach decyzyjnych** i współpracy
- **Interaktywna forma** z aktywnym udziałem wszystkich graczy

3.2 Fazy ćwiczenia

Faza I: Briefing (11:10-11:15)

- Przedstawienie zasad i celów
- Rozdział ról

Faza II: Realizacja scenariusza (11:15-12:45)

- Sekwencyjne wprowadzanie zdarzeń
- Podejmowanie decyzji przez zespoły
- Moderowana dyskusja

Faza III: Podsumowanie (12:45-13:00)

- Kluczowe wnioski
- Obszary do poprawy

4. Organizacja ćwiczenia

4.1 Zespół zarządzający ćwiczeniem

Exercise Director
Adam Paturej (ICCSS)

- Ogólne kierownictwo nad ćwiczeniem
- Koordynacja wszystkich aspektów

Facilitator - Lech Starostin - ICCSS
Moderator – Florian Naumczyk - RCB

- Prowadzenie ćwiczenia, moderacja dyskusji
- Wprowadzanie scenariusza
- Kontrola tempa i zadawanie pytań

5. Scenariusz główny

5.1 Tło scenariusza
Sytuacja wyjściowa:

- Trwająca fala upałów w regionie
- Dzień największego zapotrzebowania na wodę
- Normalne funkcjonowanie systemów miejskich

5.2 Główne zdarzenie
Cyberatak na system wodociągowy połączony z:

- Awarią głównego ujęcia wodociągowego
- Podejrzeniem sabotażu fizycznego
- Spadkiem ciśnienia w sieci
- Zgłoszeniami mieszkańców o problemach z wodą

5.3 Wektory zagrożeń

1. **Cybernetyczne:** Atak na systemy SCADA, manipulacja parametrów
2. **Fizyczne:** Sabotaż infrastruktury, uszkodzenie pomp
3. **Informacyjne:** Dezinformacja, fake news, atak na strony www

6. Role i odpowiedzialności uczestników

6.1 Główni gracze
Gminny Zespół Zarządzania Kryzysowego (GZZK)

- Zwołanie zespołu kryzysowego
- Koordynacja działań służb
- Wydawanie komunikatów publicznych

Powiatowa Stacja Sanitarno-Epidemiologiczna (PSSE)

- Pobór i analiza próbek wody
- Ocena ryzyka zdrowotnego
- Wydawanie zaleceń sanitarnych

Miejskie Przedsiębiorstwo Wodociągów (MPWiK)

- Analiza stanu technicznego

- Uruchomienie systemów awaryjnych
- Współpraca z zespołami IT

Państwowa Straż Pożarna (PSP)

- Zapewnienie beczkowozów
- Organizacja punktów dystrybucji wody
- Wsparcie logistyczne

Zespół Komunikacji

- Przygotowanie komunikatów
- Monitorowanie mediów społecznościowych
- Przeciwdziałanie dezinformacji

Zespół IT/Cyberbezpieczeństwa

- Analiza logów systemów SCADA
- Izolacja zainfekowanej infrastruktury
- Zgłoszenie do CSIRT NASK

7. Harmonogram ćwiczenia

7.1 Szczegółowy harmonogram

Czas	Zdarzenie	Zespoły
11:10	**STARTEX** - Briefing	Wszyscy
11:15	**Inject #1 do #9**	Właściwe podmioty
12:45	**Podsumowanie**	Wszyscy
13:00	**ENDEX**	-

8. Zasady prowadzenia ćwiczenia

8.1 Zasady ogólne

1. **Środowisko nauki** - bez oceniania personalnego
2. **Konstruktywna dyskusja** - różnice zdań mile widziane
3. **Realność decyzji** - tylko istniejące zasoby
4. **Fokus na rozwiązaniach** - problemy + propozycje

8.2 Kluczowe pytania facilitatora

Komunikacja:

- "Jak przebiega przepływ informacji między zespołami?"
- "Kto odpowiada za komunikację z mediami?"

Procedury:

- "Jakie procedury aktywujecie?"
- "Kto podejmuje decyzje o ewakuacji?"

Cyberbezpieczeństwo:

- "Jak izolujecie zaatakowane systemy?"
- "Kiedy przechodzicie na sterowanie manualne?"

Dokument opracowany przez:
Międzynarodowe Centrum Bezpieczeństwa Obywatelskiego i Społecznego (ICCSS)
W ramach I Samorządowego Forum Ochrony Ludności i Odporności Społecznej

Kontakt:
Adam Paturej: a.paturej@iccss.eu, www.iccss.network