

Ministerstwo Cyfryzacji
ul. Królewska 27
00-060 Warszawa
NIP: 5252955037
REGON: 525189465

Otwarcie danych Regionalnego Systemu Ostrzegania (RSO) w formacie CAP jako publicznego, bezobsługowego zasobu API oraz publikacja tego zasobu w portalu dane.gov.pl.

Na podstawie art. 63 Konstytucji RP oraz Ustawy o petycjach, wnoszę o podjęcie przez Ministerstwo Cyfryzacji działań zmierzających do:

1. Udostępnienia publicznego, bezobsługowego feedu danych Regionalnego Systemu Ostrzegania (RSO) w formacie zgodnym ze standardem OASIS Common Alerting Protocol (CAP) 1.2 (lub jego odpowiednika JSON), pod stałym, publicznym adresem URL, bez konieczności rejestracji, logowania czy uzyskiwania indywidualnych kluczy API.
2. Opublikowania tego zasobu w portalu dane.gov.pl jako zbioru danych o wysokiej wartości (High-Value Dataset), zgodnie z Ustawą z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego oraz dyrektywą Parlamentu Europejskiego i Rady (UE) 2019/1024 (Open Data Directive).
3. Objęcia nadzorem Ministerstwa Cyfryzacji kwestii architektury technicznej udostępniania danych RSO - w tym zastosowania mechanizmów buforowania brzegowego (Edge Caching/CDN) - niezależnie od tego, jaki podmiot będzie w przyszłości pełnił funkcję operatora technicznego systemu.
4. Podjęcia międzyresortowych działań (we współpracy z MSWiA) w celu zapewnienia stabilnej podstawy instytucjonalnej dla operatora technicznego systemów ostrzegania ludności, wobec niepewnego statusu prawnego obecnego wykonawcy (patrz uzasadnienie, pkt 4).

Uzasadnienie

1. Aktualny stan rzeczy narusza zasadę otwartości danych z domniemania

System RSO, prowadzony technicznie przez Telewizję Polską S.A. na zlecenie wojewódzkich centrów zarządzania kryzysowego, wymaga obecnie kontaktu z administratorem systemu w celu uzyskania danych dostępowych do interfejsu API opisanego jako "OpenAPI/Swagger". Tymczasem standard CAP, na którym opiera się treść komunikatów, jest z założenia formatem promującym otwartość i interoperacyjność - stosują go m.in. amerykańska National Weather Service czy Google Public Alerts, udostępniając swoje feedy bez żadnych barier rejestracyjnych.



Zgodnie z art. 5 i art. 17 Ustawy o otwartych danych, informacje sektora publicznego powinny być udostępniane w sposób otwarty, w formacie nadającym się do odczytu maszynowego, bez zbędnych barier proceduralnych. Wymóg indywidualnego wnioskowania o klucz API dla odczytu publicznych komunikatów ostrzegawczych stoi w sprzeczności z tą zasadą.

2. Bariera dostępu blokuje integrację z otwartymi systemami automatyki i realnie zmniejsza zasięg ostrzeżeń

Automatyka domowa nie jest w tym kontekście udogodnieniem drugorzędym, lecz realnym narzędziem ochrony życia i mienia, zwłaszcza w pierwszych minutach zagrożenia, zanim zadziałają kanały wymagające ręcznej reakcji człowieka (SMS, media). Otwarty, maszynowo czytelny feed CAP pozwoliłby systemom automatyki domowej na natychmiastową, bezobsługową reakcję na komunikat ostrzegawczy, np. poprzez:

- automatyczne zamknięcie rolet zewnętrznych i żaluzji - ochrona przed odłamkami szkła i falą uderzeniową w przypadku zagrożeń związanych z nalotem lub eksplozją;
- automatyczne zamknięcie bram garażowych i innych otworów budynku - ograniczenie dostępu niepowołanych osób oraz ochrona mienia w sytuacji ewakuacji lub chaosu;
- wyłączenie systemów klimatyzacji i wentylacji mechanicznej - kluczowe przy zagrożeniach chemicznych lub skażeniu powietrza, gdzie dalsze wymuszanie obiegu powietrza z zewnątrz zagraża zdrowiu domowników;
- włączenie oświetlenia awaryjnego i komunikatów głosowych w budynku - szybkie poinformowanie domowników, w tym osób starszych, niesłyszących lub śpiących, które mogą nie usłyszeć syren ani nie zauważyć powiadomienia w telefonie.

Tego rodzaju automatyzacje działają dziś w praktyce w innych krajach, w tym w Ukrainie, gdzie funkcjonuje oficjalna integracja "Ukraine Alarm" dla platformy Home Assistant, korzystająca z publicznego API ostrzeżeń o nalotach (serwis siren.pp.ua, wykorzystujący dane Ukraine Alarm). Integracja ta, obecna w oficjalnym katalogu integracji Home Assistant, tworzy czujniki binarne informujące o zagrożeniu lotniczym, artyleryjskim, chemicznym, nuklearnym oraz walkach miejskich dla wybranego regionu, umożliwiając mieszkańcom zbudowanie w pełni automatycznych scenariuszy bezpieczeństwa bez potrzeby ręcznej reakcji na powiadomienie. Polska, znajdując się w podobnym otoczeniu geopolitycznym, nie dysponuje żadnym analogicznym rozwiązaniem.

3. Argument techniczny o zagrożeniu DDoS nie wytrzymuje konfrontacji ze standardami branżowymi

Udostępnienie statycznego pliku XML/JSON odpornego na duży ruch jest zadaniem podstawowej klasy technologicznej - rozwiązywanym od kilkunastu lat przez zastosowanie buforowania brzegowego (Edge Caching, CDN) oraz przechowywania plików w magazynach obiektowych. Systemy takie jak Krajowy System e-Faktur (KSeF), znacznie bardziej złożone pod względem obciążenia, uwierzytelniania i wymogów prawnych, funkcjonują bez konieczności stosowania analogicznych barier dostępowych dla prostego odczytu danych. Utrzymywanie zamkniętego dostępu do statycznego feedu ostrzeżeń w imię ochrony przed przeciążeniem serwerów świadczy o architekturze nieadekwatnej do współczesnych standardów.

1. The first part of the paper discusses the importance of the study and the objectives of the research.

2. The second part of the paper describes the methodology used in the study.

3. The third part of the paper presents the results of the study and discusses the findings.

4. The fourth part of the paper discusses the implications of the study and the conclusions.

5. The fifth part of the paper discusses the limitations of the study and the future research.

6. The sixth part of the paper discusses the contributions of the study to the field.

7. The seventh part of the paper discusses the practical applications of the study.

8. The eighth part of the paper discusses the ethical considerations of the study.

9. The ninth part of the paper discusses the funding of the study.

10. The tenth part of the paper discusses the acknowledgments.

4. Wydarzenia z 30 lipca 2026 r. potwierdzają praktyczne konsekwencje obecnego stanu rzeczy

W nocy z 29 na 30 lipca 2026 r. w miejscowości Tarnawa-Kolonia (woj. lubelskie) doszło do upadku rosyjskiego pocisku manewrującego Ch-101, który naruszył polską przestrzeń powietrzną. W trakcie zdarzenia uruchomiono syreny alarmowe (nie we wszystkich objętych zagrożeniem powiatach), natomiast:

- mieszkańcy nie otrzymali wiadomości SMS w ramach Alertu RCB - służby wyjaśniły to czasem potrzebnym na przygotowanie i zatwierdzenie komunikatu, przy czym całe zdarzenie trwało około 13 minut;
- w aplikacji Regionalnego Systemu Ostrzegania (RSO) - zgodnie z ustaleniami dziennikarskimi - nie pojawiło się żadne powiadomienie o zdarzeniu.

Oba równoległe kanały ostrzegania zawiodły jednocześnie. Wydarzenie to pokazuje, że poleganie wyłącznie na scentralizowanych, ręcznie zatwierdzanych kanałach dystrybucji (SMS, zamknięta aplikacja) nie zapewnia wystarczającej odporności systemu ostrzegania ludności. Otwarty, maszynowo czytelny feed danych umożliwiłby niezależnym, zdecentralizowanym systemom (w tym systemom automatyki domowej) reagowanie na komunikaty regionalne w czasie rzeczywistym, równoległe do oficjalnych kanałów, bez oczekiwania na akt administracyjny każdorazowego zatwierdzania i wysyłki.

Dodatkowo, jak wynika z doniesień prasowych, Rządowe Centrum Bezpieczeństwa od 2021 r. pracuje nad wdrożeniem technologii cell broadcast, stosowanej już m.in. w Izraelu, USA, Holandii, Hiszpanii, Francji i Niemczech, jednak do dziś system ten nie został uruchomiony. Otwarcie istniejącego już API CAP w RSO stanowi rozwiązanie znacznie tańsze i szybsze do wdrożenia niż budowa nowej infrastruktury cell broadcast, a jednocześnie realnie zwiększyłoby odporność systemu ostrzegania już dziś, niezależnie od postępu prac nad cell broadcast.

5. Niepewny status prawny operatora technicznego wymaga zaangażowania Ministerstwa Cyfryzacji

Telewizja Polska S.A., obecny operator techniczny RSO, pozostaje od stycznia 2024 r. w stanie likwidacji, zarządzana przez likwidatora, którego ustawowy zakres kompetencji nie obejmuje podejmowania decyzji rozwojowych dotyczących architektury systemów IT. W tej sytuacji odpowiedzialność za standaryzację i otwarcie danych powinna zostać przejęta na poziomie międzyresortowym (Ministerstwo Cyfryzacji, we współpracy z MSWiA), niezależnie od bieżącego statusu prawnego wykonawcy technicznego, tak aby dostępność krytycznej infrastruktury bezpieczeństwa publicznego nie była uzależniona od sytuacji korporacyjnej jednego podmiotu.

Wnoszę o rozpatrzenie niniejszej petycji zgodnie z Ustawą o petycjach oraz o pisemną odpowiedź w ustawowym terminie. Postulaty zawarte w petycji nie wymagają istotnych nakładów finansowych ani nowej infrastruktury - dotyczą zmiany polityki dostępu do danych już generowanych przez system oraz zastosowania standardowych, powszechnie stosowanych mechanizmów buforowania ruchu sieciowego.

