



Ministerstwo Cyfryzacji

Sekretarz Stanu
Dariusz Standerski

BM.WP.057.183.2026
Warszawa, 11 października 2026 r.

**Szanowny Pan
Włodzimierz Czarzasty
Marszałek Sejmu RP**

Dot. pisma z 8 września br. Pośła na Sejm RP Pana Marcina Józefaciuka w sprawie podstaw twierdzeń o bezpieczeństwie danych w komercyjnych dziennikach elektronicznych oraz działań państwa po ujawnieniu incydentów (interpelacja nr 19528)

Szanowny Panie Marszałku,

poniżej przedstawiam odpowiedzi na zadane przez Pośła pytania będące we właściwości Ministra Cyfryzacji.

VI.1 Jakie testy bezpieczeństwa państwowego eDziennika były zakończone przed komunikatami z 26 i 28 sierpnia 2026 r.? Proszę podać datę, testowaną wersję, wykonawcę i jego niezależność, zakres, metodykę, liczbę ustaleń krytycznych i wysokich oraz stan ich usunięcia, bez publikowania danych umożliwiających atak.

Przed publikacją komunikatów prowadzono weryfikację bezpieczeństwa eDziennika, obejmującą m.in. analizę architektury, mechanizmów bezpieczeństwa, uprawnień dostępowych i integracji z systemami uwierzytelniania. Dalsze prace były uzależnione od usunięcia stwierdzonych niezgodności zgodnie z procesem zarządzania podatnościami i oceną ryzyka. Szczegóły testów, w tym terminy, wersje, metodyka i wyniki, nie mogą zostać ujawnione, ponieważ mogłoby to zagrozić bezpieczeństwu eDziennika oraz innych komponentów systemu mObywatel i aplikacji mObywatel.

VI. 3 Jakie mechanizmy poza uwierzytelnieniem przez Węzeł Krajowy miały gwarantować, że dostęp otrzyma wyłącznie osoba uprawniona, z uwzględnieniem nadawania i odbierania ról, błędów konfiguracji, przejęcia aktywnej sesji lub urządzenia, zmian opieki prawnej, kont serwisowych oraz zagrożeń wewnętrznych? Jak i kiedy je przetestowano?

Tożsamość użytkowników miała być potwierdzana za pośrednictwem Węzła Krajowego, z wykorzystaniem publicznych systemów i rejestrów. Dostęp ograniczały mechanizmy uwierzytelniania, autoryzacji i kontroli uprawnień stosowane w systemach administracji publicznej. Ponadto architektura rozwiązania została przygotowana z uwzględnieniem wymagań interoperacyjności oraz powszechnie obowiązujących przepisów prawa, w szczególności przepisów wykonawczych wydanych na podstawie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne¹.

Szczegóły techniczne, konfiguracja zabezpieczeń i sposób ich testowania nie mogą zostać ujawnione ze względów bezpieczeństwa ekosystemu mObywatel.

VI. 4 Czy przed użyciem rzeczywistych danych wykonano lub zaplanowano pełne testy funkcjonalne, integracyjne, wydajnościowe, odtworzeniowe i bezpieczeństwa na danych syntetycznych? Proszę podać kryteria przejścia do danych rzeczywistych, kryteria zatrzymania pilotażu oraz osoby uprawnione do podjęcia decyzji stop.

¹ Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2025 r. poz. 1703 z późn. zm.)

W ramach prac związanych z przygotowaniem eDziennika przeprowadzono kompleksowy proces weryfikacji poprawności działania, stabilności, wydajności, odtwarzalności oraz bezpieczeństwa systemu. Zrealizowano 675 przypadków testowych dla aplikacji webowej Dziennik Ucnia oraz 147 dla aplikacji mobilnej. Testy z wykorzystaniem danych syntetycznych, obejmowały m.in. kontrolę dostępu, uwierzytelnianie, autoryzację, stabilność i odtwarzanie systemu. Szczegółowe kryteria przejścia do danych rzeczywistych, wstrzymania pilotażu i procedury decyzyjne stanowią element wewnętrznych procesów zarządzania projektem i bezpieczeństwem.

VI. 5 Jakie były parametry ciągłości działania i odtwarzania, w tym RTO, RPO, dostępność, częstotliwość kopii, separacja kopii, testy odtworzenia, procedura awaryjna szkoły i komunikacja incydentu? Które z tych wymagań były zatwierdzone i zweryfikowane przed publiczną deklaracją najwyższego poziomu bezpieczeństwa?

Przygotowywane rozwiązanie obejmowało wdrożenie oraz weryfikację mechanizmów mających zapewnić ciągłość działania, możliwość odtwarzania systemu po zdarzeniach awaryjnych oraz właściwą obsługę incydentów bezpieczeństwa. Szczegółowe informacje w tym zakresie stanowią element architektury bezpieczeństwa systemu. Szczegółowe parametry, w tym RTO, RPO, dostępność, zasady wykonywania i przechowywania kopii oraz procedury awaryjne, są elementem architektury bezpieczeństwa i nie mogą zostać ujawnione.

VI. 6 Gdzie, na dzień weta, były wiążąco określone szczegółowe wymagania dotyczące szyfrowania, niezależnych audytów, testów penetracyjnych, retencji logów, terminów reakcji na incydenty, zarządzania podatnościami i nadzoru nad podwykonawcami, skoro projekt ustawy zawierał przede wszystkim ogólne obowiązki dotyczące integralności, dostępności i dostępu?

Szczegółowe wymagania dotyczące m.in. szyfrowania, audytów, testów penetracyjnych, retencji logów, obsługi incydentów, zarządzania podatnościami i nadzoru nad podwykonawcami wynikały ze standardów, procedur i metodyk jednostki realizującej projekt eDziennika. Informacje te mają charakter wewnętrzny i nie mogą zostać ujawnione ze względów bezpieczeństwa systemów administracji publicznej obsługiwanych przez tę jednostkę (w tym ekosystemu mObywatel).

VI. 7 Czy MEN i MC nadal podtrzymują, że komunikaty po wecie opisywały zweryfikowany stan faktyczny, a nie przewidywaną cechę przyszłego rozwiązania? Jeżeli tak, proszę wskazać dowody. Jeżeli nie, czy resorty sprostują lub doprecyzują przekaz, rozróżniając przejęcie konta, naruszenie zabezpieczeń systemu, naruszenie ochrony danych i faktyczny wyciek?

Komunikaty Ministra Cyfryzacji opierały się na aktualnym stanie wiedzy z prac projektowych, analitycznych i testowych. Odnosiły się do faktycznie prowadzonych działań i zastosowanych rozwiązań, a nie wyłącznie do planowanych cech systemu.

Z wyrazami szacunku
Dariusz Standerski
Sekretarz Stanu
/dokument podpisany elektronicznie/

Do wiadomości:

Kancelaria Prezesa Rady Ministrów - Departament Spraw Parlamentarnych