



PREZYDENT MIASTA KRAKOWA

OR-03.0003.112.2026

**Pan
Rafał Zawiaślak
Radny Miasta Krakowa**

Odpowiadając na Pana interpelację w sprawie awarii i blokowania użytkowników serwisu budzet.krakow.pl 16 lutego oraz przygotowania infrastruktury na wzmożony ruch po uruchomieniu formularza BO, przekazaną przez Pana Jakuba Koska, Przewodniczącego Rady Miasta Krakowa 18 lutego 2026 r., uprzejmie informuję.

Ad 1.

Po uruchomieniu formularzy do zgłaszania projektów w ramach Budżetu Obywatelskiego Miasta Krakowa 16 lutego 2026 r. mechanizmy WAF zablokowały czasowo 22 adresy IP. Blokady wyłączyły się automatycznie po upływie kilku godzin (sam okres blokad może ulegać zmianie w zależności od poziomu zagrożenia serwisów MPI). Czasowy problem z dostępem do serwisu mógł dotknąć 15 użytkowników. Blokady nie przeszkodziły w składaniu projektów: do godziny 7⁰⁰ 16 lutego br. zostało złożonych 36 projektów, do godziny 11⁰⁰ tego samego dnia zostało złożonych 46 projektów i nadal napływają nowe projekty bez żadnych zgłoszeń dotyczących funkcjonowania platformy.

Okres składania projektów wynosi 30 dni, więc chwilowa blokada dostępu dla konkretnego adresu IP (który może być też współdzielony) nie blokuje możliwości dokończenia procesu składania projektu, a dane do zgłoszenia zapisywane są w trybie roboczym do profilu użytkownika, więc do 17 marca br. można kontynuować w dowolnym terminie edycję projektu.

Ad 2.

Odblokowano automatycznie wszystkie adresy IP. Do Zespołu ds. Budżetu Obywatelskiego nie wpłynęły żadne zgłoszenia (telefoniczne ani mailowe) dotyczące problemów związanych z zablokowanymi adresami IP bądź innymi problemami technicznymi związanymi z funkcjonowaniem strony. Do Referatu ds. Bazy Wiedzy i Obsługi Zgłoszeń wpłynęło jedno zgłoszenie.

Ad 3.

Akademickie Centrum Komputerowe Cyfronet AGH od lat obsługuje platformę do składania projektów w ramach BO oraz głosowania nad projektami. Prace nad przygotowaniem platformy oraz testy trwały od połowy grudnia 2025 r. Biorąc pod uwagę duże doświadczenie operatora oraz skrupulatność w przygotowaniach z poprzednich lat, zablokowanie adresów IP nie jest odbierane jako błąd czy uchybienie w przygotowaniu narzędzia. Bezpieczeństwo danych, w tym także osobowych przechowywanych w serwisach MPI, a szczególnie w serwisie budzet.krakow.pl jest bardzo ważne, dlatego w porównaniu z poprzednimi edycjami BO, w reakcji na docierające m.in. z CERT Polska ostrzeżenia o możliwych atakach, zastosowane zostały metody filtrowania danych wysyłanych w formularzach i czasowej blokady adresów IP w przypadku wykrycia niestandardowych aktywności.

Serwisy chronione są wielopoziomym systemem bezpieczeństwa, na który składa się wiele elementów np. system anty-DDOS-owy, reguły filtrujące na routerach, wielopoziomowy firewall sieciowy, firewall aplikacyjny i inne narzędzia wykrywające podejrzane połączenia, *SQL injection*, ataki DDOS. Reguły dostępu do serwisów są na bieżąco dostosowywane do występujących zagrożeń i do aktualnych potrzeb serwisów.

Ad 4.

System jest przetestowany i przygotowany wydajnościowo do obsługi ruchu wielokrotnie wyższego niż standardowy. Od momentu uruchomienia formularzy nie doszło do żadnego przeciążenia infrastruktury i aplikacji MPI. W niektórych przypadkach wystąpienia blokad problem mógł być związany z konfiguracją mechanizmów ochronnych, które musiały być dostrojone do zwiększonego zagrożenia atakami w związku z ostrzeżeniami CERT Polska dotyczącymi planowanych i powtarzających się ataków na MPI w ciągu ostatnich 2 tygodni i obecnie. Mechanizmy ochronne dotyczą m.in. przypadków konieczności reagowania w sytuacji jednoczesnego wzrostu ruchu do serwisu, szybkiego wysyłania danych, co może być potraktowane jako automatyczne generowanie zapytań, prób ataków typu *brute force* i *SQL injection*, ataków DDOS, itp. zagrożeń. Blokady tworzone przez system WAF i firewalle są czasowe i po upływie np. godziny adres zostaje odblokowywany. Blokady czasowe są zwiększane lub zmniejszane w zależności od sytuacji. Standardowo wynoszą godzinę, ale w przypadku podwyższonego zagrożenia są zwiększane.

Uprzejmie informuję, że od 15 lutego br. znacznie wzrosła liczba prób ataków na System MPI, w tym portale krakow.pl i budzet.krakow.pl. Od początku startu Budżetu Obywatelskiego konieczne było zablokowanie ponad 7500 adresów IP, z których były zidentyfikowane ataki typu *brute force* i *SQL injection*. Ze względu na masowy charakter ataków wykraczający poza normalną aktywność klientów serwisów MPI, ataki na serwisy MPI zostały zgłoszone do CERT Polska, gdzie została przekazana lista adresów IP, z których były realizowane próby blokady serwisów i hackowania bazy danych.

Ad 5.

Zaistniała sytuacja nie została uznana za incydent. System zadziałał prawidłowo w reakcji na wykrycie podejrzanych aktywności. Takie działanie nie wymaga przedstawienia raportów technicznych. Jeżeli są sporządzane jakiegokolwiek raporty techniczne, stanowią one wewnętrzną dokumentację ACK Cyfronet.

Ad 6.

Zapewnienie bezpieczeństwa kont użytkowników oraz integralności procesu składania projektów wymaga ciągłego rozwijania i udoskonalania systemów ochronnych. Zagrożenia w cyberprzestrzeni mają charakter dynamiczny, dlatego niezbędne jest stałe aktualizowanie procedur oraz narzędzi zabezpieczających, przy jednoczesnym zachowaniu wysokiej dostępności usług dla mieszkańców.

Platforma została odpowiednio dostosowana, a wdrożone i planowane usprawnienia mają na celu zapewnienie jej stabilnego, bezpiecznego i prawidłowego działania w kolejnych edycjach Budżetu Obywatelskiego, bez nieuzasadnionego blokowania legalnej aktywności użytkowników. Za związane z tymi działaniami chwilowe utrudnienia w korzystaniu z platformy przepraszam.

Gmina Miejska Kraków dokłada wszelkich starań, aby platforma do składania projektów w ramach Budżetu Obywatelskiego działała bez zarzutów z jednoczesnym zachowaniem bezpieczeństwa użytkowników i ochrony ich danych osobowych na najwyższym poziomie. Bezpieczeństwo serwisów internetowych i danych wrażliwych przechowywanych w serwisach MPI jest bardzo ważne i wymusza konieczność stosowania narzędzi analizy aktywności użytkowników i blokady dostępu do serwisów w przypadku wykrycia podejrzanych aktywności.

z up. PREZYDENTA MIASTA

Łukasz Sęk

Zastępca Prezydenta Miasta Krakowa



Signed by / Podpisano przez:

Łukasz Bartłomiej Sęk
Gmina Miejska Kraków
- Urząd Miasta Krakowa

Date / Data: 2026-03-04 11:40

Otrzymują:

1. Adresat
2. Wydział Dialogu, Konsultacji i Kontaktu Obywatelskiego
3. Centrum Obsługi Informatycznej
4. Biuletyn Informacji Publicznej
5. Aa