

Wiadomość e-mail z 16.07.2026 r.

Interpelacja w sprawie zapewnienia bezpieczeństwa teleinformatycznego podczas planowanych testów autobusu elektrycznego marki Yutong przez MPK S.A. w Tarnowie

Sz. P.

Jakub Kwaśny

Prezydent Miasta Tarnowa

w związku z planowanym rozpoczęciem testów autobusu elektrycznego marki Yutong przez MPK S.A. w Tarnowie zwracam się z prośbą o udzielenie informacji dotyczących przygotowania tego przedsięwzięcia pod kątem bezpieczeństwa teleinformatycznego, ochrony danych oraz zabezpieczenia systemów informatycznych wykorzystywanych przez miejskiego operatora transportu.

Wiemy, że testy pojazdu miały rozpocząć się w lipcu, jednak termin ten został przesunięty. Proszę o wskazanie przyczyn zmiany harmonogramu oraz wyjaśnienie, czy było to związane z kwestiami technicznymi dotyczącymi pojazdu lub innymi okolicznościami.

Współczesne autobusy elektryczne są zaawansowanymi technologicznie pojazdami wyposażonymi w systemy elektroniczne, diagnostyczne, moduły komunikacji oraz rozwiązania umożliwiające aktualizację oprogramowania i zdalną obsługę. Z tego względu cyberbezpieczeństwo transportu publicznego staje się coraz ważniejszym elementem oceny nowych technologii.

Przykładem takiego podejścia są działania norweskiego operatora transportowego Ruter, który w 2025 roku przeprowadził szczegółowe testy bezpieczeństwa dwóch autobusów elektrycznych, w tym autobusu marki Yutong. Analiza wykazała potrzebę stosowania dodatkowych zabezpieczeń dotyczących systemów cyfrowych i komunikacji pojazdów. Jednocześnie wskazano, że wyzwania te dotyczą przede wszystkim technologii stosowanych w nowoczesnych pojazdach, a nie wyłącznie konkretnego producenta.

Podobne pytania dotyczące bezpieczeństwa cyfrowego pojawiły się również w Polsce. Po zakupie autobusów elektrycznych marki Yutong przez Warszawę zwracano uwagę na konieczność analizy potencjalnych zagrożeń związanych z zaawansowanymi systemami komunikacji i przetwarzania danych stosowanymi w tego typu pojazdach. Kwestia ta została również skierowana do analizy przez instytucje administracji państwowej odpowiedzialne za bezpieczeństwo.

W obecnej sytuacji geopolitycznej szczególnego znaczenia nabiera ochrona infrastruktury cyfrowej oraz danych. Publikacje europejskich mediów, w tym Der Spiegel oraz Le Monde, dotyczące współpracy Chin i Rosji w obszarze technologicznym pokazują, że kwestie bezpieczeństwa technologicznego wymagają szczególnej uwagi.

Tarnów jest miastem, w którym funkcjonują podmioty o istotnym znaczeniu gospodarczym i strategicznym, w tym Grupa Azoty S.A. oraz Zakłady Mechaniczne Tarnów S.A. Dlatego zasadne jest, aby również przy wdrażaniu nowych technologii w miejskich spółkach stosowane były najwyższe standardy bezpieczeństwa oraz odpowiednia analiza ryzyka.

Celem niniejszej interpelacji nie jest kwestionowanie konkretnego producenta ani technologii autobusów elektrycznych, lecz uzyskanie informacji, czy przed rozpoczęciem testów przeprowadzono

odpowiednią ocenę bezpieczeństwa oraz czy zastosowano procedury chroniące dane, systemy informatyczne i infrastrukturę MPK S.A. w Tarnowie.

Bezpieczeństwo teleinformatyczne powinno być jednym z podstawowych kryteriów oceny każdego nowoczesnego środka transportu, niezależnie od jego producenta.

W związku z powyższym zwracam się z prośbą o udzielenie odpowiedzi na następujące pytania:

1. Na jakich zasadach autobus marki Yutong został przekazany MPK S.A. w Tarnowie do testów oraz jaki jest zakres prowadzonych testów?
2. Czy przesunięcie terminu rozpoczęcia testów było związane z awarią pojazdu lub innymi problemami technicznymi?
3. Czy przed rozpoczęciem testów przeprowadzono analizę ryzyka w zakresie cyberbezpieczeństwa pojazdu, obejmującą możliwość zdalnego dostępu do systemów autobusu, diagnostyki, aktualizacji oprogramowania oraz transmisji danych?
4. Czy producent lub inne podmioty zewnętrzne posiadają możliwość zdalnego połączenia z systemami autobusu podczas jego eksploatacji w Tarnowie? Jeżeli tak, jaki jest zakres takiego dostępu i jakie zabezpieczenia zastosowano?
5. Czy autobus posiada aktywne moduły komunikacji zewnętrznej, takie jak karta SIM, modem LTE/5G lub inne rozwiązania umożliwiające transmisję danych? Jeżeli tak, jakie dane są przesyłane, gdzie są przechowywane oraz kto ma do nich dostęp?
6. Jakiego rodzaju dane będą gromadzone podczas testów, w szczególności dotyczące lokalizacji, tras przejazdu, parametrów pracy pojazdu, baterii oraz infrastruktury ładowania?
7. Czy testowany autobus będzie podłączany do systemów informatycznych MPK S.A., systemów zarządzania taboru lub innych elementów infrastruktury cyfrowej spółki? Jeżeli tak, jakie środki bezpieczeństwa zostaną zastosowane?
8. Czy przed rozpoczęciem testów konsultowano kwestie bezpieczeństwa teleinformatycznego z instytucjami odpowiedzialnymi za cyberbezpieczeństwo, w szczególności Agencją Bezpieczeństwa Wewnętrznego, NASK lub właściwymi zespołami CSIRT?
9. Czy kwestie cyberbezpieczeństwa, ochrony danych oraz odporności systemów informatycznych będą uwzględniane jako jedno z kryteriów przy podejmowaniu ewentualnej decyzji o zakupie autobusów tego producenta lub innych producentów?

Z poważaniem
Dominik Gondek
Radny Miasta Tarnowa