Minister
Infrastruktury

Znak pisma: DTK-4.054.2.2025
Warszawa, 12 maja 2025

Pan
Szymon Hołownia
Marszałek Sejmu
Rzeczypospolitej Polskiej

Szanowny Panie Marszałku,

w odpowiedzi na interpelację nr 7394 Posłanki na Sejm RP Pani Pauliny Matysiak *w sprawie cyberbezpieczeństwa i bezpieczeństwa transportu kolejowego w kontekście problemów z pociągami Impuls produkowanymi przez firmę Newag S.A.*, poniżej przedstawiam stosowne informacje w odniesieniu do pytań.

Na wstępie należy podkreślić, że sprawą wykrycia mechanizmów wywołujących awarię w systemach sterowania taborem kolejowym spółki Newag S.A. zajmuje się Prokuratura Regionalna w Krakowie, która pod sygn. 2004-1.Ds.8.2023 prowadzi postępowanie przygotowawcze w przedmiotowej sprawie. W związku z powyższym Minister Infrastruktury wstrzymuje się od udzielenia odpowiedzi na pytania zawarte w interpelacji, gdyż toczące się śledztwo i okoliczności sprawy, w tym jej poufny charakter, nie dają możliwości przedstawienia stanowiska jeszcze przed rozstrzygnięciem prowadzonej sprawy przez organy ścigania oraz odniesienia się do informacji nagłośnionych przez media. Ponadto ewentualne stanowisko Ministra Infrastruktury na obecnym etapie mogłoby zostać uznane jako wywieranie wpływu na toczące się śledztwo prowadzone przez niezależne od Ministra organy ścigania.

Natomiast z informacji przekazanych przez Ministerstwo Cyfryzacji wynika, że Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy z siedzibą w Warszawie (dalej „CSIRT NASK"), działający na podstawie ustawy o krajowym systemie cyberbezpieczeństwa (dalej „KSC"), o sprawie potencjalnych praktyk monopolistycznych firmy Newag S.A., został poinformowany przez firmę Serwis Pojazdów Szynowych sp. z o.o. 5 grudnia 2022 r., z prośbą o interwencję w sprawie złożonego dwa miesiące wcześniej zawiadomienia w Urzędzie Ochrony Konkurencji i Konsumenta (dalej „UOKiK"). Tego samego dnia Zespół CSIRT NASK wysłał zapytanie do UOKiK o poinformowaniu o podjętych krokach i ewentualnym wszczęciu postępowania. Zespół CSIRT NASK ocenił raporty techniczne zespołu Dragon Sector jako wiarygodne - ich treść była rzeczowa i spójna z przyjętą metodologią zgodną z przyjętymi w branży praktykami z zakresu informatyki śledczej oraz inżynierii wstecznej oprogramowania. Sprawa w ocenie zespołu CSIRT NASK, jako zagrożenie cyberbezpieczeństwa mogła również wypełniać znamiona przestępstwa wymagającego podjęcia czynności przez organ ścigania. W związku z tym, w celu przedstawienia wniosków z raportów, zespół CSIRT NASK 20 grudnia 2022 r. spotkał się z funkcjonariuszami Centralnego Biura

Antykorupcyjnego, a 20 stycznia 2023 r. w siedzibie NASK zorganizowano spotkanie z funkcjonariuszami Agencji Bezpieczeństwa Wewnętrznego i członkiem zespołu Dragon Sector. Z kolei 15 maja 2023 r., na wniosek Zespołu CSIRT NASK, zorganizowano w Kancelarii Prezesa Rady Ministrów spotkanie Kolegium ds. Cyberbezpieczeństwa z udziałem przedstawicieli najważniejszych organów odpowiedzialnych za cyberbezpieczeństwo w celu zaprezentowania raportów przez członka zespołu Dragon Sector. Spotkanie miało charakter niejawny. Na dalszym etapie czynności w tej sprawie prowadziła Agencja Bezpieczeństwa Wewnętrznego, zgodnie ze swoimi ustawowymi kompetencjami. Obecnie postępowanie w sprawie prowadzi Prokuratura Regionalna w Krakowie.

Ministerstwo Cyfryzacji w procedowanym projekcie nowelizacji ustawy o KSC, która ma na celu wdrożenie w Polsce m.in. dyrektywy NIS 2, przewiduje także uwzględnienie mechanizmu umożliwiającego wykluczenie dostawców wysokiego ryzyka (HRV), co stanowić będzie implementację Toolbox 5G. Instytucja dostawcy wysokiego ryzyka ma za zadanie eliminować z użycia niebezpieczny sprzęt i usługi z kluczowych dla funkcjonowania państwa systemów. Obecnie nie istnieją środki prawne umożliwiające nakazanie wycofywania tego rodzaju rozwiązań. Mechanizm HRV będzie mieć istotny wpływ na bezpieczeństwo państwa oraz jego instytucji i newralgicznej infrastruktury. Ustawa określi proces umożliwiający wykluczenie danego typu sprzętu w przypadku zidentyfikowania, że stanowi zagrożenie dla bezpieczeństwa narodowego. Aby procedura taka została uruchomiona muszą wystąpić realne i potwierdzone przesłanki. Taki proces obejmować będzie zarówno szczebel techniczno-merytoryczny (badania przez zespoły CSIRT), jak i strategiczny (Kolegium ds. Cyberbezpieczeństwa, w którym zasiadają najważniejsi dla bezpieczeństwa państwa ministrowie oraz szefowie służb). Dodatkowo przewidziano możliwość weryfikacji decyzji przez właściwy sąd. W procesie tym opcjonalnie będą mogły także uczestniczyć organizacje społeczne i UOKiK. Podjęta decyzja będzie uwzględniać zarówno przesłanki w zakresie ryzyka stworzenia zagrożeń w wymiarze ekonomicznym czy terrorystycznym, jak i techniczne, takie jak liczba i rodzaj wykrytych podatności oraz incydentów, tryb i zakres w jakim dostawca sprawuje nadzór nad procesem wytwarzania i dostarczania sprzętu lub oprogramowania, posiadanie przez dostawcę certyfikatów.

Przy nowelizacji tej ustawy planowane jest także wprowadzanie do porządku prawnego instytucji polecenia zabezpieczającego. Polecenie to będzie mogło być wydane przez ministra właściwego do spraw informatyzacji w przypadku wystąpienia incydentu krytycznego, w celu skoordynowania efektywnej reakcji na ten incydent. Przed wydaniem polecenia zabezpieczającego niezbędne będzie przeprowadzenie analizy uzasadniającej wydanie tych środków nadzwyczajnych. Będzie ona przeprowadzana wspólnie z Zespołem do spraw incydentów krytycznych. Następnie minister właściwy do spraw informatyzacji będzie mógł wydać w drodze decyzji administracyjnej polecenie zabezpieczające odnoszące się do incydentu krytycznego. Będzie w nim zawarte wskazanie określonego zachowania, które zmniejszy skutki incydentu lub zapobiegnie jego rozprzestrzenianiu się. Wprowadzenie do polskiego porządku prawnego polecenia zabezpieczającego (z rygorem natychmiastowej wykonalności) jest konieczne dla zapewnienia bezpieczeństwa narodowego w obliczu coraz częstszych i poważniejszych cyberataków. W obecnym stanie prawnym Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa może wydawać rekomendacje dotyczące stosowania urządzeń informatycznych lub oprogramowania.

Przy nowelizacji ustawy planowane jest wzmocnienie mechanizmu rekomendacji. Warto także podkreślić, że projektowane przepisy przewidują również sformalizowanie na poziomie ustawowy funkcjonowania Połączonego Centrum Operacyjnego Cyberbezpieczenstwa (dalej „PCOC"). Działanie PCOC umożliwia szybką wymianę informacji, co pozwala podnieść poziom cyberbezpieczeństwa w kraju, w szczególności w zakresie reagowania na pojawiające się incydenty cyberbezpieczeństwa. W spotkaniach PCOC uczestniczą CSIRT-y poziomu krajowego oraz inne podmioty kluczowe dla bezpieczeństwa państwa. W związku z tym bieżąca koordynacja oraz zarządzanie incydentami cyberbezpieczeństwa o charakterze i skali mającej potencjalny wpływ na funkcjonowanie państwa odbywa się - na poziomie operacyjnym w ramach spotkań PCOC. Natomiast w przypadku poziomu strategicznego - podczas posiedzeń Kolegium ds. Cyberbezpieczeństwa.

Z wyrazami szacunku,

Dokument podpisany elektronicznie przez:

z upoważnienia Ministra Infrastruktury
Piotr Malepszak
Podsekretarz Stanu