Minister
Infrastruktury

Znak pisma: DTK-4.054.1.2025
Warszawa, 10 kwietnia 2025

Pan
Szymon Hołownia
Marszałek Sejmu
Rzeczypospolitej Polskiej

Szanowny Panie Marszałku,

w odpowiedzi na interpelację nr 7393 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.

Uprzejmie informuję, że kwestie poruszone w przedmiotowej interpelacji w dużej części pokrywają się z zakresem pytań zawartych w interpelacji 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.*, na którą została przygotowana odpowiedź.

Ministerstwo Infrastruktury realizuje zadania organu właściwego ds. cyberbezpieczeństwa zgodnie z art. 42 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (dalej „ustawa o KSC"), w szczególności w zakresie postępowań o uznanie podmiotów za operatorów usług kluczowych oraz monitorowania stosowania przepisów przez uznane podmioty. Ministerstwo utrzymuje także stałą współpracę z Ministerstwem Cyfryzacji, w szczególności w zakresie realizacji zadań wynikających z ustawy o KSC.

Podmioty kwalifikujące się do uznania za operatora usługi kluczowej określa rozporządzenie wykonawcze do ustawy o KSC - rozporządzenie Rady Ministrów z dnia 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych (Dz. U. z 2018 poz. 1806).W przypadku Newag S.A. nie została wydana przez Ministra Infrastruktury decyzja administracyjna o uznaniu tego podmiotu za operatora usługi kluczowej.

W przedmiotowej sprawie działania związane z weryfikacją przyczyn i następstw analizy przeprowadzonej przez grupę Dragon Sector w odniesieniu do Spółki Newag S.A. były podejmowane przez różne instytucje na wielu szczeblach – zgodnie ze swoją, określoną przepisami ustawy o KSC, rolą.

Z informacji przekazanych przez Przewoźników wynika, że przy dostawie pojazdów, tabor kolejowy jest weryfikowany przez końcowego użytkownika zgodnie z zapisami zawartych umów. O tym jakie czynności są podejmowane przez upoważnionego komisarza odbiorczego ze strony przyszłego użytkownika decydują zapisy tych umów. Sprawdzenie pojazdów kolejowych i ich elementów, zarówno tych nowo produkowanych, jak i tych po realizacji czynności utrzymaniowych realizowane jest zgodnie z wymaganiami stawianymi w dokumentacji technicznej pojazdu, w szczególności Warunkach Technicznych Wykonania i Odbioru, Dokumentacji Sytemu Utrzymania oraz Dokumentacji Techniczno-Ruchowej. Kolejnym etapem weryfikacji pojazdu są odbiory techniczne, w trakcie których weryfikowana jest zgodność pojazdu z wymaganiami określonymi w specyfikacji zamówienia. Jednocześnie należy podkreślić, że zarówno w trakcie odbiorów etapowych jak i technicznych kontroli podlegają funkcje i osiągi poszczególnych systemów sterowanych przez oprogramowanie wytworzone zarówno przez dostawców poszczególnych systemów jak i producenta pojazdu, nie zaś kod źródłowy tego oprogramowania. Oprogramowanie wytworzone przez poszczególnych producentów stanowi ich „know-how", stąd nie jest ono powszechnie udostępniane. Należy zatem zaakcentować fakt, że zamawiający w trakcie odbiorów pojazdów nie mają fizycznej możliwości weryfikacji czy dane oprogramowanie nie posiada dodatkowych funkcji, które nie są bezpośrednio związane z jego przeznaczeniem i funkcjami, które musi spełnić by dany system czy układ w pojeździe działał prawidłowo. Zamawiający może prowadzić zestawienie i weryfikować wersje oprogramowania w poszczególnych systemach, które udostępniają taką informację i na podstawie tego sprawdzać czy nie uległa zmianie wersja danego oprogramowania. Zamawiający nie ma jednak technicznej możliwości weryfikacji czy wewnątrz danej wersji oprogramowania nie ma zaszytych niepożądanych funkcji.

Należy zwrócić uwagę, że problem użytkowników pojazdów związany był z brakiem szczegółowych przepisów odnoszących się do dokumentacji przetargowej w zakresie licencji na oprogramowanie główne sterujące pojazdem w postępowaniach na dostawę pojazdów, które zostały ogłoszone do 2020 roku. Dotyczy to zwłaszcza przepisów dotyczących uzyskiwania dostępu, modyfikacji i dokonywania eksportu danych. W przedmiotowym postępowaniu, działania użytkowników zostały ograniczone do mało precyzyjnie określonych pól eksploatacji licencji określonej w umowach.

Mając na uwadze obecne realia dotyczące cyberbezpieczeństwa i bieżących problemów użytkowników związanych z zabezpieczeniem pojazdów przed ingerencją osób nieuprawnionych do oprogramowania głównego sterującego pojazdem, obecnie większość przewoźników ma wpływ na kształtowanie postanowień zawartych w dokumentacji opisu przedmiotu zamówienia w zakresie weryfikacji i odbioru końcowego oprogramowania przy dostawie pojazdów na etapie postępowania ogłoszonego w 2024 roku. Z punktu widzenia Spółek, konieczne było zawarcie precyzyjnych postanowień odnoszących się zarówno do odbioru samego oprogramowania pod kątem technicznym i funkcjonalnym, jak i również przekazania stosownej dokumentacji i zabezpieczeń, gwarantujących wysoki poziom bezpieczeństwa eksploatowanych pojazdów kolejowych, zapobiegania sabotażom oraz zabezpieczeniem

przed nieautoryzowanym dostępem do oprogramowania głównego sterującego pojazdem.

Spółki jako podmioty odpowiedzialne za utrzymanie (ECM), w tym podmioty odpowiedzialne za zarządzanie konfiguracją eksploatowanych pojazdów, w celu monitorowania zagrożeń związanych z funkcjonowaniem mechanizmów ograniczających dostęp do oprogramowania głównego sterującego pojazdem, wdrożyły odpowiednie regulacje odnoszące się do kontroli i weryfikacji oprogramowania, mając przede wszystkim na uwadze dostęp podmiotów zewnętrznych, którym został zlecony proces przeglądowo – naprawczy zgodnie z zawartymi umowami. Wszelkie zmiany w oprogramowaniu poddawane są procesowi oceny znaczenia zmiany zgodnie z Rozporządzeniem Wykonawczym Komisji (UE) NR 402/2013 z dnia 30 kwietnia 2013 r. w sprawie wspólnej metody oceny bezpieczeństwa w zakresie wyceny i oceny ryzyka i uchylające rozporządzenie (WE) nr 352/2009 (Dz. Urz. UE L 121 z 3 maja 2013, str. 8, z późn. zm.). Wprowadzenie zmian w oprogramowaniu głównym sterującym pojazdem przez podmiot zewnętrzny świadczący usługi w zakresie utrzymania bez uzyskania zgody użytkownika traktowane jest jako działanie nieuprawnione.

Prezes Urzędu Transportu Kolejowego (dalej „UTK") jako krajowa władza bezpieczeństwa jest właściwy m.in. w sprawach nadzoru technicznego nad eksploatacją i utrzymaniem infrastruktury kolejowej oraz pojazdów kolejowych, a także bezpieczeństwa ruchu kolejowego. W obszarze cyberbezpieczeństwa Prezes UTK może działać tylko pośrednio, biorąc pod uwagę kompetencje wynikające z ustawy o transporcie kolejowym czy z przepisów unijnych w zakresie interoperacyjności i bezpieczeństwa.

Zgodnie z przeprowadzonymi przez Prezesa UTK w latach 2023-2024 konsultacjami z przedstawicielami Agencji Kolejowej Unii Europejskiej (dalej „ERA") i Komisji Europejskiej (dalej „KE") w sprawie bezpieczeństwa IT w przemyśle kolejowym, wskazuje się na zależność między bezpieczeństwem IT a bezpieczeństwem funkcjonalnym, ponieważ cyberzagrożenia mogą wpływać na możliwość realizacji funkcji istotnych dla bezpieczeństwa. Jednakże dyrektywa w sprawie interoperacyjności i techniczne specyfikacje interoperacyjności (TSI), nie regulują sposobu zapewnienia bezpieczeństwa IT. Z informacji przekazanych przez ERA oraz KE wynika, że brak regulacji w tym zakresie jest obecnie przedmiotem dyskusji z Europejską Agencją ds. Cyberbezpieczeństwa (ENISA). Instytucje te pracują nad ustaleniem niezbędnego zakresu doprecyzowania wymagań odnośnie oprogramowania w TSI dotyczącego podsystemu Tabor.

Na tym polu Prezes UTK ściśle współpracuje z odpowiednimi służbami i instytucjami odpowiadającymi w Polsce za kwestie cyberbezpieczeństwa m.in. uczestnicząc w Kolegium ds. Cyberbezpieczeństwa pod przewodnictwem Prezesa Rady Ministrów. Prezes UTK już w 2023 r. podjął działania informacyjne w zakresie cyberzagrożeń, których efektem były m.in.:

- zalecenia dotyczące zarządzania aktywami informatycznymi pod kątem cyberbezpieczeństwa, opublikowane na stronie UTK w dniu 6 kwietnia 2023 r.;
- rekomendacje Prezesa UTK w zakresie cyberbezpieczeństwa, opublikowane w magazynie „Rynek Kolejowy" nr 04/2023 oraz na stronie UTK w dniu 12 czerwca 2023 r.;
- opublikowanie na stronie UTK w dniu 11 października 2023 r. wytycznych ISAC-Kolej związanych z cyberbezpieczeństwem taboru pasażerskiego.

Należy wskazać, że na etapie wydawania przez Prezesa UTK zezwolenia na wprowadzenie do obrotu pojazdu kolejowego, przepisy TSI obligują do weryfikacji spełniania zasadniczych wymagań interoperacyjności w odniesieniu do oprogramowania związanego z podsystemem Sterowanie – urządzenia pokładowe, czyli tych aplikacji, które służą zapewnieniu bezpieczeństwa ruchu kolejowego (np. oprogramowanie Europejskiego Systemu Sterowania Pociągiem („ETCS")). Natomiast w odniesieniu do oprogramowania w podsystemie Tabor, czyli aplikacji służących do sterowania podzespołami pojazdu, np. układem hamulcowym, drzwiami, klimatyzacją, etc. (dalej „TCMS") wymogi ograniczają się tylko do wykazania bezpiecznej integracji. TCMS nie podlega weryfikacji pod kątem zastosowanych zabezpieczeń przed cyberzagrożeniami. Oprogramowanie jest elementem zarówno podsystemu Sterowanie – urządzenia pokładowe, jak i podsystemu Tabor. Zmianami w oprogramowaniu należy zarządzać na ogólnych zasadach, obowiązujących w przypadku każdej zmiany w tych podsystemach. Zasady te wynikają z dwóch aktów prawnych tj. z:

- rozporządzenia wykonawczego Komisji (UE) nr 402/2013 z dnia 30 kwietnia 2013 r. w sprawie wspólnej metody oceny bezpieczeństwa w zakresie wyceny i oceny ryzyka i uchylające rozporządzenie (WE) nr 352/2009 (Dz. Urz. UE L 121 z 3 maja 2013 r., str. 8-25);
- rozporządzenia wykonawczego Komisji (UE) 2018/545 z dnia 4 kwietnia 2018 r. ustanawiające uzgodnienia praktyczne na potrzeby procesu udzielania zezwoleń dla pojazdów kolejowych i zezwoleń dla typu pojazdu kolejowego zgodnie z dyrektywą Parlamentu Europejskiego i Rady (UE) 2016/797 (Dz. Urz. UE L 90 z 6 kwietnia 2018 r., str. 66–104).

Każde z tych rozporządzeń ustanawia określony proces zarządzania zmianą, który można określić mianem bezpiecznej integracji. Rozporządzenie 402/2013 reguluje proces zarządzania ryzykiem zmian, natomiast rozporządzenie 545/2018 odnosi się do zarządzania konfiguracją pojazdu. Pierwszy ma na celu zapewnienie, że zmiany wprowadzane w pojazdach są bezpieczne (nie powodują niedopuszczalnego ryzyka), natomiast drugi ma na celu zapewnienie, że realizowane są właściwe obowiązki związane z oceną zgodności i homologacją. Procesy te są ze sobą powiązane w ten sposób, że ocena zgodności w odniesieniu do wymagania zasadniczego (tj. bezpieczeństwa), musi uwzględniać wyniki zarządzania ryzykiem zmian.

Nad prawidłową realizacją tych procesów nadzór sprawuje Prezes UTK, stąd obszar kontroli w przedmiotowej sprawie obejmował: nadzór nad pojazdami kolejowymi, ze szczególnym uwzględnieniem zarządzania zmianą i zarządzania konfiguracją pojazdu oraz nadzór nad przeprowadzaniem czynności utrzymania pojazdów kolejowych.

Najważniejsze ustalenia wynikające z przeprowadzonych kontroli u przewoźników będących dysponentami pojazdów kolejowych serii Impuls oraz w Newag S.A. były następujące:

- proces zarządzania konfiguracją pojazdów kolejowych nie został uregulowany w procedurach systemu zarządzania bezpieczeństwem/utrzymaniem;
- podmioty nie posiadały informacji o aktualnej wersji oprogramowania TCSM zainstalowanego na pojeździe kolejowym;

- podmioty nie prowadziły rejestru zmian w konfiguracji pojazdów, w tym konfiguracji oprogramowania;
- zabrakło właściwej współpracy przewoźników z producentem pojazdów w zakresie ustalenia elementów krytycznych dla bezpieczeństwa;
- zabrakło przeprowadzenia weryfikacji metodyki wyznaczania elementów krytycznych.

W wyniku stwierdzonych nieprawidłowości, podmioty kontrolowane podjęły i wdrożyły w swoich organizacjach działania pokontrolne, w tym m.in.:

- zaktualizowały procedury wewnętrzne o proces zarządzania konfiguracją oraz w zakresie zarządzania elementami krytycznymi;
- dokonały weryfikacji oprogramowania poprzez wystąpienie do producentów pojazdów kolejowych o informacje dotyczące oprogramowania;
- uregulowały zasady gromadzenia informacji o oprogramowaniach i zmianach w oprogramowaniu pojazdów kolejowych;
- zweryfikowały metodykę wyznaczania elementów krytycznych dla bezpieczeństwa;
- określiły obowiązki dostawcy oprogramowania w przypadku potrzeby wprowadzenia zmiany.

Reasumując, Minister Infrastruktury z dużą uwagą podchodzi do wszelkich spraw związanych z bezpieczeństwem w ruchu kolejowym, również w obszarze zagrożeń wywołanych przez awarie w systemach sterowania taborem kolejowym. Współpracując z innymi organami państwowymi i instytucjami podległymi wszelkie przypadki potencjalnych zagrożeń dla infrastruktury krytycznej państwa są analizowane w pracach nad zwiększeniem bezpieczeństwa w transporcie kolejowym.

Z wyrazami szacunku,

Dokument podpisany elektronicznie przez:
z upoważnienia Ministra Infrastruktury
Piotr Malepszak
Podsekretarz Stanu