MINISTER INFRASTRUKTURY

Warszawa, dnia 04 maja 2022 r.

Znak sprawy: DTK-4.054.7.2022.MS.1

Pan
Tomasz Grodzki
Marszałek Senatu
Rzeczypospolitej Polskiej

Szanowny Panie Marszałku,

w odpowiedzi na oświadczenie złożone przez sanatora Stanisława Lamczyka podczas 38. posiedzenia Senatu Rzeczypospolitej Polskiej w dniu 17 marca 2022 r. przedstawiam poniższe informacje.

Z informacji otrzymanych od producenta systemu, tj. firmy Alstom wynika, że przyczyną awarii w dniu 17 marca 2022 r. nie były ataki hakerskie, tylko błąd systemowy związany z formatowaniem zegara czasu w systemie sterowania ruchem kolejowym, który wpłynął na dostępność sieci kolejowej i w rezultacie na transport kolejowy w Polsce. Należy podkreślić, że bezpieczeństwo pasażerów nie było i nie jest zagrożone. Komputerowe systemy sterowania ruchem kolejowym są systemami zamkniętymi i nie ma do nich dostępu z poziomu sieci internetowej. Pracują one w sieciach zamkniętych zgodnie z definicją normy PN-EN 50159 (Zastosowania kolejowe - Systemy łączności, sterowania ruchem i przetwarzania danych - Łączność bezpieczna w systemach transmisyjnych). Sprzęt komputerowy systemu sterowania ruchem kolejowym zainstalowany jest w zamkniętych i zaplombowanych serwerowniach, a dostęp do tych pomieszczeń jest ograniczony do grona uprawnionych osób i obwarowany procedurami kontroli dostępu. Komputery systemów nadrzędnych (pulpitów nastawczych) zainstalowane są na nastawniach i znajdują się pod stałym nadzorem dyżurnych ruchu.

Niezależnie od powyższego informuję, że PKP Polskie Linie Kolejowe S.A w zakresie cyberbezpieczeństwa podejmuje następujące działania:

- prowadzi szacowania ryzyka wystąpienia incydentu oraz zarządza tym ryzykiem;
- wdraża odpowiednie i proporcjonalne do oszacowanego ryzyka środki bezpieczeństwa (organizacyjne, techniczne, osobowe, fizyczne, proceduralne), w tym m.in. wdraża środki kontroli bezpieczeństwa (systemy klasy AV/IS, Firewall, IDS/IPS, UTM, DLP, SIEM/SOAR, EDR, PAM, IAM/IDM), WCF, MDM);
- wdraża polityki i procedury związane z zapewnieniem bezpieczeństwa informacji i ciągłości działania;
- monitoruje usługi IT w trybie ciągłym w ramach zawartej umowy na świadczenie usług w zakresie Operacyjnego Centrum Cyberbezpieczeństwa (usługi „SOC" w trybie 24h);
- zbiera informacje o zagrożeniach cyberbezpieczeństwa i podatnościach oraz niezwłocznie podejmuje działania po ich stwierdzeniu;
- zarządza incydentami bezpieczeństwa;

- raportuje incydenty do Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV oraz współpracuje z tym podmiotem w zakresie obsługi incydentu;
- przeprowadza audyty i oceny bezpieczeństwa teleinformatycznego.

Niezależnie od powyższego, w związku z informacjami zawartymi w przedmiotowym oświadczeniu Pana Senatora kwestionującymi ustalenia producenta urządzeń zamontowanych na Lokalnych Centrach Sterowania i sugerującymi inną przyczynę zaistniałej awarii, informuję, że wystąpiłem do Agencji Bezpieczeństwa Wewnętrznego z prośbą o zbadanie sprawy pod wskazanej przez Pana Senatora możliwości ingerencji osób trzecich.

Łączę wyrazy szacunku,

Dokument podpisany elektronicznie przez:

z upoważnienia Ministra Infrastruktury

Andrzej Bittel

Sekretarz Stanu