Cyberbezpieczeństwo kluczowe dla bezpiecznej kolei

12.06.2023

Na przestrzeni ostatnich lat polska kolej przeszła rewolucję w wielu obszarach jej funkcjonowania. Pozwoliło to odwrócić trend spadku liczby pasażerów, a także podnieść poziom bezpieczeństwa. Od początku tego procesu kluczowy był rozwój nowoczesnych technologii cyfrowych, dzięki którym wiele działań na kolei zostało znacznie uproszczonych i przyspieszonych. Niestety w ślad za rozwojem cyfryzacji, rośnie ryzyko poważnych incydentów wynikających z ataków hakerskich, które mogą mieć bezpośredni wpływ na bezpieczeństwo kolei i pasażerów. Dlatego niezwykle istotne jest, aby równolegle do informatyzacji kolei rozwijane były metody jej zabezpieczenia.

Postępująca cyfryzacja odgrywa ogromną rolę w podnoszeniu poziomu bezpieczeństwa transportu kolejowego w Polsce. Szczególne znaczenie ma to w obszarze zarządzania ruchem kolejowym, handlowym, a także prowadzenia i utrzymania pojazdów kolejowych. Możliwość cyfrowej diagnozy stanu infrastruktury, pojazdów, elektroniczna sprzedaż biletów oraz nowoczesne systemy sterowania ruchem kolejowym sprawiły, że obecna kolej jest bardziej bezpieczna, szybsza, komfortowa i dostępna. Codziennością stały się systemy zarządzania pojazdami kolejowymi, które umożliwiają śledzenie na bieżąco nie tylko przebiegu pociągu, ale przede wszystkim aktualnego

stanu technicznego, rozpoznanie awarii czy łączność z obsługą. Trzeba jednak pamiętać, że rozwój cyfryzacji to także nowe zagrożenia w zakresie bezpieczeństwa kolei, która w coraz większym stopniu funkcjonuje w formule on-line. Wyzwaniem w tej dziedzinie jest zatem nie tylko dostosowanie prawa do nowych rozwiązań IT, ale przede wszystkim właściwe zarządzanie oprogramowaniem i przestrzeganie przepisów w tym zakresie.

O tym, jak realne jest zagrożenie w transporcie kolejowym w zakresie usług cyfrowych, kolej w Europie przekonała się już niejednokrotnie. Pomimo obowiązujących przepisów nakładających na uczestników rynku kolejowego określone przez rozporządzenia i opisy standardów wymagania, ryzyko jest realne.

W 2020 roku brytyjska kolej musiała zmierzyć się z wyciekiem danych blisko 10 tys. osób, które korzystały z bezpłatnego internetu WiFi na stacjach kolejowych. Dane te zostały opublikowane w sieci, a całość zawierała ok. 146 mln rekordów wraz z danymi kontaktowymi czy datami urodzeń. W tym samym roku cyberprzestępcy wykradli wrażliwe dane oraz dokumenty objęte tajemnicą szwajcarskiego producenta taboru kolejowego. Dane te zostały upublicznione. Również w 2020 r. hiszpański zarządca infrastruktury kolejowej padł ofiarą ataku hakerskiego, w wyniku którego narażone zostały dane osobowe i handlowe, ale atak nie wpłynął na infrastrukturę krytyczną.

Jeden z poważniejszych incydentów miał miejsce w 2017 r. w Szwecji. Doszło wówczas do ataków DoS oraz DDoS na szwedzki organ ds. bezpieczeństwa w transporcie. Ruch pociągów był prowadzony manualnie. Zaatakowane zostały systemy poczty elektronicznej czy śledzenia pociągów. Niedostępne były systemy rezerwacyjne oraz informacja o utrudnieniach w ruchu pociągów. Także w 2017 r. koleje niemieckie padły ofiarą ataku hakerskiego, w wyniku którego przestała działać część urządzeń systemu informacji pasażerskiej. Rok później duński przewoźnik DSB musiał zmierzyć się z atakiem na system sprzedaży biletów, w wyniku którego nie było możliwości zakupu biletów m.in. w biletomatach, on-line i w niektórych kasach

biletowych[1].

Wskazane przypadki działań wymierzonych w branżę kolejową pokazują, jak poważne zagrożenie stanowią nieodpowiednie zabezpieczenia systemów teleinformatycznych. Zagrożenia związane z cyberbezpieczeństwem na przestrzeni ostatnich lat stają się coraz bardziej realne – także w branży kolejowej. Stopień informatyzacji w pojazdach kolejowych jest już na tyle wysoki, iż ewentualne usterki lub awarie mogą doprowadzić do nieakceptowalnych skutków.

ZADBAĆ O WYSOKIE STANDARDY

Dlatego tak ważne jest zarządzanie oprogramowaniem zgodnie z zapisami TSI CCS oraz Listy Prezesa UTK. Obydwa dokumenty wskazują normę EN 50128:2011 - „Zastosowania kolejowe – Systemy łączności, przetwarzania danych i sterowania ruchem – Oprogramowanie kolejowych systemów sterowania i zabezpieczenia" - jako obowiązującą w tym zakresie.

Norma EN 50128:2011 określa zestaw wymagań dotyczących rozwoju, wdrażania i konserwacji dowolnego mającego wpływ na bezpieczeństwo oprogramowania stosowanego w kolejowych systemach sterowania i ochrony. Obejmuje swoim zakresem systemy operacyjne, narzędzia wsparcia, oprogramowanie sprzętowe, jak również programowanie aplikacji. Ponadto norma określa wymagania dotyczące struktury organizacyjnej, relacji między organizacjami i podziału odpowiedzialności. Wskazuje również kryteria dotyczące kwalifikacji i wiedzy specjalistycznej personelu.

Kluczową koncepcją normy są poziomy nienaruszalności bezpieczeństwa oprogramowania. Zdefiniowano pięć poziomów nienaruszalności bezpieczeństwa oprogramowania, gdzie 0 jest najniższym, a 4 najwyższym. Im większe ryzyko wynikające z awarii oprogramowania, tym wyższy będzie poziom nienaruszalności. Stosowanie tej metody pozwala skutecznie zarządzać ryzykiem i utrzymywać go na odpowiednim poziomie.

Choć nie ma możliwości zagwarantowania całkowitej

bezawaryjności oprogramowania związanego z bezpieczeństwem kolei, przestrzeganie przepisów minimalizuje ryzyko zagrożeń i pozwala czerpać w pełni z korzyści związanych z informatyzacją. Stosowanie normy EN 50128:2011 oraz pozostałych norm wyszczególnionych w technicznych specyfikacjach interoperacyjności oraz Liście Prezesa UTK jest obowiązkowe w celu zapewnienia integralności oprogramowania służącego funkcjom bezpieczeństwa.

Zmiany wprowadzane w oprogramowaniu pojazdów kolejowych podlegają procesowi zarządzania zmianą zgodnie z obowiązującymi przepisami rozporządzenia wykonawczego Komisji (UE) 2018/545. Wytyczne w zakresie zarządzania zmianami na pojazdach kolejowych dostępne są na stronie internetowej UTK.

REKOMENDACJE PREZESA UTK

Prezes UTK rekomenduje, aby każdy podmiot eksploatujący pojazdy kolejowe wyposażone w informatyczne systemy pokładowe przeprowadził inwentaryzację aktywów informatycznych i odpowiednio nimi zarządził pod kątem bezpieczeństwa w całym cyklu życia pojazdu.

W szczególności Prezes UTK rekomenduje wszystkim przewoźnikom kolejowym:

- przeprowadzić przegląd zabezpieczeń ewentualnych dostępów zdalnych oraz bezpośrednich interfejsów komunikacyjnych z systemami pokładowymi pojazdów kolejowych, w szczególności należy zwrócić uwagę na modemy komórkowe i metody zdalnego dostępu serwisu,
- na bazie inwentaryzacji oraz przeglądu należy przeprowadzić odpowiednią analizę ryzyka uwzględniającą zagrożenia związane z przestrzenią cyberbezpieczeństwa pojazdów kolejowych w całym cyklu życia pojazd kolejowego,
- należy ograniczyć bezpośrednio dostępne usługi pozwalające na zdalny dostęp tylko do właściwie

zidentyfikowanych, zabezpieczonych, nadzorowanych i akceptowalnych przypadków,

- tam gdzie dostęp zdalny jest niezbędny należy właściwie go zabezpieczyć minimalnie z wykorzystaniem prywatnych APN (Access Point Name), połączeń VPN (Virtual Private Network) i zastosowaniu wieloskładnikowego uwierzytelniania. Należy rozważyć wdrożenie zapór sieciowych klasy UTM (Unified Threat Management),
- tam gdzie to jest możliwe należy ograniczyć dostęp przez VPN wyłącznie do znanych adresów IP i połączeń z terenu Polski lub innych akceptowalnych krajów (jeżeli serwis jest położony poza terenem kraju),
- należy wprowadzić segmentacje i mikro segmentacje systemów, w szczególności zapewnić separację systemów dostępnych dla pasażerów od systemów OT (Operational Technology) oraz wdrożyć ścisłe monitorowanie i kontrolowanie przepływów pomiędzy tymi systemami,
- stosowanie silnych, co najmniej 12 znakowych haseł (o ile to możliwe) i upewnienie się, że do jakichkolwiek urządzeń pokładowych nie są stosowane domyślne hasła producentów i dostawców,
- w odniesieniu do dostępu fizycznego do interfejsów urządzeń pokładowych przewoźnicy kolejowi powinni opracować procedury zarządzania takim dostępem, weryfikacji personelu serwisowego i bezpieczeństwa urządzeń podłączanych do systemów pokładowych pojazdów kolejowych,
- tam gdzie to możliwe po przeprowadzeniu procedury zarządzania zmianą stosować aktualizacje oprogramowania urządzeń pokładowych,
- regularne i właściwe zarządzanie podatnościami zinwentaryzowanych aktywów informatycznych. Informacje o podatnościach urządzeń oraz systemów informatycznych publikowane są w powszechnie dostępnych bazach danych.

ODPOWIEDNIA WYMIANA INFORMACJI

Jednym z największych wyzwań, obok skutecznych regulacji prawnych oraz narzędzi teleinformatycznych, jest wymiana informacji pomiędzy podmiotami zobowiązanymi do podejmowania działań minimalizujących cyberzagrożenie. Bieżąca informacja jest kluczowa z punktu widzenia zapewnienia bezpieczeństwa cyfrowego kolei. Aby ułatwić wymianę informacji i doświadczeń dotyczących cyberbezpieczeństwa w sektorze kolejowym w Polsce, w 2020 r. powołano Centrum Wymiany i Analiz Informacji podsektora transportu kolejowego (ISAC-Kolej), do którego mogą dołączyć wszyscy zarządcy infrastruktury i przewoźnicy kolejowi. Centrum ISAC-Kolej (z ang. ISAC – Information Sharing and Analysis Center) powstało w wyniku porozumienia spółek kolejowych, Instytutu Kolejnictwa oraz NASK – Państwowego Instytutu Badawczego. Inicjatywa przyczynia się również do podniesienia odporności na cyberzagrożenia systemów teleinformatycznych wykorzystywanych przez transport kolejowy.

W Centrum Wymiany i Analizy Informacji ISAC-Kolej opracowano wytyczne dotyczące cyberbezpieczeństwa dla pracowników kolei. Opracowanie powstało na podstawie udostępnionego przez Komisję Europejską dokumentu „Transport cybersecurity toolkit”. Wytyczne dostępne są w najnowszym wydaniu „Problemów Kolejnictwa”.

Mając na uwadze sprawną obsługę incydentów Prezes UTK zaleca zgłoszenie osoby kontaktowej do CSIRT (Computer Security Incident Response Team) NASK, który jest właściwy w sprawach incydentów cyberbezpieczeństwa w sektorze kolejowym. Równocześnie rekomenduje się udział w ISAC-Kolej (information sharing and analysis centre), które stanowi centrum

Nowoczesne i innowacyjne rozwiązania w obszarze cyfryzacji znajdują swoje szerokie zastosowanie zarówno we wsparciu działalności przedsiębiorstw współtworzących system kolei, jak i w zakresie wspierania prowadzenia ruchu i nadzoru jej

eksploatacji. Obecnie kolej to pewnego rodzaju system naczyń połączonych, dlatego każdy z jej uczestników powinien dołożyć wszelkich starań, aby ustrzec się przed cyberprzestępcami. Skuteczny atak na jeden podmiot może mieć wpływ na działalność całej branży. Jak pokazują przytoczone incydenty, brak odpowiednich zabezpieczeń IT może mieć negatywne skutki nie tylko dla pasażerów lub producentów pojazdów kolejowych, ale również na bezpieczeństwo transportu kolejowego. Z tego względu wprowadzenie wszystkich możliwych i aktualnie dostępnych zabezpieczeń IT powinno być traktowane priorytetowo.

---

[1] Przykłady naruszeń cyberbezpieczeństwa można znaleźć w artykule Marka Pawlika „Wytyczne dotyczące cyberbezpieczeństwa dla pracowników podmiotów kolejowych” opublikowanym w „Problemach Kolejnictwa”, zeszyt 191.

Artykuł autorstwa dr. inż. Ignacego Góry ukazał się w magazynie "Rynek Kolejowy" nr 04/2023