Cyberbezpieczeństwo w transporcie szynowym – wyzwania i rozwiązania, w tym podsumowanie konferencji IT/OT w Transporcie Szynowym

Cybersecurity in rail transport – challenges and solutions, including a summary of the IT/OT conference in rail transport

Marek Pawlik

Dr hab. inż., prof. IK

zast. dyr. Instytutu Kolejnictwa, przewod. ISAC-Kolej, członek Komitetu Naukowego Konferencji IT/OT w Transporcie Szynowym

mpawlik@ikolej.pl

Streszczenie: Artykuł przedstawia wyzwania i rozwiązania w zakresie cyberbezpieczeństwa transportu szynowego bazując na prezentacjach i dyskusjach jakie miały miejsce podczas Konferencji Naukowo-Technicznej IT/OT w Transporcie Szynowym 2023, która miała miejsce w dniach 29-31 stycznia 2024 r. Tak jak podczas konferencji artykuł rozpoczyna się od przedstawienia wyzwania z lotu ptaka, przechodzi do krótkiego przeglądu omawianych kwestii szczegółowych by dojść do sposobów budowania kompetencji pracowników oraz wytycznych dla cyberbezpieczeństwa kolei.

Słowa kluczowe: *Infrastruktura Transportowa; Sterowanie Ruchem; Łączność; Pojazdy Kolejowe; Cyberbezpieczeństwo*

Abstract: Paper presents challenges and solutions regarding rail transport cybersecurity on the basis of the presentations and discussions that took place during the IT/OT in Rail Transport 2023 Scientific and Technical Conference, which took place on the 29th -31st January 2024. As at the conference, paper starts with helicopter view of the state of the art of cybersecurity in rail transport, proceeds to an overview of the specific issues discussed during conference, to reach the ways appropriate for staff competence building and guidelines for railway cybersecurity.

Keywords: *Transport Infrastructure; Control Command & Signalling; Communication; Rolling Stock; Cybersecurity*

Wstęp

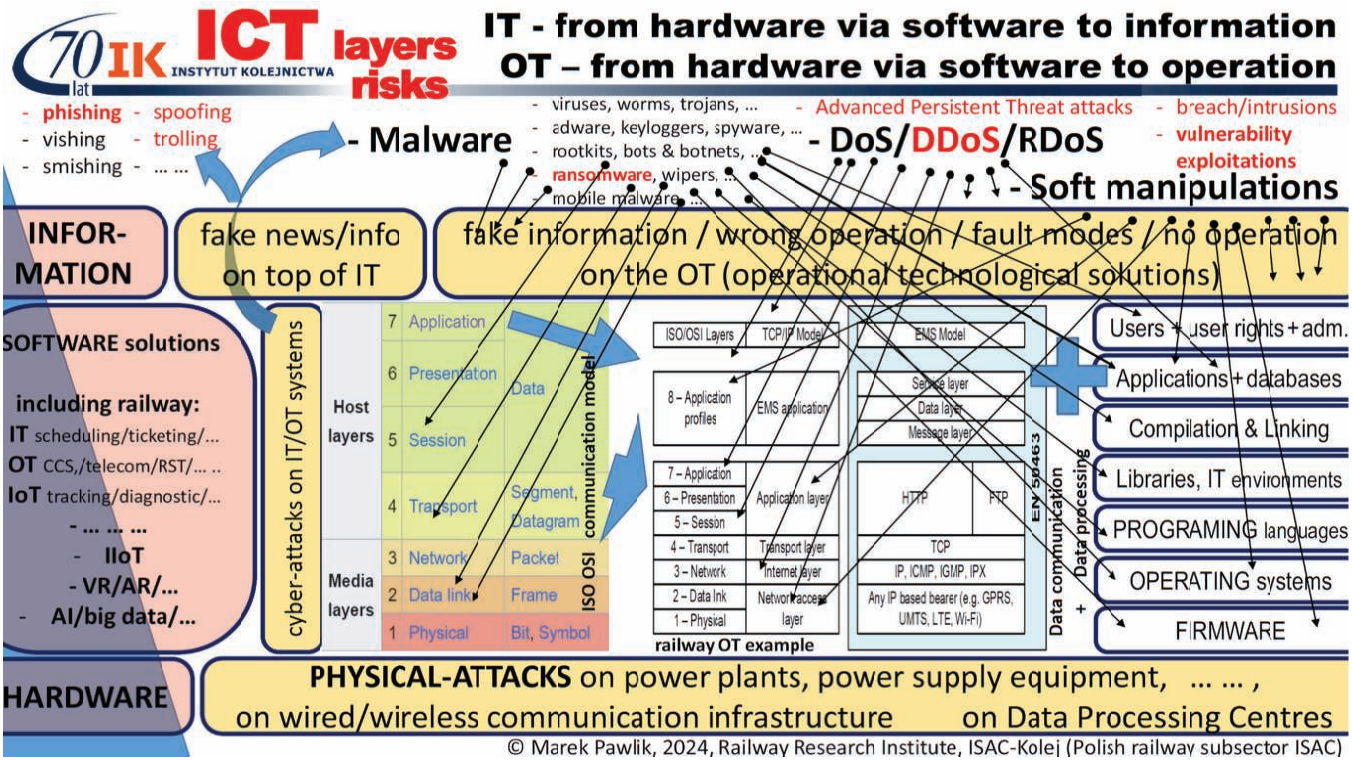
W dniach 29-31 stycznia 2023 miała miejsce Konferencja Naukowo-Techniczna IT/OT w Transporcie Szynowym 2023. Formalnie szósta, ale pierwsza w nowej odsłonie. Wcześniejsze konferencje organizowane przez SITK RP koncentrowały się na wspieraniu transportu przez systemy informatyczne. Ta po raz pierwszy była współorganizowana przez Zarząd Główny SITK RP oraz Instytut Kolejnictwa i miała o wiele szerszy zakres merytoryczny. Podjęty został szerszy temat – systemy informacyjne IT oraz systemy eksploatacyjne OT. Tym samym konferencja objęła wyzwania i rozwiązania cyfrowe także w sterowaniu ruchem kolejowym, zasilaniu, łączności, czy budowie i eksploatacji taboru kolejowego. Zmieniła się także formuła konferencji. Stała się ona międzynarodowa w odniesieniu do treści i uczestników, nowoczesna w zakresie środków oraz powiązana z budowaniem kompetencji i wiedzy, także poprzez możliwość udziału w wizycie technicznej.

Podnoszone i omawiane były tematy bardzo zyskujące obecnie na znaczeniu. Świat, także kolejowy, stał się bardzo cyfrowy, a jednocześnie trwa konflikt w cyberprzestrzeni, o czym informują nawet przedstawiciele wojska. Jesteśmy też w przededniu wejścia w życie *Dyrektywy w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii (2022/2555)*, zgodnie z zapisami której zarządcy kolejowej infrastruktury i przewoźnicy kolejowi, którzy zatrudniają więcej niż 49 osób lub posiadają obroty, względnie roczną sumę bilansową, powyżej 10 milionów euro, będą jeszcze w roku 2024 zobowiązani do zidentyfikowania własnych usług i systemów wykorzystujących rozwiązania cyfrowe oraz wdrożenia procedur: identyfikowania cyberzagrożeń, doskonalenia zabezpieczeń przed cyberzagrożeniami, i raportowania cyberataków i cyberincydentów.

Tym samym, bez żadnej wątpliwości, zasadne jest wykorzystanie informacji przekazanych podczas Konferencji IT/OT w Transporcie Szynowym do uporządkowania wiedzy o wyzwaniach i proponowanych rozwiązaniach, czemu służyć ma niniejsza publikacja.

Widok z lotu ptaka na cyberwyzwania

Nie tylko pasażerowie nie dostrzegają złożoności cyfrowych rozwiązań wykorzystywanych w transporcie szynowym. Jest ona pochodną obecnie stosowanych rozwiązań cyfrowych wspierających funkcjonowanie nie



1. *Widok z lotu ptaka na cyberwyzwania*

tylko podmiotów gospodarczych, ale także państw i społeczeństw.

Wszyscy wiemy, że pod spodem jest hardware, a całkiem na górze informacja. Zwykle hardware kojarzy nam się z naszym komputerem, tymczasem z perspektywy społeczeństw, państw, czy transportu szynowego hardware to elektrownie, sieci energetyczne, obiekty i sieci telekomunikacyjne, czy centra przetwarzania danych. Ataki fizyczne na tak rozumiany hardware mogą sparaliżować transport. Obrona przed takimi atakami to domena wojska.

Wszyscy wiemy, że możliwe i wykorzystywane są manipulacje informacjami. Nikogo już nie zaskakuje fakt pojawiania się fake newsów w dobie oprogramowania typu DeepFake oraz dynamicznego rozwoju sztucznej inteligencji. Przed dezinformacją w środkach masowego przekazu, ale także w sieciach społecznościowych chronić mają nas dedykowane zespoły funkcjonujące w ramach Krajowych Zespołów Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT.

Pomiędzy hardwarem a informacjami mamy software – oprogramowanie. Jako software postrzegamy przede wszystkim nasze oprogramowanie biurowe oraz systemy operacyjne, bez których to oprogramowanie nie działa. Tymczasem do funkcjonowania systemów informacyjnych IT i systemów eksploatacyjnych OT konieczny jest firmware czyli oprogramowanie układowe, bez którego nie działają prawidłowo komponenty sprzętowe, konieczne są systemy operacyjne, języki programowania, związane z nimi biblioteki i środowiska cyfrowe, kompilatory i linkery, dzięki którym powstają programy wykonywalne oraz wykorzystywane przez nie struktury na przykład bazy danych. Poszczególne komputery, serwery i centra przetwarzania danych oraz sterowniki, kontrolery, czy terminale wymieniają dane dla których zachowane musi być cyberbezpieczeństwo rozumiane jako CIA, angielskie Confidentiality, Integrity, Accessibility czyli poufność, integralność i dostępność. Fizyczna reprezentacja transmitowanych danych, zer i jedynek, zależy od środka transmisji. Warstwa fizyczna to jednak dopiero początek. Ogólny model ISO OSI wyróżnia siedem warstw transmisji w systemach informatycznych: warstwę fizyczną, warstwę łącza danych, sieciową, transportową, sesji, prezentacji i warstwę aplikacji. W praktyce warstwy zależą od stosowanych rozwiązań, trzy dolne od rozwiązań w zakresie mediów transmisyjnych a cztery górne od rozwiązań w zakresie narzucanym przez hosta. Inny jest podział funkcji i relacji dla stron internetowych (http), a inny dla serwerów udostępniania plików (ftp). Przesyłanie danych w systemach wspomagających transport szynowy ma miejsce zarówno lokalnie, jak i na duże odległości. Wykorzystuje w większości standardowe ramki, protokoły, telegramy, z ich nadmiarowościami danych, zabezpieczeniami, adresowaniem, których opisy są publicznie dostępne i wykorzystywane przez różniej proweniencji zainteresowane strony. W nielicznych przypadkach tworzone są indywidualne dedykowane rozwiązania kolejowe.

Powszechnemu dostępowi do wielu stosowanych rozwiązań oraz szybkiemu rozwojowi technologii cyfrowych towarzyszą różnego rodzaju ataki na rozwiązania cyfrowe, programowalne, elektroniczne, komputerowe. Mamy więc malware (złośliwe oprogramowanie), w tym wirusy, robaki, trojany, adware, itd. Mamy cyfrowe włamania i kradzieże oraz wykorzystywany w tym celu ransomware. Mamy ataki poprzez infekowanie systemów w eks-

ploatacji, ale także poprzez ingerencje w hardware i software integratorów, ich dostawców, czy poddostawców dostawców. Mamy do czynienia z atakami socjotechnicznymi. O phishingu wszyscy słyszeli dzięki kampaniom informacyjnym banków. Vishing, smishing, whaling, pharming, spoofing, to ciągle techniki, które nie tylko pozostają nienazwane w wielu językach krajowych, ale także są szerzej nieznane lub słabo rozpoznawane, a tymczasem ilość ataków bardzo wyraźnie rośnie. Dziś nie atakują nas hakerzy, a przede wszystkim booty. Dopiero jak booty znajdą lukę i zainfekują system dalsze działania przejmują hakerzy, coraz częściej działający w zorganizowanych grupach sponsorowanych czy wręcz finansowanych przez państwa, czy organizacje terrorystyczne. Działają także crackerzy i haktywiści i chociaż pierwsi dopiero raczkują w hakowaniu, a drudzy mają dobre intencje, to także oni stanowią realne zagrożenie.

Dziś funkcjonują publicznie dostępne bazy podatności. Wspierać mają przede wszystkim tych, którzy chcą się zabezpieczać przed cyberatakami. Są jednak wykorzystywane także przez drugą stronę – coraz częściej mają miejsce tzw. vulnerability exploitations. Przed podatnościami często zabezpiecza patching, updating, upgrading, ale zmiany softwaru w warstwach poniżej mogą zakłócać a nawet uniemożliwiać działanie aplikacji. W dodatku wersje oprogramowania często traktowane są jako parametry w formalnych dokumentach dopuszczających rozwiązania techniczne do stosowania w transporcie szynowym, skutkiem czego często rezygnuje się z jakichkolwiek ingerencji w software. Stoi to w sprzeczności z praktyką w odniesieniu do powszechnie wykorzystywanych rozwiązań cyfrowych – nikogo już nie dziwi, że komputer, tablet, czy telefon informuje że dostępne są aktualizacje, które należy zainstalować ze względów bezpieczeństwa. W wielu przypadkach możemy odmówić, ale w nocy i tak aktualizacja zostanie zainstalowana.

W darknecie za bitcoiny można kupić cyberatak wskazując obiekt ataku i skalę oraz moment ataku. Coraz częstsze i coraz poważniejsze są ataki wolumetryczne, od zwykłych DoS, przez rozproszone DDoS, które znaczne trudniej jest wykryć i zablokować, po RDoS, które mają umożliwić żądanie okupu. Ataki wolumetryczne wykorzystywane są do blokowania funkcjonowania systemów czy usług niezależnie od tego czy mówimy o systemach informacyjnych IT czy eksploatacyjnych OT. Skutki w przypadku tych drugich mogą być poważne nie tyle dla bezpieczeństwa transportu co dla gospodarki kraju, a nawet zdolności obronnych, bo kolej odgrywa poważną rolę w odniesieniu do działań wojennych co widać wyraźnie na przykładzie działań jakie mają miejsce za naszą wschodnią granicą.

Cyfrowe aspekty podnoszone podczas konferencji IT/OT w transporcie szynowym

Konferencja obejmowała cztery panele dyskusyjne oraz czterdzieści prezentacji. Nie sposób omówić wszystkich w jednym artykule. Część zagadnień omówiona jest w innych artykułach tego numeru Przeglądu Komunikacyjnego, ale o części wypada przynajmniej wspomnieć.

Wśród materiałów udostępnionych po konferencji znajdziecie państwo wspólną rozbudowaną wypowiedź dyrektora wykonawczego Agencji Unii Europejskiej do spraw Kolei Josefa Doppelbauera oraz dyrektora Departamentu Bezpieczeństwa i Interoperacyjności Kolei w Dyrektoriacie Generalnym Komisji Europejskiej do spraw Transportu i Mobilności Keira Fitcha. Z ich wypowiedzi jasno wynika jak bardzo bezpieczeństwo cyfrowe w najbliższych latach będzie wpływało na transport kolejowy.

Wspomniane cztery panele dyskusyjne dotyczyły:

- Podejścia do cyberbezpieczeństwa i związanych z tym wyzwań w transporcie szynowym, w tym w szczególności barier formalnoprawnych w zakresie aktualizacji oprogramowania układowego rozwiązań technicznych przenaczonych dla kolei, a podlegających pod dopuszczenia świadectwowe;
- Wyzwań związanych z Rozporządzeniem Komisji (UE) 2023/1695 wprowadzającym nowe wydanie Technicznej Specyfikacji Interoperacyjności w zakresie podsystemów „sterowanie" systemu kolei w Unii Europejskiej TSI CCS (Control Command and Signalling); Specyfikacja TSI CCS 2023 wprowadza między innymi wzorzec 4. Europejskiego Systemu Sterowania Pociągiem ETCS (European Train Control System), pierwsze wydania specyfikacji przyszłego standardu bezprzewodowej łączności kolejowej oparte na standardzie 5G tzw. FRMCS (Future Railway Mobile Communication System) przedstawiając GSM-R i FRMCS jako mobilne radio kolejowe RMR (Railway Mobile Radio), oraz pierwsze specyfikacje automatycznego prowadzenia pojazdów ATO (Automatic Train Operation) zapewniające drugi poziom autonomiczności GoA 2 (Grade of Automation). Przyjęta TSI CCS obejmuje po raz pierwszy załącznik B z trzema tabelami podającymi zasady uaktualniania funkcjonalności i usuwania odchyleń od specyfikacji szczegółowych w instalacjach na liniach kolejowych i w taborze kolejowym na różnych etapach realizacji, włącznie z instalacjami już przekazanymi do eksploatacji. Takie zmiany, już budzą obawy w zakresie zgodności z prawem zamówień publicznych oraz w zakresie ich finansowania, a będą niemal na pewno kłopotliwe formalnie ze względu na wielokrotne zmiany oprogramowania poprzez patching, updating, czy upgrading;
- Rozwiązań technicznych w zakresie łączności bezprzewodowej i transmisji tor-pojazd, ze szczególnym uwzględnieniem wyzwań w zakresie planowania, budowania i zabezpieczania przed cyberatakami sieci GSM-R (Global System for Mobile Communication – Railways); oraz
- Potrzeb w zakresie odporności taboru na cyberzagrożenia, ze szczególnym uwzględnieniem wyzwań związanych z cyberbezpieczeństwem pasażerskiego ta-

boru kolejowego, uwzgledniając fakt, że obecnie zamawiany tabor dostarczany będzie po wejściu w życie dyrektywy NIS2 (dyrektywy (UE) 2022/2555), w świetle której przewoźnicy pasażerscy swój tabor postrzegają jako zestawy urządzeń cyfrowych sterowanych przez maszynistów z wykorzystaniem sieci pokładowych oraz wymieniających bezprzewodowo dane dla potrzeb rozlicznia energii, utrzymywania aktualności informacji pasażerskiej podawanej na pokładzie, diagnostyki, itd.

Wspomniane czterdzieści referatów przedstawionych zostało podczas sześciu sesji merytorycznych, z których dwie dedykowane były wprost cyberbezpieczeństwu, dwie łączności i transmisji tor-pojazd, jedna dedykowana była wymaganiom dla nowego taboru pasażerskiego oraz cyberbezpieczeństwu taboru w eksploatacji, a jedna była sesją otwarcia, podczas której cyberbezpieczeństwo w transporcie szynowym przedstawione zostało z lotu ptaka w zakresie złożoności stosowanych rozwiązań i skali wyzwań. W sesji otwarcia miały miejsce także wspomniane już wypowiedzi dyrektora wykonawczego Agencji Unii Europejskiej do spraw Kolei oraz dyrektora Departamentu Bezpieczeństwa i Interoperacyjności Kolei w Dyrektoriacie Generalnym Komisji Europejskiej do spraw Transportu i Mobilności.

Uzupełnieniem paneli dyskusyjnych i sesji merytorycznych była także sesja warsztatowa zorganizowana przez pracowników Agencji Unii Europejskiej do spraw Kolei w całości poświęcona wyzwaniom związanym ze zmianami specyfikacji TSI w roku 2023.

Przeciwdziałanie cyberzagrożeniom – działania i rozwiązania

Nie ma odwrotu od stosowania w transporcie szynowym rozwiązań cyfrowych, programowalnych, softwarowych, elektronicznych, mechatronicznych, hybrydowych, komputerowych. Musimy jednak podejmować działania dla zapewnienia i ciągłego doskonalenia ich zabezpieczeń przed cyberzagrożeniami. Atakujący wykorzystują także najnowsze rozwiązania techniczne, oraz świeżo ujawnione podatności, i nie respektują ani zasad moralnych ani przepisów prawa zamówień. Nie jesteśmy jednak na straconej pozycji.

W październiku 2020 roku powołane zostało Centrum Wymiany i Analiz Informacji podsektora transportu kolejowego ISAC-Kolej. Równolegle do wojny za naszą wschodnią granicą, przez ostatnie dwa lata, członkowie ISAC-Kolej otrzymali ponad 1200 ostrzeżeń związanych z cyberzagrożeniami. Obejmowały one: informacje o nowych kampaniach phishingowych; informacje o zarejestrowaniu domen podszywających się pod transport i podmioty związane z transportem; rekomendacje blokowania domen na urządzeniach brzegowych, stosowania odpowiednich filtrów antyspamowych; informacje o wykryciu podatności, szczególnie podatności typu zero-day; informacje o dystrybucji złośliwego oprogramowania, rekomendacje w zakresie reguł do stosowania na urządzeniach filtrujących pocztę elektroniczną; informacje o atakach DDoS, o możliwych atakach na strony internetowe i serwisy; rekomendacje antyDDoS, dotyczące monitorowania i ograniczania ruchu przy eskalacji; oraz inne przydatne informacje, np. dotyczące działalności grup APT, Killnet, itp.

Niezależnie od ostrzeżeń członkowie ISAC-Kolej otrzymują codzienne raporty krajowe dotyczące złośliwego ruchu sieciowego z rekomendacjami dotyczącymi blokowania konkretnych adresów IP; tygodniowe raporty krajowe zawierające informacje na temat wykrytych podatności w produktach IT z rekomendacjami w zakresie uaktualniania systemów i oprogramowania; oraz dwutygodniowy biuletyn informacyjny Centrum Bezpieczeństwa Operacyjnego PKP Informatyka dedykowany cyberbezpieczeństwu transportu kolejowego.

Niemal wszyscy pracownicy podmiotów kolejowych korzystają w swojej pracy z systemów informacyjnych IT i/lub systemów eksploatacyjnych OT. Jednocześnie nie bez powodu mówi się, że najsłabszym ogniwem w bezpieczeństwie systemów cyfrowych jest człowiek. Konieczne jest więc budowanie wiedzy pracowników w zakresie cyberhigieny. Od właściwego podejścia do definiowania i wykorzystywania haseł do reagowania na symptomy wskazujące na malware, ataki wolumetryczne DoS/DDoS/RDoS, ransomware, czy ingerencje w oprogramowanie. Już w kwietniu 2021 ISAC-Kolej przyjął *Wytyczne dotyczące cyberbezpieczeństwa dla pracowników podmiotów kolejowych*. Są one publicznie dostępne na www.isac-kolej.pl i są wykorzystywane przez podmioty kolejowe zarówno do budowania wiedzy pracowników w zakresie cyberhigieny jak i do weryfikowania kompletności procedur wewnętrznych w zakresie bezpieczeństwa informacji i ich doskonalenia.

Na konferencji szczegółowo przedstawione zostały najnowsze *Wytyczne dotyczące cyberbezpieczeństwa pasażerskiego taboru kolejowego* przyjęte przez ISAC-Kolej w lipcu 2023 r. Od stycznia 2024 r., ze względu na potrzeby przemysłu taborowego, w tym jego międzynarodowy charakter w zakresie łańcuchów dostaw i w zakresie klientów końcowych, wytyczne te są dostępne w pełnej wersji dwujęzycznej obejmującej język polski i język angielski (także dostępna na www.isac-kolej.pl). Wytyczne zawierają zarówno podstawy, w tym definicje, jak i czternaście kart kontrolnych i związaną z nimi metodologię. Przyjęta metodologia pozwala na identyfikowanie niedostatków zabezpieczeń przed cyberatakami dla konkretnych typów taboru. Pozwala na proste definiowanie wymagań w zakresie odporności na cyberzagrożenia przez podmioty zamawiające tabor kolejowy, czy szerzej tabor szynowy. Pozwala także na różnicowanie poziomów zabezpieczeń przed cyberzagrożeniami. To rozbudowany dojrzały dokument.

W roku 2023 dla członków ISAC-Kolej zorganizowane zostały także pierwsze dwudniowe warsztaty na cyberpoligonie. Środowisko sieciowe obejmujące wiele powiązanych maszyn wirtualnych opartych na różnych systemach operacyjnych (linux, unix, windows) i aplikacjach webowych odtwarza infrastrukturę IT/OT pozwalając

na szkolenie pracowników z wykorzystaniem systemów i procedur używanych na co dzień w podmiotach kolejowych. Pozwala na weryfikowanie odporności organizacji, weryfikowanie i doskonalenie umiejętności pracowników odpowiedzialnych za ochronę przed cyberzagrożeniami, np. pracowników zespołów SOC (Security Operation Centre), czy administratorów sieci. Instalacje takie wykorzystuje się np. w trybie threat hunting informując zespoły niebieskie, których zadaniem jest wykrycie źródła ataku i uszczelnienie systemów, o ataku/atakach, które są realizowane przez równolegle pracujące atakujące zespoły czerwone.

Na zakończenie

Autor w imieniu Komitetu Naukowego Konferencji IT/OT w Transporcie Szynowym chce podziękować wszystkim uczestnikom paneli dyskusyjnych oraz autorom prezentacji za wkład w budowanie świadomości wyzwań oraz wiedzy i umiejętności w zakresie ich pokonywania w odniesieniu do digitalizacji otaczających nas rozwiązań technicznych.

Jednocześnie zwrócić należy uwagę, że szybki rozwój technologii cyfrowych informacyjnych IT i eksploatacyjnych OT w powiązaniu z długimi okresami trwałości kolejowych instalacji i rozwiązań infrastrukturalnych i taborowych z całą pewnością będzie wymagał ciągłego uzupełniania wiedzy i doskonalenia umiejętności ekspertów od transportu szynowego. W imieniu Komitetu Naukowego oraz Komitetu Organizacyjnego autor deklaruje, że kolejne Konferencje IT/OT w Transporcie Szynowym z całą pewnością będą wychodzić naprzeciw tym wyzwaniom.

Na zakończenie słowa podziękowania należą się Komitetowi Organizacyjnemu za sprawną organizację i wielkie zaangażowanie oraz firmie Alstom, która udostępniła uczestnikom konferencji możliwość udziału w wycieczce technicznej w centrum utrzymania pociągów pendolino. ◄

Materiały źródłowe

[1] Dyrektywa w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii (NIS2, czyli dyrektywa (UE) 2023/2555)
[2] Wytyczne dotyczące cyberbezpieczeństwa dla pracowników podmiotów kolejowych. www.isac-kolej.pl
[3] Wytyczne dotyczące cyberbezpieczeństwa pasażerskiego taboru kolejowego. www.isac-kolej.pl