INSTYTUT KOLEJNICTWA

100 LAT BADAŃ W POLSKIM KOLEJNICTWIE

Krajowa Sekcja Kolejowa
Stowarzyszenia Inżynierów
i Techników Komunikacji RP

Instytut Kolejnictwa, W-wa 10.03.2026 r.

Budowanie kompetencji pracowników podmiotów kolejowych w zakresie **cyberbezpieczeństwa**

dr hab. inż. Marek Pawlik, prof. IK
Instytut Kolejnictwa, zastępca dyrektora Instytutu

1. Cyberprzestrzeń

Cyberprzestrzeń kolejowa

LAT BADAŃ W POLSKIM KOLEJNICTWIE

IT - informacja

OT - działanie

INFOR-MACJA

fake info / zła praca on top of IT / syst. IT

fake info / nieprawidłowe działanie / brak działania / błędne tryby pracy systemów OT (cyfrowych rozwiązań eksploatacyjnych)

SOFTWARE

systemy kolejowe:

- **IT** scheduling/ticketing/...
- **OT** CCS,/telecom/RST/... ..
- **IoT** tracking/diagnostic/...
- **... ... ...**
- **IIoT**
- **VR/AR/...**
- **AI/big data/...**

oprogramowanie

HARDWARE

ATAKI FIZYCZNE na elektrownie, systemy i sieci zasilania, ... ,
przewodowe / bezprzewodowe systemy łączności Centra Przetwarzania Danych

Ryzyka w cyberprzestrzeni kolejowej

LAT BADAŃ W POLSKIM KOLEJNICTWIE

- **phishing**
- vishing
- smishing
- **quishing**
- spoofing
- jamming
- trolling
- … …

- Ransomware

- Malware
- viruses, worms, trojans, …
- adware, keyloggers, spyware, …
- rootkits, bots & botnets, …
- **ransomware**, wipers, …
- mobile malware, …

- Advanced Persistent Threat attacks

- DoS/DDoS/RDoS

- breach/intrusions
- **vulnerability exploitations**

- Soft manipulations

INFOR-MACJA

fake info / zła praca on top of IT / syst. IT

fake info / nieprawidłowe działanie / brak działania / błędne tryby pracy systemów OT (cyfrowych rozwiązań eksploatacyjnych)

SOFTWARE

systemy kolejowe:
- **IT** scheduling/ticketing/…
- **OT** CCS,/telecom/RST/… ..
- **IoT** tracking/diagnostic/…
- **… … …**
- **IIoT**
- **VR/AR/…**
- **AI/big data/…**

cyber-ataki na systemy IT/OT

Host layers	7	Application	Data
	6	Presentation	
	5	Session	
	4	Transport	Segment, Datagram
Media layers	3	Network	Packet
	2	Data link	Frame
	1	Physical	Bit, Symbol

ISO OSI communication model

- **Ransomware** (ransomware)
- **Threats against data** (zagrożenia dla danych)
- **Malware** (złośliwe oprogramowanie)
- **Denial of service** (ataki DoS / DDoS)
- **Vulnerability exploitation** (podatności)
- **Social engineering** (inżynieria społeczna)
- **Supply-chain attacks** (na łańcuchy dostaw)
- **Breach/intrusion (**naruszenie/włamanie)
- **credential harvesting** (zabór uwierzytelnień)
- **geolocation spoofing** (fałsz geolokalizacji)
- **… …**

Data communication + Data processing

- Użytkownicy + uprawnieni
- Aplikacje + bazy danych
- Compilation & Linking
- Biblioteki i środowiska IT
- Języki PROGRAMOWANI
- Systemy OPERACYJNE
- FIRMWARE

HARDWARE

ATAKI FIZYCZNE na elektrownie, systemy i sieci zasilania, … … ,
przewodowe / bezprzewodowe systemy łączności Centra Przetwarzania Danych

2. Kolejowe cyberwyzwania

na przykładzie systemów sterowania ruchem kolejowym

gamechangers

uwarunkowania kolejowego IT & OT:

Techniczne

- komputerowe systemy sterowania ruchem – **elektronika**, **oprogramowanie**, normy **RAMS**
- obowiązkowe stosowanie 11 **specyfikacji TSI** w tym **TSI TAF**, **TSI TAP**, **TSI CCS**, **TSI LOC&PAS**
- systemy detekcji stanów awaryjnych taboru **DSAT**, stanów awaryjnych pantografów **DSAP**
- ocena ryzyka wg rozporządzenia **CSM RA** oraz norm **RAMS**
- **cyberataki na** cyfrowe **kolejowe** systemy informacyjne **IT** i eksploatacyjne **OT**
- **migracja** od sprzęgu śrubowego **do** cyfrowego sprzęgu samoczynnego **DAC**
- **migracja** od łączności analogowej przez GSM-R **do FRMCS** – kolejowej łączności 5G

Formalne

- podział kolei na **IMs, RUs, NSAs,** NIBs, NoBo, DeBo, AsBo, … (zarządców, przewoźników, …
- procesy **oceny zgodności WE** oraz **weryfikacji WE** obok procesów **świadectwowych**
- systemy zarządzania bezpieczeństwem **SMS** oraz zarządzania utrzymaniem **MMS** a sys. **SZBI**
- dyrektywy i rozporządzenia UE w zakresie cyberbezpieczeństwa **NIS2**, **CER**, **CRA**, ……..
- ustawa o Krajowym Systemie Cyberbezpieczeństwa – wejście NIS2 ustawą z 23.01.2026

Wyzwania techniczne i organizacyjne
przykład systemów sterowania

Co się może zdarzyć w systemach sterowania ?

1. Ataki wolumetryczne - blokowanie
2. Zdalne wyłączenie
3. Zaszyfrowanie i żądanie okupu
4. Długotrwałe podsłuchiwanie w celu przygotowania manipulacji oprogramowaniem
5. Manipulacje oprogramowaniem
6. …

Co sprzyja ryzyku cyberataków na systemy sterowania ?

1. Braki uaktualnień oprogramowania
2. Braki zarządzania uprawnieniami
3. Braki kopii danych i programów
4. Łatwy dostęp do terminali
5. Łatwy dostęp do aktywnych urządzeń sieciowych
6. Braki w wiedzy użytkowników o konfiguracjach i komponentach
7. Braki w zakresie analiz podatności
8. Brak systemu raportowania uszkodzeń oraz działań korekcyjnych (FRACAS)
9. …

Co się może zdarzyć

w systemach pokrewnych do systemów sterowania ?

1. **Haktywiści/hakerzy w systemach informacji pasażerskiej**
2. **Wyłączanie: zasilania, HVAC, EOR, oświetlenia, nagłośnienia, …**
3. **Możliwe niezauważalne zbieranie danych z LCS-ów lub syst. Łączności, o ruchu pociągów i ładunków**
4. **Ataki na systemy łączności oraz z wykorzystaniem syst. łączności**

Co dodatkowo sprzyja ryzyku cyberataków na syst. pokrewne ?

1. **Brak formalnych dopuszczeni na poziomie UE lub krajowym**
2. **Korzystanie z rozwiązań pozbawionych wsparcia technicznego producentów**
3. **Brak pełnej świadomości ryzyka**
   - **widzimy bezpieczeństwo ruchu**
   - **nie widzimy zagrożeń dla gospodarki / obronności**
4. **Brak stosowania analizy ryzyka dla zmian otoczenia technicznego**
5. **…**

3. Dyrektywa NIS2 ➔ Ustawa KSC

DYREKTYWA 2022/2555 w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium UE

Ustawa o zmianie ustawy o Krajowym Systemie Cyberbezpieczeństwa

DZIENNIK USTAW
RZECZYPOSPOLITEJ POLSKIEJ

Warszawa, dnia 2 marca 2026 r.

Poz. 252

USTAWA

z dnia 23 stycznia 2026 r.

o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw[1)]

Czy my podlegamy ?

pod regulacje dot. cyberbezpieczeństwa

- **Trzy możliwości identyfikowania podmiotów** jako kluczowe lub ważne
  - **Samoidentyfikacja,**
  - **Decyzja organu właściwego,**
  - Decyzja ministra właściwego do spraw informatyzacji … w sektorze podmiotów publicznych, jeżeli realizuje … zadanie publiczne i spełnia … warunki (art. 7m).
- **Podmioty średnie i większe**
  - Określonego typu (w tym **zarządcy infrastruktury i przewoźnicy kolejowi**) **należące do sektora kluczowego** (w tym transportu szynowego) lub ważnego
  - Zatrudniające ponad 49 osób, o obrotach rocznych (sumie bilansowej) ponad 10 mln €

Co z tego wynika ?

- **Liczne konieczne prace własne zarządców i przewoźników**
- **Konieczne wspólne prace sektora kolejowego**
  - **Wymiana informacji i cyber-ostrzeżeń**
  - **Definiowanie wspólnych wytycznych**
  - **Budowanie kompetencji i umiejętności**
  - **Analizy podatności i cyberincydentów**

Obowiązki podmiotów 1/3

16) art. 8 otrzymuje brzmienie:

„Art. 8. 1. Podmiot kluczowy lub podmiot ważny wdraża system zarządzania bezpieczeństwem informacji w systemie informacyjnym wykorzystywanym w procesach wpływających na świadczenie usługi przez ten podmiot, zapewniający:

1) prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzanie tym ryzykiem;

2) wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy, koszty wdrożenia, wielkość podmiotu, prawdopodobieństwo wystąpienia incydentów, narażenie podmiotu na ryzyka, skutki społeczne i gospodarcze, w szczególności:

   a) polityki szacowania ryzyka oraz bezpieczeństwa systemu informacyjnego, w tym polityki tematyczne,

   b) bezpieczeństwo w procesie nabywania, rozwoju, utrzymania i eksploatacji systemu informacyjnego, w tym testowanie systemu informacyjnego,

   c) bezpieczeństwo fizyczne i środowiskowe uwzględniające kontrole dostępu,

   d) bezpieczeństwo zasobów ludzkich,

   e) bezpieczeństwo i ciągłość łańcucha dostaw produktów ICT, usług ICT i procesów ICT, od których zależy świadczenie usługi, z uwzględnieniem związków pomiędzy bezpośrednim dostawcą sprzętu lub oprogramowania a podmiotem kluczowym lub podmiotem ważnym,

Obowiązki podmiotów 2/3

f) wdrażanie, dokumentowanie, testowanie i utrzymywanie planów ciągłości działania umożliwiających ciągłe i niezakłócone świadczenie usługi oraz zapewniających poufność, integralność, dostępność i autentyczność informacji, planów awaryjnych oraz planów odtworzenia działalności umożliwiających odtworzenie systemu informacyjnego po zdarzeniu, które spowodowało straty przekraczające zdolności podmiotu do odbudowy za pomocą własnych środków,

g) objęcie systemu informacyjnego wykorzystywanego do świadczenia usługi systemem monitorowania w trybie ciągłym,

h) polityki i procedury oceny skuteczności środków technicznych i organizacyjnych,

i) edukację z zakresu cyberbezpieczeństwa dla personelu podmiotu,

j) podstawowe zasady cyberhigieny,

k) polityki i procedury stosowania kryptografii, w tym w stosownych przypadkach szyfrowania,

l) stosowanie bezpiecznych środków komunikacji elektronicznej w ramach krajowego systemu cyberbezpieczeństwa oraz wewnątrz podmiotu, uwzględniających uwierzytelnianie wieloskładnikowe w stosownych przypadkach,

m) zarządzanie aktywami,

n) polityki kontroli dostępu;

Obowiązki podmiotów 3/3

3) zbieranie informacji o cyberzagrożeniach i podatnościach na incydenty systemu informacyjnego wykorzystywanego do świadczenia usługi;

4) zarządzanie incydentami;

5) stosowanie środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego wykorzystywanego do świadczenia usługi, w tym:

   a) stosowanie mechanizmów zapewniających poufność, integralność, dostępność i autentyczność danych przetwarzanych w systemie informacyjnym,

   b) regularne przeprowadzanie aktualizacji oprogramowania, stosownie do zaleceń producenta, z uwzględnieniem analizy wpływu aktualizacji na bezpieczeństwo świadczonej usługi oraz poziomu krytyczności poszczególnych aktualizacji,

   c) ochronę przed nieuprawnioną modyfikacją w systemie informacyjnym,

   d) niezwłoczne podejmowanie działań po dostrzeżeniu podatności lub cyberzagrożeń, w tym również czasowe ograniczenie ruchu sieciowego przychodzącego do infrastruktury podmiotu kluczowego lub podmiotu ważnego, które może skutkować zakłóceniem usług świadczonych przez ten podmiot, z uwzględnieniem konieczność minimalizacji skutków ograniczenia dostępności tych usług, z uwagi na podjęte działania.

Obowiązki podmiotów

podsumowanie

Wdrożenie systemu zarządzania bezpieczeństwem informacji

Obsługa, zgłaszanie incydentów poważnych i współdziałanie przy obsłudze incydentu poważnego i incydentu krytycznego

Zgłoszenie **wczesnego ostrzeżenia oraz złożenie sprawozdań: końcowego i okresowego**

Systematyczne przeprowadzanie **audytu bezpieczeństwa** systemu informacyjnego

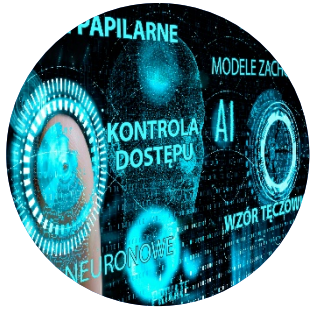
Opracowanie, wdrożenie i aktualizacja dokumentacji bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi

Korzystanie z systemu teleinformatycznego s46

Wyznaczenie osób odpowiedzialnych za utrzymywanie kontaktów z podmiotami ksc;

Zapewnienie użytkownikowi usługi dostępu do wiedzy pozwalającej na zrozumienie cyberzagrożeń i stosowanie skutecznych sposobów zabezpieczania

Obowiązkowe **szkolenia** dla kadry kierowniczej



Przekazywanie informacji na żądanie OW w ramach nadzoru i kontroli

zapewnienie użytkownikowi usługi **możliwości zgłoszenia cyberzagrożenia**, incydentu lub podatności związanych ze świadczoną usługą

Dostosowanie się do **polecenia zabezpieczającego**

4. Działania Instytutu Kolejnictwa

Działania systemowe IK

1. **Budowanie kompetencji pracowników zarówno zarządców jak i przewoźników**
   a. W postaci informacji dla pracowników korzystających z rozwiązań cyfrowych, w tym
      i. ogólnego IT (biurowych, finansowo-księgowych, zarządzania majątkiem, poczty, intranetu, …)
      ii. kolejowego IT (sprzedaży tras/biletów, informacji pasażerskiej www, ewidencji pracy ekspl., …)
      iii. kolejowego OT (srk, łączności, diagnostyki, taboru, informacji pasażerskiej (w taborze/na stacji, …)

   b. W postaci CLK – Cyfrowego Laboratorium Kolejowego dla pracowników odpowiedzialnych za akceptację, utrzymanie, zabezpieczanie, tworzenie, nadzorowanie rozwiązań cyfrowych wykorzystywanych na kolei
      i. opartego na szkoleniu i indywidualnej realizacji zadań na cyberpoligonie wykorzystywanym przez WOC
      ii. w tym budowania oraz weryfikowania kompetencji oraz symulowania ataków, w warunkach poligonu
      iii. z wykorzystaniem kompetencji IK oraz ekspertów AGH (wspierających polskie WOC)

2. **Działania wspierające bezpieczeństwo cyfrowe transportu kolejowego w Polsce realizowane przez IK**
   a. Centrum Wymiany i Analizy Informacji podsektora transportu kolejowego „ISAC – Kolej”
      i. bieżąca wymiana informacji o zagrożeniach
      ii. definiowanie dobrych praktyk w zakresie bezpieczeństwa cyfrowego transportu kolejowego
      iii. współpraca z Biurem Zarządzania kryzysowego MI

   b. Analiza ryzyk cyfrowych dla kluczowych przewoźników i zarządców kolejowych

   c. Oceny bezpieczeństwa w odniesieniu do ryzyk cyfrowych dla przemysłu
      i. dla taboru nowego i modernizowanego
      ii. dla zmian w infrastrukturze
      iii. dla budowy nowej infrastruktury

ISAC-Kolej

- PKP S.A.
- PKP Polskie Linie Kolejowe S.A.
- PKP Intercity S.A.
- PKP Szybką Koleją Miejską sp. z o. o.
- PKP CARGO S.A.
- PKP Linia Hutnicza Szerokotorowa sp. z o. o.
- PKP Informatyka sp. z o.o.
- NASK Państwowy Instytut Badawczy
- Instytut Kolejnictwa
- POLREGIO S.A.
- Koleje Śląskie
- Koleje Małopolskie
- Pomorska Kolej Metropolitalna
- SKM Warszawa
- Umowa o współpracy z UTK

W październiku 2020 r. powołane zostało

Centrum Wymiany i Analizy Informacji podsektora transportu kolejowego ISAC–Kolej

Koordynacja prac ISAC-Kolej realizowana jest przez Instytut Kolejnictwa we współpracy z PKP PLK oraz PKP Informatyka.

ISAC-Kolej wspiera podmioty kluczowe podsektora transportu szynowego

wytyczne dot. cyberbezpieczeństwa
dla pracowników kolei

Wytyczne dot. cyberbezpieczeństwa dla pracowników podmiotów kolejowych

European Commission
Transport cybersecurity toolkit

Aktorzy zagrożeń

Osoby fizyczne lub organizacje mogą umyślnie lub nieumyślnie ujawniać i wykorzystywać podatności, które mogą potencjalnie powodować incydenty i wpływać na usługi transportowe, w tym na ich bezpieczeństwo, ochronę, działanie, finanse i reputację. Aktorzy zagrożeń to między innymi grupy sponsorowane przez organy państwowe, cyberprzestępcy, cyberterroryści, haktywiści[1], hakerzy (w tym skrypt krakerzy[2]) oraz osoby legalnie posiadające dostęp do wewnętrznych informacji (w tym uprzywilejowane osoby posiadające legalny dostęp do takich informacji).

Najważniejszymi destrukcyjnymi aktorami celowo atakującymi organizacje transportowe są **cyberprzestępcy, osoby legalnie posiadające dostęp do wewnętrznych informacji**, państwa narodowe i **grupy sponsorowane przez organy państwowe**. Przeciwnicy, tacy jak cyberprzestępcy, przeprowadzają zmasowane kampanie cyberataków i często starają się uzyskiwać pieniężne profity.

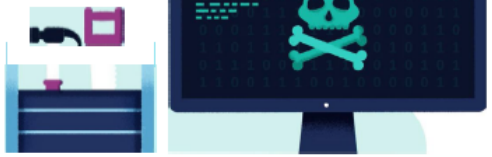
Legalnie posiadający dostęp do wewnętrznych informacji znają specyfikę organizacji, dla których pracują, i często doskonale zdają sobie sprawę z subtelnych luk w zabezpieczeniach. Wewnętrzni aktorzy zagrożeń to między innymi niezadowoleni pracownicy, dostawcy i indywidualni wykonawcy. W miarę wzrostu globalnych napięć geopolitycznych, państwa narodowe i **grupy sponsorowane przez organy państwowe** stawiają sobie długoterminowe cele strategiczne. Często próbują one ukryć się w głębi struktury organizacji i gromadzić wrażliwe informacje. Po zdobyciu przyczółków w systemach cyfrowych, napastnicy sponsorowani przez organy państwowe starają się zająć pozycje, które zagwarantują spowodowanie jak największych szkód. Na przykład, mogą zaatakować systemy innych organizacji, wykorzystując połączenia sieciowe zinfiltrowanej organizacji.

Do aktorów zagrożeń zalicza się także osoby posiadające dostęp do wewnętrznych informacji, które mogą nieumyślnie lub przypadkowo podejmować działania skutkujące zdarzeniami związanymi z cyberbezpieczeństwem, a w najgorszych przypadkach incydentami cybernetycznymi mającymi wpływ na bezpieczeństwo i ochronę usług transportowych.

Pojawiające się cyber-zagrożenia

Istnieje wiele cyber-zagrożeń ukierunkowanych na transport: rozproszone blokowania usług (DDoS), blokowania usługi (DoS), kradzieże danych, rozpowszechnianie złośliwego oprogramowania (malwaru), phishing, manipulacje oprogramowaniem, nieuprawniony dostęp, ataki destrukcyjne, fałszowanie lub obchodzenie procesów decyzyjnych angażujących operatorów cyberbezpieczeństwa, maskarady tożsamości, nadużywanie przywilejów dostępu, inżynieria społeczna, niszczenie wizerunku, podsłuchy, niewłaściwe wykorzystywanie aktywów, czy manipulacje sprzętem.

W oparciu o obszerne badanie literaturowe publicznie dostępnych dokumentów oraz wywiady z ekspertami uznano, że do najpilniejszych pojawiających się cyber-zagrożeń mających wpływ na transport należą: złośliwe oprogramowanie (malware), (rozproszone) blokowania usług (DDoS & DoS), nieuprawnione uzyskiwanie dostępu, kradzieże oraz manipulacje oprogramowaniem.



[1] **haktywiści** to osoby, które używają komputerów i sieci do promowania celów społecznych i politycznych, zwłaszcza wolności słowa, praw człowieka i dostępu do informacji.
[2] **skrypt krakerzy** to osoby które używają programów i skryptów napisanych przez innych bez dogłębnej znajomości zasad ich działania, jedynie po to, aby uzyskać nieuprawniony dostęp do komputerowych kont użytkowników lub plików lub żeby przeprowadzać ataki na systemy komputerowe.

Zagrożenie #1: złośliwe oprogramowanie (Malware)
Złośliwe oprogramowanie, które może mieć potencjalny wpływ na osoby lub organizacje w różnych rodzajach transportu.

Zagrożenie #2: (rozproszone) blokowanie usługi ((D)DoS)
Ataki cybernetyczne uniemożliwiające osobom fizycznym lub organizacjom dostęp do odpowiednich usług i zasobów transportowych.

Zagrożenie #3: nieuprawniony dostęp i kradzież
Nieuprawniony dostęp, przywłaszczenie i wykorzystanie krytycznych zasobów.

Zagrożenie #4: manipulacje oprogramowaniem
Ataki cybernetyczne na oprogramowanie w celu zmiany jego działania i przeprowadzania specyficznych ataków.

Zagrożenie #1 złośliwe oprogramowanie (Malware)

European Commission
Transport cybersecurity toolkit

Złośliwe oprogramowanie (Malware) obejmuje szkodliwe programy, które mogą obejmować różne rodzaje aplikacji, takie jak robaki, ransomware, cryptocurr wszelkie aplikacje, które mogą p negatywny wpływ na organizacj prywatne w różnych rodzajach t

Ograniczanie rozprzestrzeniania oprogramowania przeznaczone uszkadzania komputerów, serw sieci lub wszystkich tych elemen z głównych priorytetów cyberbe wszystkich rodzajach transportu ataku może obejmować wiadom e-mail typu phishing skierowane pracowników. Inne wektory atak obejmować różne i wyrafinowar inżynierii społecznej, takie jak p

klucza USB do wolnego portu (np. w celu naładowania telefonu komórkowego). Klikając

Zagrożenie #2 (rozproszone) blokowanie usługi

European Commission
Transport cybersecurity toolkit

Ataki typu rozproszone blokowanie usługi (DDoS – ang. Distributed Denial of Service) oraz blokowanie usługi (DoS – an wpływają na dostępność i o usług, systemów i innych za ataki mogą trwać przez różn skierowane na więcej niż jed system jednocześnie. Ataki wiele systemów (lub kanałó przeciążenia docelowych us żądaniami. Udane ataki wpr usług i możliwości systemó niespodziewanej ilości żąda blokowaniem dostępu do u

komputery osobiste i specjalizowane urządzenia) w celu uzyskania dostępu do

Należy zauważyć, że dotknię należące do organizacji tran być wykorzystywane do prz ataków DDoS i DoS, których systemy eksploatacyjne lub Zaatakowane mogą zostać korporacyjne systemy infor

Zagrożenie #3 nieuprawniony dostęp i kradzież

European Commission
Transport cybersecurity toolkit

Aktorzy zagrożeń mogą chcieć uzyskać logiczny lub fizyczny dostęp bez zezwolenia do sieci, systemu, aplikacji, danych lub w celu przeprowadzenia dest w tym kradzieży wrażliwych d (w tym zasobów fizycznych).

W odniesieniu do nieuprawnionego dostępu

Zagrożenia związane z nieupr dostępem i kradzieżą dotycz i zastrzeżonych (w tym identy dane uwierzytelniające do ko uprzywilejowanych, systemó rodzajów informacji poufnyc Zagrożenia te mogą wykorzy systemach, jak również niezw ujawniające dane wrażliwe, t uwierzytelniające (np. login, osobowe (np. e-mail, osobist identyfikacyjny itp.).

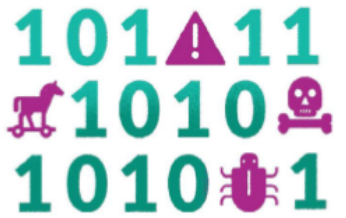
Zagrożenie #4 manipulacja oprogramowaniem

European Commission
Transport cybersecurity toolkit

Nieprawidłowe konfiguracje i manipulacje oprogramowaniem oraz powiązanymi z nim systemami lub składnikami mogą mieć bezpośredni wpływ na stan bezpieczeństwa usług i systemów transportowych. Ataki cybernetyczne wykorzystujące manipulacje oprogramowaniem modyfikują ustawienia oprogramowania lub wpływają na integralność danych w celu zmiany zachowania systemów i usług.

Atakujący mogą celowo manipulować oprogramowaniem (lub jego częścią) w celu uzyskania korzyści z dostępu do wrażliwych zasobów (np. uzyskania nieuprawnionego dostępu, uniemożliwienia uprawnionym osobom lub systemom dostępu do niezbędnych zasobów, gromadzenia poufnych informacji, wprowadzania zmian w sposobie realizacji funkcji itp.).

Na przykład atakujący mogą celować w kanały komunikacyjne producentów w celu przesyłania destrukcyjnych aktualizacji oprogramowania usług i systemów (w tym technologii eksploatacyjnych) w czasie eksploatacji. Atakujący wykorzystują naruszone poświadczenia autoryzacji, aby uzyskać dostęp do zabezpieczonego interfejsu sieciowego zdalnego serwisu w celu zainstalowania zmanipulowanego oprogramowania i dalszego narażania na utratę bezpieczeństwa innych dostępnych usług i systemów. Następnie instalują zmanipulowane oprogramowanie, które narusza bezpieczeństwo docelowych usług i systemów lub atakują inne podłączone usługi i/lub systemy.



Dobre praktyki przeciw manipulacjom oprogramowaniem

Możesz pomóc w ochronie swojej organizacji poprzez przestrzeganie dobrych praktyk w zakresie identyfikacji i zapobiegania manipulacji oprogramowaniem, takich jak:

- ☐ Unikanie instalowania niewiarygodnego oprogramowania na systemach i urządzeniach (w tym komputerach osobistych, serwerach, urządzeniach peryferyjnych, urządzeniach sieciowych, smartfonach itp.).
- ☐ Instalowanie zawsze oprogramowania i aktualizacji z oficjalnych źródeł i stron internetowych (np. producentów, repozytoriów firmowych itp.).
- ☐ Unikanie pobierania oprogramowania i aplikacji (oraz wszelkich plików) z nielegalnych źródeł.
- ☐ Odinstalowywanie niepotrzebnego lub ostatnio nieużywanego oprogramowania i wyłączanie niepotrzebnych połączeń (np. protokołów i usług sieciowych), w tym dostępu do usług zdalnych (np. usług przechowywania danych w chmurze).
- ☐ Skanowanie wszelkiego oprogramowania i urządzeń pamięci masowej za pomocą niezawodnego i zaktualizowanego programu antywirusowego.
- ☐ Pobieranie bezpiecznego oprogramowania przemysłowego (np. aktualizacji, poprawek, nowych produktów itp.) od zaufanych dostawców, stosując zasadę białej stacji.
- ☐ Aktualizowanie całego zainstalowanego oprogramowania zgodnie z zasadami i praktykami organizacyjnymi.

wytyczne 2021

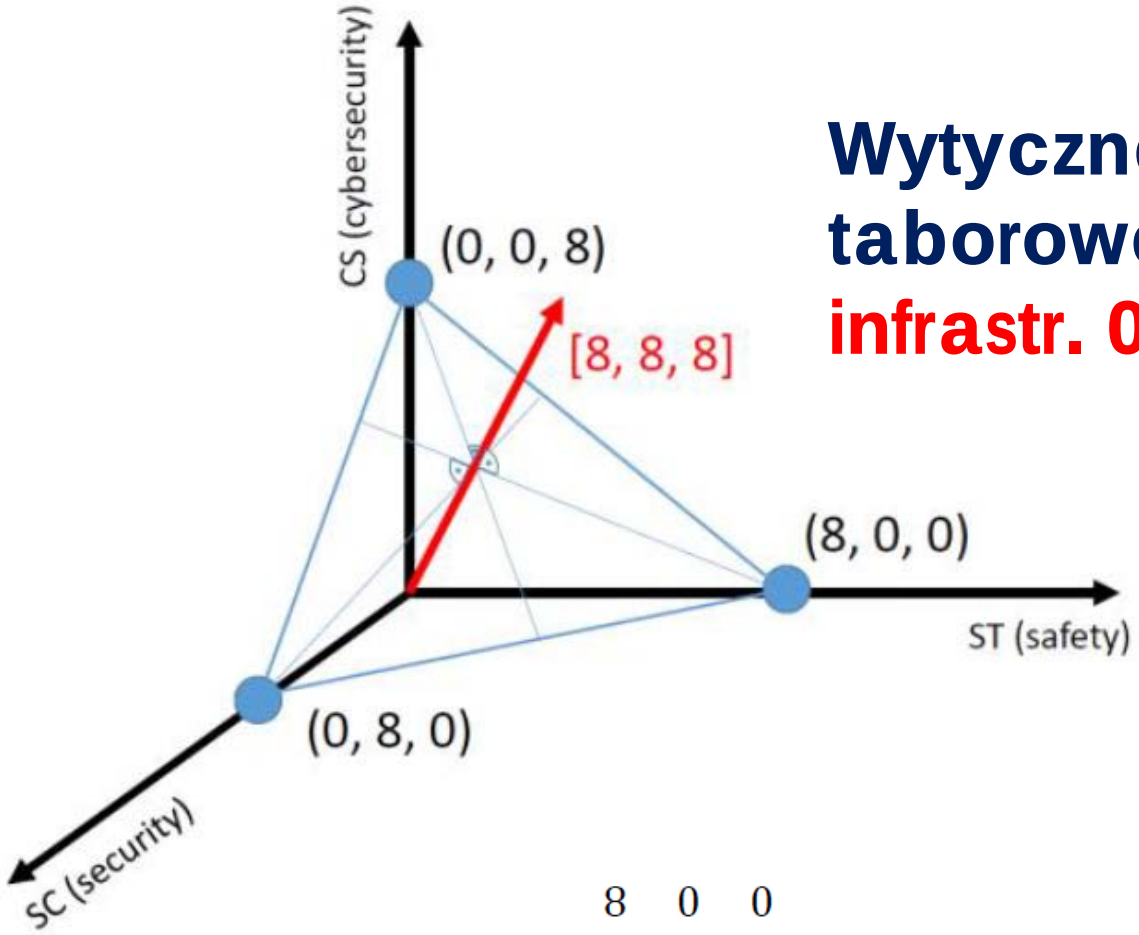
wytyczne dot. cyberbezpieczeństwa:
- pasażerskiego taboru kolejowego – przyjęte 30.07.2023
- wyposażenia linii kolejowych w srk, bkjp i systemy tele.

Centrum Wymiany i Analizy Informacji
podsektora transportu kolejowego
„ISAC – Kolej"

Wytyczne dotyczące cyberbezpieczeństwa pasażerskiego taboru kolejowego

wersja 1.0

Warszawa, 31 lipca 2023



Wytyczne:
taborowe 2023
infrastr. 04.2026

$$FIL_{SS\&C} = \sin\measuredangle\left(\begin{matrix}8 & 0 & 0\\ 0 & 8 & 0\\ 0 & 0 & 8\end{matrix}, [SF, SC, CS]\right)$$

$$\begin{vmatrix} SF \neq 0 \\ SC \neq 0 \\ CS \neq 0 \end{vmatrix}$$

cyberpoligon

Centrum Technologii Bezpieczeństwa AGH

- **Projekty rozwojowe w programie bezpieczeństwo i obronność**
- **Projekty badawcze dotyczące analizy informacji i poprawy bezpieczeństwa obywateli wspólnoty europejskiej**
- **Usługi dotyczące wytwarzania zaawansowanych rozwiązań wspomagających działalność instytucji bezpieczeństwa publicznego oraz biznesu**

AGH

CENTRUM TECHNOLOGII BEZPIECZEŃSTWA AGH

Umowa o współpracy Instytut Kolejnictwa – AGH

Umowa o współpracy PLK - IK - AGH

100 LAT BADAŃ W POLSKIM KOLEJNICTWIE

przechodzimy
do gorącej
dyskusji

Instytut Kolejnictwa
ul. Józefa Chłopickiego 50
04-275 Warszawa
e-mail: ikolej@ikolej.pl