PROBLEMY KOLEJNICTWA
RAILWAY REPORT Issue 191 (June 2021)
INSTYTUT KOLEJNICTWA
DOI: 10.36137/1915E
ISSN 0552-2145 (print) ISSN 2544-9451 (on-line)

Cybersecurity Guidelines for the Employees of the Railway Entities

Marek PAWLIK[1]

Summary

European Commission has published a nearly 50-page-long document on cybersecurity in transport called the *Transport cybersecurity toolkit*. As part of the work of ISAC-Kolej (the Information Sharing and Analysis Center for the railway transport sub-sector), guidelines in terms of cybersecurity for the employees of the railway entities have been developed and adopted. This article briefly discusses the European and Polish activities taken in order to protect railway transport against cyberthreats and shares the guidelines for employees adopted by ISAC-Kolej. Considering the increasingly widespread use of digital solutions, both for supporting operations of the business entities that constitute the railway system and for railway traffic management and supervision, these guidelines should be disseminated to the maximum possible extent among railway employees that use computers in their work.

Keywords: information systems (IT), operational systems (OT), cybersecurity

1. Introduction

In 2016, simultaneously with the works on the fourth railway package (adopted by the European Parliament in May 2016), works were under way on a directive concerning the measures that would ensure a high level of security for networks and information systems in the EU, i.e. the NIS Directive (*Network and Information Systems security*) [1], which was adopted in July 2016. As a result, on the one hand, the fourth railway package, transposed into Polish law by means of the Act Amending the Polish Railway Transport Act, does not contain clear provisions as to how cyberthreats should be taken into account in the railway system, while, on the other hand, the NIS Directive, transposed into Polish law by means of the Polish Act on the National Cybersecurity System [4] (the NCS Act), imposes in this respect a number of duties on railway infrastructure managers and railway undertakings classified by means of the relevant decisions as operators of the key services.

Currently, nearly all railway infrastructure managers and railway undertakings use digital solutions to support their operations, but only some of them are officially classified, under the NCS Act, as operators of the key services and are therefore obliged to take actions intended to improve cybersecurity. However, it should be pointed out that, at the European level, works are under way on the NIS-2 Directive. The guiding principle is that all railway infrastructure managers and railway undertakings will become, by law, operators of the key services, unless they are micro enterprises, which in the case of railway transport is extremely rare.

2. Who should take care of cybersecurity?

Both the NIS Directive and the NCS Act that implements it impose duties in terms of cybersecurity on a number of entities operating in seven sectors (energy, transport, banking, financial markets infrastructure, health care, supply and distribution of drinking water, and digital infrastructure). In the energy sector, the electrical energy, oil, and gas sub-sectors have been specified, while in the transport sector, these are the air transport, rail transport, water transport, and road transport sub-sectors. In each of these areas, by means of sector regulations, certain business entities have been designated as, and are obliged to carry out the duties of, operators of the key services. These entities have to take actions necessary to ensure a high level of cybersecurity.

[1] Ph.D. Eng.; prof. of the Railway Research Institute, Deputy Director for Railway Interoperability; e-mail: mpawlik@ikolej.pl.

3. Is the threat for railway transport real?

Certain business entities are formally required to take specific actions. However, the question remains: are cyberthreats in railway transport real? Unfortunately, the answer is yes. In November 2020, the European Union Agency for Cybersecurity (ENISA) has published its first report dedicated to railway transport [2]. According to the report, railway transport has been a target for cyberattacks in recent years. The report lists the following attacks:

1. 2015, Ukraine: large-scale coordinated DoS attack from an advanced persistent threat actor, intended to destabilize the Ukrainian government through attacking power stations, mines, and railway infrastructure.
2. July 2015–2016, United Kingdom: intrusion. Four cyberattacks were discovered on the UK railway network, perceived as a reconnaissance by a national state threat actor. No disruption or modification of data was detected.
3. May 2017, Germany: ransomware[2]. Deutsche Bahn was a victim of the WannaCry ransomware. Some devices were corrupted and, due to this, could show no information to the passengers anymore. Train operation was not disrupted.
4. October 2017, Sweden: DoS and DDoS attacks on the Sweden Transport Administration (Trafikverket) via its two internet service providers. The DDoS attack reportedly affected the IT system that monitors trains' locations. It also took down the agency's e-mail system and road traffic maps. Customers during this time were unable to make reservations or receive updates on delays. Public transport operator was also affected. As a result, train traffic had to be managed manually.
5. May 2018, Denmark: a DDoS attack impacted the ticketing systems of the DSB railway undertaking. Travelers could not purchase tickets from ticket machines, online, and from certain station kiosks. 15,000 passengers were affected.
6. March 2020, United Kingdom: data breach. The e-mail addresses and travel details of about 10.000 people who used the free Wi-Fi provided by UK railway stations have been exposed online. The database contained 146 million records, including personal contact details and dates of birth.
7. May 2020, Switzerland: malware. The Swiss rail vehicle manufacturer Stadler was hit by a malware attack that impacted all of its locations and have allowed attackers to steal sensitive company data and confidential documents. The documents were published after the manufacturer refused to give in to ransom demands.
8. July 2020, Spain: ransomware. The Spanish infrastructure manager ADIF has been hit by ransomware not affecting critical infrastructure, but exposing gigabytes of personal and business data.

4. The establishment and functioning of ISAC-Kolej

Since the threats are real and some of the entities obliged to take actions intended to minimize cyberthreats do not have up-to-date information concerning cyberthreats or resources allowing them to make quick use of such information, it is necessary to ensure proper exchange of this information between entities that constitute the railway transport system. This also applies to the materials that allow competences to be built in the particular entities. This is because the attackers do not differentiate between individual entities or even between the particular sectors since they use the same hardware and software solutions. Therefore, in 2020, the Information Sharing and Analysis Center for the railway transport sub-sector (ISAC--Kolej) was established; all railway infrastructure managers and railway undertakings may join. The Center was created jointly by PKP, PKP PLK, PKP IC, PKP Cargo, PKP LHS, PKP SKM, PKP Informatyka Kolejowa, and two institutes: the Railway Research Institute and the NASK Institute.

We hope that, in the future, ISAC-Kolej will ensure the exchange of information, but today, at the early stage, a number of activities intended to organize the cybersecurity area are necessary. Importantly, cybersecurity concerns both information systems (IT) and the operational systems (OT) used for the purposes of railway transport. IT systems and solutions cover both the solutions that support infrastructure managers and railway undertakings in carrying out their general tasks and business operations (e.g. personnel

[2] Ransomware (ransomware – a bundle of ransom words "ransom" and software "software"). Software that blocks access to a computer system or prevents the reading of data stored in it, and then demands a ransom from the victim to restore it to its original state. Ransomware programs belong to the so-called malware.

and property management systems, invoicing systems, group work systems based on IT tools) and solutions that help them to perform the tasks related to railway transport (e.g. systems for creating timetables). OT systems and solutions cover both hard OT, i.e. the electronic components of the control command and signaling, traffic safety systems, and operational communication systems (e.g. computer-operated signal boxes or the European Train Control System) and soft OT, i.e. systems and solutions that ensure transport protection as an add on to traffic safety. Furthermore, both the IT and OT systems use the same type of mechanisms that improve the security of networks and systems. These include:

- organizational and procedural security measures, including systems for managing information security and systems for granting and revoking access rights;
- systems and solutions that ensure the continuity of operation of IT and OT systems, including the systems for creating and using backup copies, hardware and software redundancies, and measures for securing data processing centers against the loss of power or a fire;
- technological security measures, including authentication systems, malware protection, and systems for controlling the processes in terms of data processing and transmission; and
- physical security measures, including remotely controlled locks, CCTV systems, and other systems supporting physical protection.

Defining organization of the cybersecurity area has to take into account exchange of information between business entities that constitute the railway transport system, but also between the sub-sectors of the transport sector, as well as the need to gather and use knowledge from other sectors since the same types of hardware and software solutions are often used. Therefore, the relevant actions are also taken at the national and European levels.

5. Guidelines for the employees of the railway entities

One of the documents recently published is the *Transport cybersecurity toolkit* [3]. This document covers air, water, and land transport, including railway transport. It contains the fundamental information about threats and recommendations for two levels of persons: all employees (regardless of the type of transport) and persons and bodies responsible for the transport cybersecurity (separately for different types of transport).

On 23 April 2021, ISAC-Kolej accepted five-panel guidelines for the employees of the railway infrastructure managers, railway undertakings, the entities in charge of maintenance, and other companies carrying out works for the railway transport. These guidelines are based directly on the European Commission's *Transport cybersecurity toolkit*. They are attached to this article, so they are widely available to employees. The guidelines cover the general nature of cyberthreats in transport and four panels dedicated to threats and good practices, to be used by all employees, with respect to:

- malware,
- (distributed) denial of services (D)DoS,
- unauthorized access and theft, and
- software manipulation.

ISAC-Kolej recommends (to railway infrastructure managers, railway undertakings, entities in charge of maintenance, and all other entities carrying out works for railway transport) that the guidelines are used to build the awareness of all employees. These panels may be distributed via internal networks or official e-mails or may be displayed when employees log in to the corporate network or to services used for company purposes. The statement that people are the weakest link in the system of protection against cyberthreats may sound like a cliché, but this does not excuse the entities responsible for railway transport from taking actions that at least minimize the threats that follow the employees' lack of knowledge. This is why the guidelines for employees are provided on the following pages. We encourage you to follow them to the maximum possible extent.

References

1. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ EU L 194/1.
2. Railway cybersecurity – Security measures in the Railway Transport Sector", European Union Agency for Cybersecurity (ENISA), November 2020, DOI: 10.2824/235164.
3. Transport Cybersecurity Toolkit, European Commission, European Union, 16 Decemeber 2020.
4. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa [Act on the National Cybersecurity System of 5 July 2018], Dz.U. 2018, poz. 1560.

Cybersecurity guidelines for the employees of the railway entities

European Commission
Transport cybersecurity toolkit

Threat Actors

Individuals or organisations may intentionally or unintentionally expose and exploit vulnerabilities, which have the potential of causing incidents and affecting transport services including their safety, security, business, finance and reputation. Threat actors involve, among others, state-sponsored groups, cyber criminals, cyber terrorists, hacktivists, hackers (including script kiddies), and insiders (including privileged insiders).

The most significant malicious actors intentionally targeting transport organisations are **cyber criminals, insiders,** nation states and **state-sponsored groups.**
Adversaries such as cyber criminals conduct massive attack campaigns and are often in the game for monetary rewards.

Insiders, know the singularities of the organisations they work for and are often well aware of subtle security vulnerabilities. Insider threat actors may involve disgruntled employees, suppliers and individual contractors.
As global geopolitical tensions intensify, nation states and **state-sponsored groups** target strategy long-term objectives. They often try to conceal themselves in the depth of organisations' systems and collect sensitive information. Once they establish their foothold into systems, state sponsored attackers look to gain a position that has the potential to create the worst damage possible. For example, they may target other organisations' systems by exploiting the organisations' network connections.

Other threat actors involve insiders, who may unintentionally or accidentally perform actions resulting in cybersecurity events and, in worst cases, cyber incidents affecting the safety and security of transport services.

Emerging Cyber-Threats

There are a substantial number of cyber threats targeting transport: distributed denial of service, denial of service, data theft, malware diffusion, phishing, software manipulation, unauthorised access, destructive attacks, falsification or bypassing of security operator decision process, masquerading of identity, abuse of access privileges, socialengineering, defacement, eavesdropping,
misuse of assets, and hardware manipulation.

Based on comprehensive literature research of publicly available documentations and interviews with experts, the most pressing emerging cyber threats affecting transport are: Malware, (Distributed) Denial of Service, Unauthorised Access and Theft, and Software Manipulation.

Threat #1: Malware

Malicious software that may potentially affect individuals or organisations across transport modes.

Threat #2: (Distributed) Denial of Service

Cybersecurity attacks preventing individuals or organisation access relevant transport services and resources

Threat #3: Unauthorised Access and Theft

Unauthorised access, appropriation, and exploitation of critical assets.

Threat #4: Software Manipulation

Cybersecurity attacks targeting software in order to modify its behaviour & conducting specific attacks.

Threat #1 Malware

Malware consists of malicious software, which may include different types of software applications such as viruses, trojans, worms, ransomwares, cryptocurrency-miners, or any software that may have potentially adverse impacts on organisations or individuals across transport modes.

Mitigating the diffusion of malware designed for intentionally damaging computers, servers, clients, networks, or all of them is amongst the main priorities of cybersecurity across all modes of transport. A typical attack vector may involve phishing emails targeting employees. Other attack vectors may involve different and sophisticated social engineering strategies such as plugging in a USB key into a free port (e.g. charging of mobile phone). By clicking hyperlinks in suspicious emails or opening file attachments, the user may unknowingly be installing software or knowingly jeopardising transport services and resources.

For example, the WannaCry ransomware cyber-attack affected more than 150 countries and infected over 230,000 systems. It involved a ransomware that usually spreads via phishing emails containing malicious attachments or hyperlinks. This type of attack exploits social engineering maliciously in order to mislead system users into installing (or activating) specific malware.

Good practices against Malware

You can help to protect your organisation by following good practices for **identifying and preventing the diffusion of malware**, such as:

❑ **Follow security policies** such as scanning storage media and files for viruses, avoiding opening and emailing specific types of files (e.g. executable files such as .exe, .bat .com, etc.), installing only authorised software, ensuring software (including antivirus) is up to date and functioning properly, and other policies.

❑ **Backup your data** regularly into secure (and authorised) data storage devices or services, which should support encryption mechanisms in order to protect data at rest and being available for data restore procedures.

❑ Protect with suitable **security measures** (e.g. password, encryption, etc.) all systems including mobile and endpoint devices, and remember to lock (physically and digitally) securely all systems if unattended.

❑ Avoid opening attachments and clicking on hyperlinks contained in unexpected emails and suspicious web browser popup windows with a strange body text or from unknown senders and internet domains.

❑ Avoid inserting into your computer **untrusted or unknown removable devices** such as USB sticks, hard disks, and other storage devices.

❑ Avoid disabling malware security measures (e.g. antivirus software, content filtering software, firewall, etc.).

❑ **Update installed software** regularly to the latest available versions (which information security officers or system administrators may release with regular updates).

❑ Avoid using privileged (e.g. administrator-level) accounts and credentials for regular activities and operations.

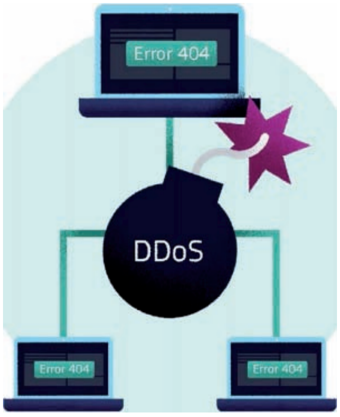
❑ Report to information security officers or system administrators any suspicious email or unexpected system behaviour.

❑ Focus attention on information security among daily routine work in order to recognise IT security concerns and respond accordingly.

Threat #2 (Distributed) Denial of Service

Distributed Denial of Service (DDoS) and Denial of Service (DoS) attacks affect availability and accessibility of data, services, systems, and other resources. These types of attacks can range in duration and may target mare than one service or system at a time. DDoS attacks employ multiple systems (or channels of attack) in order to overload target services or systems with requests. Successful attacks affect service and system capabilities to deal with unexpected volume requests. This results in denying access to services and resources.

Note that affected services and systems belonging to transport organisations may be exploited in order to conduct DDoS and DoS attacks to target specific systems in operations or other organisations as well.
For example, corporate information systems (such as personal computers and devices) may be targeted in order to access operation technologies, which may be connected to the internet or accessing networks in order to transfer
operational data. Connections between different systems and networks (such as corporate networks, operation technologies and remote maintenance accesses) may represent exploitable vulnerabilities for conducting DDoS or DoS attacks to critical transport services and systems. For example, DDoS and DoS attacks can exploit common network and communication protocols such as the Web Services Dynamic Discovery (WS Discovery), which IoT devices may use to automatically discover each node on Local Area Networks (LANs). If IoT devices present vulnerabilities, attackers may exploit them in order to discover other connected devices and conduct DDoS or DoS attacks.



Good practices against (Distributed) Denial of Service

You can help in protecting your organisation by identifying **Distributed Denial of Service (DDoS)** and **Denial of Service (DoS)** attacks. You should contact immediately your security and IT teams if you detect or experience any of the following indicators of potentially ongoing DDoS and DoS attacks for your services or systems:

- □ Increasing requests consuming network capacity (perceived as slow services and responses) resulting in service or system failures due to overload.
- □ Increasing demand of memory resources usage without an obvious reason.
- □ **Unexpected behaviours of services and systems,** frequent crashes and strange error messages due to malicious consumptions of computational resources or network connections.
- □ **Degraded performances** of devices, long executions for trivia/ tasks and noticeable activities (e.g. noisy fan while de vices performing slowly).
- □ **Unexpected internet connections or loss of connections** to services and systems.
- □ Subtle behavioural changes of operation controls or technologies resulting in physical damages.
- □ Denials of accesses to privileged or administrative ac counts in order to block incident response procedures from recovering.

Threat #3 Unauthorised Access & Theft

Threat actors may want to gain logical or physical access without permission to a network, system, application, data, or another resource in order to conduct malicious activities, including theft of sensitive data or resources (including physical resources).

Unauthorised access and theft threats target confidential and proprietary assets (including personal identities, credentials of privileged accounts, systems, and other types of confidential and proprietary information). These threats may exploit systems vulnerabilities as well as unaware individuals disclosing sensitive data such as credentials (e.g. login, password, etc.) or personal data (e.g. email, personal identification number, etc.).

In relation to unauthorised access, identity theft is the illicit use of personal data or unique identifiers in order to impersonate persons or services and systems to gain access to private or proprietary resources (e.g. including financial and physical resources). Such cybersecurity threats may target also physical assets across transport modes.

Good practices against Unauthorised Access & Theft

In order to prevent attacks involving unauthorised access and theft, it is necessary to follow principles such as 'need to know' and 'security and privacy by default: which emphasise that sensitive and confidential assets (including personal and sensitive data, transport systems, etc.) should be accessible only to whom has the right to access them in order to perform their duties. You can help in protecting your organisation by following good practices for identifying and preventing unauthorised access and theft, such as:

❑ Follow security organisational policies.

❑ Avoid sharing and publishing online credentials and personal data, including pictures that may contain such information.

❑ Avoid using or transmitting credentials and personal data (and other sensitive data) to untrusted and unsecure networks, devices or web services (e.g. websites that use unsecure protocols or addresses http:// and not secure ones https://).

❑ **Never reveal to anyone your credentials** (e.g. login and password) even via email or phone.

❑ Protect sensitive data typed on keyboards or shown on screens (including on mobile devices)from unauthorised individuals, install privacy screens, and avoid working from public places with private devices, and avoid leaving any device unlocked and unattended.

❑ **Use complex passwords** (e.g. suff1ciently long password combining alphanumerical and special characters) complying with relevant organisational security policies in order to prevent unauthorised access.

❑ **Change default passwords** of connected systems and devices (e.g. printers, routers, cameras, smart lock, etc.).

❑ Avoid using the same credentials (e.g. login and password) for multiple services and systems, and avoid using the same credentials for services and systems that require privileged accounts.

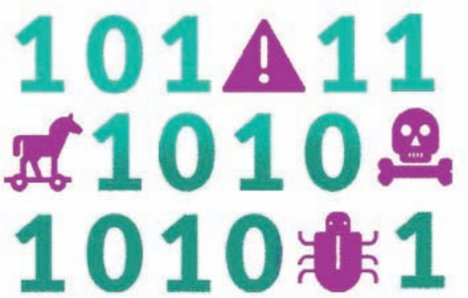
❑ Send passwords and keys for transferred protected files (e.g. ZIP archives) only via an out of band channel (e.g. SMS via GSM and phone call) and never via email.

❑ **Activate Two-Factor Authentication (2FA)** or Multi Factor Authentication (MFA), if possible.

Threat #4 Software Manipulation

Misconfigurations and manipulations of software and related systems or components may have a direct impact on the security posture of transport services and systems. Cybersecurity attacks exploiting software manipulations modify software settings or affect the integrity of data in order to change the behaviours of systems and services. Attackers may intentionally manipulate software (or part of it) in order to gain advantages (e.g. obtaining unauthorised access, preventing legitimate individuals or systems access to necessary resources, collecting sensitive information, changing functional behaviours, etc.) over sensitive assets.

For example, attackers may target communication channels of manufacturers in order to upload malicious software updates on services and systems (including operation technologies) in operations. A threat agent uses compromised authorisation credentials to access a secured remote maintenance network interface in order to install manipulated software and further compromise other accessible services and systems. The threat agent installs manipulated software that further compromises target services and systems, or attacks other connected services or systems



Good practices against Software Manipulation

You can help in protecting your organisation by following good practices for identifying and preventing software manipulation, such as:

□ Avoid installing unreliable software on systems and devices (including personal computers, servers, peripherals, network devices, smartphones, etc.).

□ Always install software and updates from official sources and websites (e.g. producers, corporate repositories, etc.).

□ Avoid downloading software and applications (and any file) from illegal sources.

□ Uninstall unnecessary or not recently used software, and disable unnecessary connections (e.g. network protocols and services) including access to remote services (e.g. cloud storage services).

□ Sean any software or storage devices with a reliable and updated antivirus.

□ Download safe industrial software (e.g. updates, patches, new products, etc.) from trusted suppliers using white station principle.

□ Update all installed software in compliance with organisational policies and practices.