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

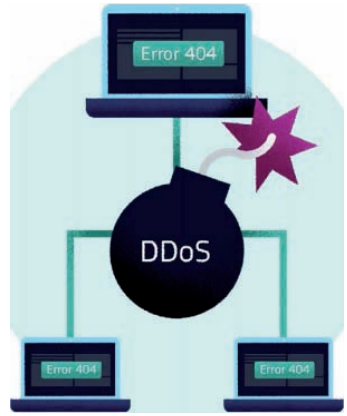
You can help to protect your organisation by following good practices for **identifying and preventing the diffusion of malware**, such as:

- ❑ **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

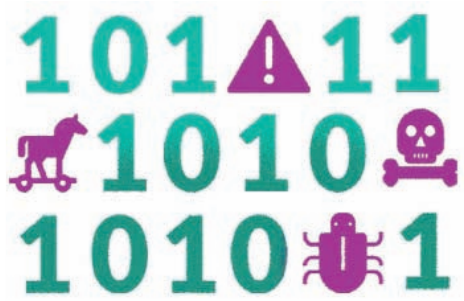
In order to prevent attacks involving unauthorised access and theft, it is necessary to follow principles such as 'need to know' and 'security and privacy by default: which emphasise that sensitive and confidential assets (including personal and sensitive data, transport systems, etc.) should be accessible 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.