CYBERSECURITY ISSUES IN TRAFFIC MANAGEMENT

Alfyorov V.A.,student
Gubareva O.S., PhD, Associate Professor
Kharkiv National Automobile and Highway University

Transportation Control Centers (TMCs) are more resilient to cyberattacks, so you need to know the basics of how to prepare for and respond to an incident. A breach occurs when an attacker can gain access to a secure TMC network. Once an attacker has infiltrated the network, he must find out what is in it in order to attack deeper. Using the same analogy, an intruder is now walking around your house, trying to figure out the layout and finding out where the valuables are hidden. What is important to an operator may be useless to an attacker, and operational support systems can be very attractive. Exit can be an important element of a successful attack.

If an attacker wants to remotely control the operator's workstation, he must establish a data connection outside the TMC. Each agency must have an IT and information security policy that is understood and followed by TMC operators. TMC staff and management must be trained to identify and defend against social engineering attempts. Restoring TMC systems from a backup is a quick way to get back up and running in the event of a catastrophic loss.

The transport industry of our country quickly, safely and reliably transports people and goods across the country and abroad. This sector includes aviation, automobiles and motor transport, maritime transport and railways. As this critical industry becomes increasingly dependent on interconnected digital systems, the risk of cyberattacks increases. Historically, the industry has been more concerned with protecting passengers and cargo from physical threats, but the industry is now facing an alarming rise in cyberattacks.

Educational institutions and cybersecurity professionals must work together to advance security concepts in vehicle manufacturing, product distribution, communications and entertainment systems, and a trusted supplier ecosystem.

According to statistics, between 2020 and 2021, the number of weekly ransomware attacks increased by 186 percent in the transportation industry. Ransomware attacks are on the rise across all sectors, but the brunt of this trend appears to be in the transport industry. Because transport companies have not historically built large security teams to protect their digital assets, they are more acutely affected by the global cybersecurity skill gap than other businesses.

In various experiments to test the reliability of vehicle cybersecurity systems, "white hat hackers" - i.e. computer security experts who deliberately hack into systems to test and assess their security have shown that it is entirely possible to drive cars remotely. For example, back in 2015, such hackers demonstrated that they could take control of the braking and acceleration systems of a jeep, its dashboard, and much more. The mere thought of such a thing is terrifying.

In another experiment on a Tesla car, computer security experts managed to fool the autopilot program and force the car to swerve into oncoming traffic. "Other

incidents, such as those not involving white hat hackers, will also need to be treated with due care and attention," says Dr Gido Scharfenberger-Fabian, project leader on the expert working group. ISO WP 11 dealing with cybersecurity of electrical and electronic components of road vehicles.

Therefore, cybersecurity is big business, especially when it comes to vehicles. According to various estimates, the value of the global automotive cybersecurity market will grow from $2.4 billion in 2019 to about $6 billion by 2025. But, despite the prosperity of this sector, the war against crackers is just beginning.

References

1. ПравіковД.І., ПономарьоваЕ.А., КуприяновськийВ.П.
2. Проблеми забезпечення інформаційної безпеки високоавтоматизованих транспортних засобів.
3. 2. Алабіна Ю.Ф., Уривський А.В., Кабакова Н.В., Чефранова А.О.
4. Системи захисту інформації

TRANSPORT LOGISTICS

Kovalyov V., student
Gubareva O. S., PhD, Associate Professor
Kharkiv National Automobile and Highway University

One of the most important functional sections of general logistics science, directly related to the organization and management of the movement of material flows, is transport logistics. In modern market conditions, transport logistics plays a very important role, since any enterprise interacts with the external environment. In the process of such interaction, objects are moved: raw materials and materials from suppliers to the manufacturer, finished goods from the manufacturer to intermediaries and from them to end consumers. There is a need to ensure the physical movement of such goods in space along the optimal route at the lowest cost. This is exactly what transport logistics is doing.

Transport logistics is a section of logistics dealing with the organization of delivery, that is, the transportation of any material objects (products, substances) from one point to another along the optimal route.

The purpose of transport logistics is to deliver the right goods of the required quality and quantity at a given time and place with minimal costs (i.e., in fact, it is the fulfillment of 6 rules of logistics).

The main tasks of transport logistics are: choosing the type of transport (automobile, railway, air, etc.); choosing the method of transportation (type of transportation); choosing the carrier and other logistics partners; determining rational delivery routes; ensuring the technological unity of the transport and warehouse process; optimizing the parameters of the transport process (increasing the speed of transportation, reducing fuel costs, etc.).

Among all modes of transport, I would like to single out the most popular mode of transport in the world - automobile!