УДК 623.618

CYBER-SECURITY CHALLENGES IN AVIATION INDUSTRY

Агзямов И.И., студент гр.1244, 2 курса
Научный руководитель: Галяутдинова Р.М., к.ф.н.
Казанский национальный исследовательский технический университет имени А.Н.Туполева
г. Казань

The aviation industry has become increasingly reliant on technology, with everything from flight controls to in-flight entertainment systems being managed by computer systems. With this increased reliance on technology, cyber security has become a growing concern for aviation industry stakeholders. Any breach in cyber security could have catastrophic consequences for the aviation industry. This paper discusses the challenges and vulnerabilities facing the aviation industry in terms of cyber security.

Challenges in the Aviation Industry's Cyber Security:

1. Dependence on Technology:

The aviation industry relies on technology for almost everything. Air traffic control, navigation systems, weather forecasting, and flight control systems all require complex computer systems. However, if these systems are not secured, they are vulnerable to cyber attacks. As these systems are connected to the internet, a cyber attacker could potentially gain unauthorized access to the system.

2. Multiple Entry Points:

Cyber attackers can exploit any weak point in an aviation system. For example, computer systems are connected to a variety of entry points such as airport Wi-Fi, mobile devices and personal computers. This makes the system more vulnerable to cyber attacks. Furthermore, third-party applications installed on these devices can also create a security risk, as they may contain malware or unintentionally reveal confidential data.

3. Human Factors:

The aviation industry, like any industry, is vulnerable to human error. A careless or malicious employee can, either intentionally or unintentionally, put the entire system at risk. For example, an employee could accidentally download malware onto the system, putting it at risk of cyber attack. Furthermore, social engineering attacks can be used to trick employees into giving out sensitive information or passwords.

4. Insider Threats:

One of the most significant security risks for the aviation industry comes from insider threats. An insider can be an employee, a contractor or a third-party vendor. They have authorized access to the system and can easily compromise it, either intentionally or unintentionally.

5. Increasing Complexity:

The aviation industry has become more complex with the adoption of new technology. Aircrafts now have Wi-Fi systems and in-flight entertainment systems that are connected to the internet. Moreover, the use of cloud computing is increasingly common, presenting additional vulnerabilities for cyber attackers to exploit.

6. Lack of Standardization:

The aviation industry is made up of many different entities, including airlines, airports, government agencies, and manufacturers. This means that there is no single standard for cyber security, and different entities may take different approaches to security. This lack of standardization can make it difficult to ensure that security protocols are uniform across the industry, making it easier for cyber attackers to exploit vulnerabilities.

7. Economic Globalization:

The aviation industry is also heavily impacted by globalization. The increased mobility of goods and people has led to the development of international supply chains, which in turn create more opportunities for cyber attacks as the security of the systems used by airlines, airports, etc. varies across the globe.

The first step in solving cyber-security challenges is to have strong password policies, particularly for devices used in the aviation industry. Passwords are the first line of defense against cyber-attacks, and they should be complex and changed regularly. It is also important for aviation operators to keep their software updated regularly, and patches applied as they are released. Inappropriate configuration of systems and applications can also serve as an entry point for hackers.

Data protection is also critical in solving cyber-security challenges. There should be strict data protection policies that regulate access to sensitive data. Staff in the aviation industry should be aware of the sensitivity of the information they have access to, and they should be thoroughly trained on data protection policies. The consent of data subjects should also be obtained when their data is being collected, processed, analyzed or transmitted.

Another measure that can be implemented to solve cyber-security challenges is to improve awareness of cyber threats among stakeholders in the aviation industry. All staff should be trained on cyber security measures, and the aviation industry leaders should educate the public on the risks posed by cyber-attacks. This will enable stakeholders to identify threats and report them promptly.

In solving cyber-security challenges, it is also important to have an incident response system in place. There should be a clear chain of command that outlines the roles and responsibilities of all parties. This will enable quick response to security threats, and mitigate their impact on the aviation industry. Incident response should be reviewed and tested regularly to ensure that systems are functioning optimally.

Finally, collaboration among stakeholders in the aviation industry can go a long way in solving cyber-security challenges. Aviation operators, governments and cybersecurity agencies should work together to share information on cyber threats and jointly develop solutions that can be implemented to mitigate the impact of these threats on the aviation industry.

The aviation industry is facing multiple challenges when it comes to cyber security. These challenges are not unique to aviation only, but the consequences of a cyber attack could be potentially catastrophic. The industry must develop new strategies and technologies to mitigate these threats. Collaboration among different entities within the aviation industry is also critical to ensure a comprehensive approach to cyber security. These challenges will need to be addressed as the industry continues to evolve, and technology plays an increasingly critical role in aviation.

Список литературы:

1. Duchamp, H., Bayram, I., Korhani, R.: Cyber-security, a new challenge for the aviation and automotiveindustries. In: Seminar in Information Systems: Applied Cybersecurity Strategy for Managers, pp. 1–4 (2016)

2. Monteagudo, J.: Aviation Cybersecurity – High Level Analysis, Major Challenges and Where the Industry isHeading. Smartrev Cybersec (2020).

3. Bellekens, X., Jayasekara, G., Hindy, H., Bures, M., Brosset, D., Tachtatzis, C., Atkinson, R.: Fromcyber-security deception to manipulation and gratification through gamification. In: International Conferenceon Human-Computer Interaction, pp. 99–114 (2019). Springer

4. Haass, J., Sampigethaya, R., Capezzuto, V.: Aviation and cybersecurity: opportunities for applied research. TRNews (304), 39 (2016)

5. Lykou, G., Anagnostopoulou, A., Gritzalis, D.: Implementing cyber-security measures in airports to improvecyber-resilience. In: 2018 Global Internet of Things Summit (GIoTS), pp. 1–6 (2018). IEEE