Using Aviation Cyber Security Assessment Tools to identify Related Risk Challenges

Sofema Online (SOL) www.sofemaonline.com considers the challenges as well as understanding best practices related to Cyber Security across multiple EASA Domains including Operations, Maintenance, Airports and Air Traffic Control.

Introduction

Aviation, like other sectors that heavily rely on digital technology, is prone to cyber threats. The complexity of aviation systems makes them attractive to potential cyber-attackers, thus requiring robust cyber security measures. Aviation Cyber Security Assessment Tools are designed to identify, mitigate, and prevent security risks. These tools are designed to assess system vulnerabilities and provide recommendations for strengthening cyber security.

European Centre for Cybersecurity in Aviation (ECCSA)

- https://www.cybersecurityintelligence.com/european-center-for-cybersecurity-in-aviation-eccsa-8114.html

- ECCSA is an initiative supported by EASA aimed at increasing collaboration and information sharing amongst aviation stakeholders, a key enabler for implementing a resilient aviation cyberspace.
- ECCSA provides to its members secure means to exchange domain relevant cybersecurity information, such as vulnerabilities as well as cybersecurity events and incidents that might be worth sharing with the aviation community.
- ECCSA's operational team of analysts provides additional inputs to the information shared by the participants, with the aim to facilitate the creation and the management of an aviation cybersecurity threats knowledge and risk picture.

Identifying Related Risk Challenges

Aviation Cyber Security Assessment Tools can identify numerous risk challenges, including:

- **Unsecured Communication Channels:** Tools can help identify weak points in communication channels. Aviation heavily depends on communication between aircraft, air traffic control, maintenance crews, and other stakeholders.
- **Software Vulnerabilities:** Cyber security tools can assess the resilience of avionics software to cyber-attacks. They do this by scanning for known vulnerabilities and testing the robustness of the software against potential attacks.
- **Data Integrity Threats:** These tools can evaluate whether there are sufficient protections in place to maintain the integrity of flight data, passenger information, and other crucial data sets.
- **Access Control:** They can assess whether there are robust measures in place to control access to crucial systems and data. This includes physical access (like access to the cockpit) and digital access (like access to avionics systems).
- **Supply Chain Risks:** Tools can also evaluate whether suppliers and partners adhere to robust cyber security practices, as these entities could inadvertently introduce vulnerabilities into aviation systems.

Cyber Security Best Practices

When using these tools, there are a few best practices to consider:

- **Regular Assessments:** Regularly using these tools can help identify new vulnerabilities that could be exploited. Cyber threats are constantly evolving, so regular assessments are essential.
- **Holistic Approach:** Cyber security tools should be used as part of a holistic approach to security that includes physical security, personnel training, and organizational policies.
- **Multi-layered Security:** Implement a layered security model, where multiple security measures are in place to protect against a variety of threats. If one layer is compromised, others still offer protection.
- **Incident Response Planning:** Ensure there is a robust plan in place to respond to cyber incidents. This plan should be regularly tested and updated as necessary.
- **Education and Training:** Ongoing education and training about cyber threats can help staff identify potential risks and respond appropriately. This includes training on social engineering tactics, phishing, and other common threats.
- **Collaboration and Information Sharing:** Collaboration with other stakeholders in the aviation industry can lead to better threat intelligence and more robust security measures.
- **Secure Software Development Lifecycle:** Follow secure software development practices, including secure coding standards, code reviews, and regular software updates and patches. This ensures that aviation systems are developed and maintained with cyber security in mind.

Next Steps

Please see www.sofemaonline.com and email team@sassofia.com to understand how Sofema Online can support your company’s specific objectives.