IFALPA
The Global Voice of Pilots

Security Briefing Leaflet

16SECBL01 06 December 2016

Cyber Threats

INTRODUCTION

IFALPA has published a Position Paper on Cyber Threats articulating its concern about the possibility of a cyber-attack against an aircraft, ground facility, or other critical infrastructure resulting in unsafe situations or ultimately even loss of life. In this document some guidelines are provided that could help in establishing an environment in which this threat is fully understood and managed and the risk has been brought down to an acceptable level.

GENERAL

The typical commercial flight operation, whether passenger or cargo, generates and requires a large amount of data that is critical to the safe operation of the aircraft. This data is normally stored on computers and transmitted across networks to other computers, both on the ground and on board the aircraft. This transfer of data is critical and integral to the operation of a modern commercial aircraft. Much of the technology and communication protocols currently in use was developed at a time when aircraft were relatively unconnected to the outside world, and therefore most of the systems are not designed to protect the information they carry. Although some initiatives have been taken to improve this, most airborne systems are still inherently insecure.

It is important to understand that the majority of the damage caused by cyber-attacks is suffered by untargeted systems. Malware designed to attack a certain goal, will also penetrate other systems that then are so to speak 'collateral damage'. Therefore, the cyber threat aviation is facing is not only originating from those that intentionally want to bring down an aircraft, but even more from malware that was designed for other purposes.

With this in mind, security should be considered throughout all communications pathways and applications. As with anything, the system will only be as strong as its weakest component. This security should protect data through its entire lifespan, from initial creation to final disposal. The information should be protected not only when in motion (i.e. while traveling on a network), but when at rest as well.

SOFTWARE

Providers of software (including firmware) and operating systems should be able to demonstrate adequate security measures that have the ability to protect from both without and within. Vendors of these systems must provide updates on a regular basis and additional updates that resolve security issues shortly after they have become known.

In addition, applications should be demonstrated to function only in their intended manner. Commercially available "off-the-shelf" applications should be avoided, as they are more easily subject to security issues. Both operating systems and applications need to be designed to be highly resistant to unexpected conditions or unwanted actions initiated by users or by malicious software. Diversification of operating systems may reduce vulnerability.

Running of applications within individual so-called “sandboxes” (virtual protection zones) limits unwanted interaction of software. Anti-virus software needs to be applied and it should be updated as required. Backups need to be performed on a regular basis and stored separately (i.e. without a physical connection to a network).

HARDWARE

Hardware providers need to demonstrate the effectiveness of security measures against cyber-attacks from both within and without. If commercially available, off-the-shelf hardware is used it needs to be regularly evaluated as to its vulnerability and stability. Components need to be protected against physical access.

Storage devices need to be encrypted and secure.

A device that is used for professional purposes should never be used for private means, nor should a private device be expected or encouraged to be used for professional purposes, unless the operating system supports sandboxed application running only, and applications are from certified and trusted sources.

Systems that do not fulfil security and safety requirements should never be connected to secure systems without further security measures taking place.

Highly sensitive systems should be physically separated from the Internet and networks that have access to the Internet. This includes separation of in-flight entertainment systems and their communications from all other aircraft systems.

Facilities housing systems that store, process or send sensitive data should be considered and guarded similar to the requirements applicable to security restricted areas.

DATA PROTECTION (ELECTRONIC AND PHYSICAL)

Data transfer should only take place via a secure and encrypted channel. Internet connections should be avoided where possible. All transfer data, whether via a network or by a physical transfer, should be encrypted and secured.

Message integrity (i.e. no undetected data modification) should be guaranteed throughout the entire transportation/transmission process. Appropriate techniques should be utilized to guarantee that data, transactions, communications, and documents are genuine, parties involved are who they claim to be and they cannot deny having sent or received a transaction.

Access control should be at minimum a two-step barrier and should consist of two of the following things, depending upon the circumstances:

- Something known to an individual (i.e. a password or PIN)
- Something that one owns (i.e. a smart card or security token)
- A biometric such as an iris scan or fingerprint
- One’s physical location (i.e. inside or outside of a company firewall, or proximity of login location to a GPS device)

Data that is classified as personal or that is relevant for the safe operation of aircraft should never be stored, processed or transferred by any system that does not meet the security and safety requirements of this policy.

Network traffic, communications lines and applications should be continuously monitored. Since the majority of cyber-attacks go unnoticed for long periods of time (sometimes many months), forensic analysis should be applied to accumulated data and logs.

TRAINING

Air operators should establish clear training guidelines for all operative personnel (including flight crews and maintenance staff) who interact with aircraft equipment and infrastructure that involves data usage. Such equipment includes, but is not limited to, Flight Management Systems, FANS, ACARS, CPDLC, and Electronic Flight Bags.

The training of flight crew should address:

- Crew awareness of security vulnerabilities,
- How systems can be attacked,
- What precautionary measures could prevent an attack or minimize its consequences,
- What an attack might look like to an operating crew member, and
- Possible actions that may be taken should a crew suspect that their aircraft or any other part of the aviation infrastructure may have been the victim of a cyber-attack, including appropriate contingency procedures and mandatory reporting of all suspicious computer-related occurrences and malfunctions which could be related to a cyber-attack,
- Crew awareness of the fact that sensitive data might be sought or gleaned from social networking sites.

GOVERNANCE AND CONTROL

Security policies and procedures should be established. Roles, responsibilities, and segregation of duties have to be defined enterprise wide. All employees in the organization, as well as business partners, should understand the reasons for restrictions of access to data and the steps required for individuals to be granted this access, and understand the required security controls and handling procedures.

An Information Security Management System (ISMS) should be established, defining a system of processes, together with the identification and interactions of these processes, and their management. The ISMS should include a “Plan-Do-Check-Act” model to ensure that the required level of security is maintained at all times. Attention should be given to three specific areas:

- GRC (Policies, Governance, Risk, Compliance)
- Visibility (Monitoring, Analytics, Incident Management)
- Controls (Security solutions for secure access, encryption, firewalls, network IPs, host and workstation IPs, DLP, etc.)
- Mitigation and Measures to be taken in the event of a successful attack

As part of an ISMS system, all operators, air traffic service providers and manufacturers should be required to designate an individual to serve as a “single point of responsibility”. This person would be the “accountable executive” who would be responsible for their information security policy and procedures and its governance.

Within the ISMS an information security risk management process should be established. Risk assessments of both the own organization and external data providers should be made, to ensure the required level of assurance is provided.

ISO standards of the 27000 series provide detailed guidance in establishing and implementing such an ISMS.

States should establish legislation to make sure aviation related organisations have such an ISMS. This could be done either in separate legislation or as part of the NCASP as governance of cyber issues is pretty similar to that of physical security. Either way it is important the states approve the ISMS and audit the organisations on its application and development.

National legislators should regard all kinds of cyber-attacks towards aviation and its infrastructure as very serious and dangerous acts, and should criminalize them accordingly.

INFORMATION SHARING

In other industries information sharing has proven to be essential in the protection of critical infrastructure. In some countries structures have already been set up also for the aviation industry as well. Aviation SOCs (Security Operations Centre) and ISACs (Information Sharing and Analysis Centre) are structures that may be used to bring participants together. If parties share information on security breaches, detected attacks and best practises the security of the system in total will benefit greatly. To be able to do that confidentiality is key. Partners must be able to trust the information will not be made public in any way, so they can share information freely.

It is very important that all stakeholders participate, and share their knowledge. Airlines cannot reliably determine their risk without detailed information about aircraft systems from manufacturers. Airports cannot determine the risk the air traffic control systems face if their system is breached. Etc.

States should consider establishing a mandatory reporting system on aviation related cyber security incidents, again keeping confidentiality in mind. A coordinated disclosure process will ensure that security weaknesses can be fixed before they are made public. A reporting system would help in finding trends in threats, so appropriate measures can be taken when needed. It would also help in making sure all players in the aviation industry participate in the information sharing effort, and that they implement the necessary monitoring instruments.

Finally, where States have established national cyber monitoring and response structures, be it as a separate organization or as part of the intelligence services, aviation should be included in their scope.

IFALPA provides this data for information only, in all cases pilots should follow their company's guidance and procedures. In the interests of flight safety, reproduction of this publication in whole or in part is encouraged. It may not be offered of sale or used commercially.
All reprints must credit IFALPA.