European Union Aviation Safety Agency

Cybersecurity (General)

What is a cyber resilient aviation system?

Answer

It is a systems that maintains the ability to deliver the intended outcome and the same level of safety continuously at all times, even when regular delivery mechanisms have been attacked.

Last updated:
24/08/2017

Link:
https://www.easa.europa.eu/en/faq/24263

What is a vulnerability?

Answer

A vulnerability is ‘flaw’ or ‘mistake’ in computer-based systems, or a result of an intended feature condition, that may be exploited to compromise the network and information security of affected systems. It provides a point-of-entry or gateway to exploit a system and as such pose potentially severe security risks.

Last updated:
24/08/2017

Link:
https://www.easa.europa.eu/en/faq/24264

What is the European Centre for Cybersecurity in Aviation (ECCSA)? What’s for?

Answer

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.

The 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.

Last updated:
24/08/2017

Link:
https://www.easa.europa.eu/en/faq/24265

What is cybersecurity and how is the aviation system impacted?

Answer

The ever increasing digitalisation of services and devices is simplifying many aspects of our life and improving our well-being as well as offering new possibilities.

However such positive evolution does not come without risk. Individuals may attempt to steal information, manipulate it or disrupt services for their specific reasons, being them economic or political, causing adverse effects to the European citizens.

Civil Aviation is not immune to the so called cyber risks, in fact the whole aviation system is getting more and more digitalised and most of the services essential for flying are becoming highly interconnected.

To this extent aviation stakeholders need to ensure that digital services and devices are capable of withstanding cyber-attacks. The term cybersecurity identifies indeed the protection of the digital information which is exchanged by electronic systems and devices or stored by them.

Last updated:
24/08/2017

Link:
https://www.easa.europa.eu/en/faq/24262

What is CERT-EU, what is its role?

Answer

The Computer Emergency Response Team for the EU Institutions, bodies and agencies (CERT-EU) is composed of IT security experts from the main EU Institutions. The CERT-EU cooperates with other CERTs in the Members States and with specialised IT security companies in order to respond to information security incidents and cyber threats.

A document providing basic information about the CERT-EU, its channel of communication, its roles and responsibilities has been published by CERT-EU and can be consulted. See here

CERT-EU

Last updated:
24/08/2017

Link:
https://www.easa.europa.eu/en/faq/24266

Which structures in aviation are vulnerable to hackers and cyber-attacks?

Answer

All the systems which expose an interface, are connected to the internet, or more in general, are not physically isolated, are likely to be attacked by “hackers”. In light of this, it is of outmost importance for an organization to manage the risk of a cyber-attack. At first by understanding the potential impact and the likelihood of an occurrence and then by implementing controls for the most effective trade-off for security. In general the higher is the potential impact, the lower shall be the likelihood, so controls implementation effort should be prioritised accordingly.

Last updated:
30/04/2018

Link:
https://www.easa.europa.eu/en/faq/46472

What role does EASA play in the fight against cyber-attacks on civil aviation?

Answer

EASA’s mission is to provide the European citizens safe air travel in Europe and worldwide. EASA’s role is to ensure that cyber risks are taken into account during aircrafts design, development and operation and then controlled in order to avoid adverse effects on citizens’ safety. To this extent the objective of the Agency is to incorporate cybersecurity in the existing

safety notion through promotion (training sessions or awareness campaigns), regulatory activities as well as international cooperation.

Last updated:

30/04/2018

Link:

https://www.easa.europa.eu/en/faq/46473

Will cybersecurity and potential resulting safety issues play a more important role in the future of aviation?

Answer

Aviation is evolving, like the majority of other technological sectors, towards digitalization and systems interconnection in order to improve users' experience, provide new services, as well as reduce human errors. The flipside of this evolution is that opportunities for hackers, i.e. the "attack surface", will also increase. To deal with these potential issues, aviation will need to implement a structured approach such as an Aviation Security Information Management System.

Last updated:

30/04/2018

Link:

https://www.easa.europa.eu/en/faq/46474

How are pilots prepared for the growing threat posed by cyber-attacks on commercial aircraft?

Answer

According to a number of articles published in the last few years by representatives of the pilot community, pilots' awareness of cyber risks in aviation is increasing. However, as already mentioned above, EASA is working on a structured approach which, in this case, is the introduction of cybersecurity learning objectives in the pilots' academic training syllabus.

Last updated:

30/04/2018

Link:

https://www.easa.europa.eu/en/faq/46475