Technium Vol. 2, Issue 7 pp.398-404 (2020)
ISSN: 2668-778X
www.techniumscience.com

Development of a strategy for the protection of information resources of the airport

A. Valko senior lecture

National Aviation University, Ukraine, Kiev

pasoshka@ukr.net

Abstract. The article considers the problems of research of scientific and practical activity of the airport complex. It is proved that the aviation security system monitors the activities of the SAB, and quantitative assessment of the level of informatization of aviation security at the airport, emphasizes the need for the management system to protect the concept of creating an independent airport security system. The author argues that the assessment of cyber risks, as one of the components of the synergistic effect of the measures taken against acts of unlawful interference, will prevent cybercriminals.

Key words: airport, factors of influence, cybersecurity, quality management process, intellectual developments and IT, information resources, security, threats.

1. Actuality of theme.

Today, information security is one of most popular topic to discuss in the world. Every day there are attacks on various strategic objects in order to capture certain information about a particular person or organization. New types of attacks, security loopholes, methods of physical and remote access are evolving at a tremendous rate. For many years, from the appearance of the Morris worm to the biggest attacks in 12 years, cybersecurity was something only the technical department could worry about. Corporate leaders saw this as the responsibility of their IT department. Many believed that firewalls, antivirus programs and simple encryption tools could protect against hackers.

Employees believed that this software would be sufficient for security so that they could provide IT security to experts and focus on countless other elements of the business. In fact, the world of technology has changed dramatically over the last 12 years. The information resources of the airport system around the world are under the constant influence of cyberattacks.

2. Literature review

Analysis of recent research and publications conducted in the works of Kina R.L., Rife X., Tamargazina O.A., Linnika II, Kurbeta L.V. showed that the adequacy of the existing set of information and functional products with the ability to perform corrective actions information-functional element at the lowest level, without affecting the general logic of building software for their communication devices (BSCD), when there is a need for a new (unplanned) service, caused either by the emergence of a new task or change the conditions and methods of its solution. Scientists who have studied the issue of cybersecurity in aviation have come to the conclusion that someday they will come to the creation of deterrents, but as the practice of cyberspace shows the creation of attack technology is ahead of efforts to create effective deterrence technology.

So, the goal of this study is to identify the requirements for the defining logical elements in the development of a strategy for the protection of information resources of the airport.

3. Discussion

The problem with traditional security systems (SS) is that they are powerless to detect symptoms of wrongdoing. They will honestly record the fact of the act and take measures to eliminate it. But in the current situation, it is the preventive function of the Security Service of Ukraine that is important. Prevention of security threats is much more effective than their reflection and de facto elimination, when valuable time has already been lost and damage has been caused [1].

The overall level of security of the object depends not only on the use of high-tech systems, but also on the ability of these systems to exchange information in a single database, providing a fundamentally higher level of protection.

The synergetic solution allows to provide comprehensive protection of facilities with the possibility of centralized multi-user management of security functions, including in offline mode, which allows to minimize the cost of equipping the facility by integrating systems of existing infrastructure [2].

According to experts, the global market for airport security and video surveillance, according to analysts, will grow by 9% annually from 2019 to 2024. According to research consulting firm Global Market Insights, the global market for security of airports by 2024 will cost more than 15 billion dollars.

The active introduction of security measures is due to the high demand for such systems, it is easy to see that almost every technological business process uses video cameras, biometric access control, contactless access cards, as well as X-ray scanners with thermal cameras.

The introduction of intelligent development and IT at airports significantly increases the demand for these devices. Examples of such devices are remote flight check-in, various sensors, electronic gates, RFID-luggage processing technologies.

Figure 1: Intelligent development and IT for airports

Most of the data obtained is collected in real time, sent for long-term storage in large centralized databases. With the growth of digitalization, sensoryization and the use of sophisticated computing, airports are becoming objects of cybercriminals. If there are any security issues, statistics can be accessed by attackers from both the outside and inside of the network infrastructure. Wireless technology allows hackers to track the location of any user using various algorithms including information from the Received Signal Strength Indication (RSSI). In addition to real-time data, you can see travel history and even purchase data.

Worms. Viruses. Trojan horses. Logic bombs. Spyware.

Twenty-five years ago, these words have not yet entered the vocabulary of traditional information technology (IT). Over the past few decades, the impact and scale of cyberattacks have changed significantly - to the point that these words are not only part of the general IT terminology, but also part of the weekly headlines.

Robert Morris became the first person to be charged under the Computer Fraud and Abuse Act. In 1988, Robert Morris' "worm" was designed to measure the size of the Internet. Morris created a console command that forced the computer to install the program 7 times, even if the computer reported that the program was already installed. With each installation of the worm, the computers became more vulnerable, which eventually led to complete failure. It was the first denial attack of service (DDoS).

For Maurice, the case ended fairly quickly and successfully - he became a professor of the Massachusetts Institute of Technology, and formed a computer incident response team, which works like a nonprofit research center of a systemic problems that may affect the Internet as a whole.

After Morris' worm, viruses became more deadly and posed a major threat, affecting more and more systems. In light of these developments, the rise in popularity of antivirus began in 1987, and the first specialized antivirus company was released.

However, the Morris worm is not the first cyberattack in history, as it was accidental. And in the first place, a more ambitious and thoughtful attack in 2002 via the Internet was dealt a powerful blow, which became the first in the history of cyberattacks. Targeted at thirteen root servers of the Domain Name System (DNS), a distributed denial of service attack attacked the entire Internet for an hour. Although this did not affect most users, a DDoS attack could disable the Internet if it lasted for a longer period. Never before has there been such a complex and large-scale cyber-attack. [2]

Due to the constant increase in the number of information threats to airports and other large enterprises, the task of ensuring reliable protection of corporate networks from malware and network attacks is increasingly emerging.

Like an instance: on March 10, 1997, a hacker penetrated the control system that used to communicate the air traffic control system in Worcester (Massachusetts), causing a failure of system that cut off the phone for six hours. This has particularly affected the telephone system of the control tower, the airport fire service and airport-based airlines.

In 2016-2017, Ukraine experienced powerful cyberattacks for the first time, when the operation of critical transport infrastructure facilities and many other enterprises was blocked for some time. On January 16, 2016, the computer network of Boryspil airport was infected with the Black Energy virus (computer network workstation), which may indicate a sabotage by the Russian Federation. Other key sectors have also been hit by targeted attacks.

Information security is not only the protection of the system and data from network attacks, it is also a set of precautions against physical attacks, theft of information and damage to information collection and storage systems.

Cybersecurity - a set of tools, policies, security measures, manuals, safeguards and technologies used to implement measures to protect systems, networks and software applications from digital attacks.

The International Civil Aviation Organization (ICAO) constantly encourages stakeholders and States to encourage the coordination of information protection strategies, to develop common ways to identify and address critical vulnerabilities through the systematic exchange of information on threats and incidents.

The following normative documents have been developed in this direction:

A. European Standard (EN) 16495 for air traffic management is an information security guide for organizations supporting civil aviation operations.

B. International Society for Automation (ISA) / International Electrotechnical Commission (IEC) - 62443 - a set of standards, reports and other information defining procedures for the implementation of safe industrial automation and control systems.

C. National Institute of Standards and Technology (NIST)is the special publication 800-53 on security and privacy measures for federal information systems and organizations.

D. The NIST 800-82 Industrial Management Systems Security (ICS) Guide is a guide to the threats and vulnerabilities of the systems used. [5]

Most modern airports have robust systems to deal with known types of cyber threats. Basic (basic) approaches to controlling and preventing attacks are also used:

1. Organizational arrangements
2. Physical activities
3. Technical measures

The list of threats, estimates of the probability of their implementation, as well as the model of the violator are the basis for risk analysis of threats and the formulation of requirements for the protection of the airport system. In addition to identifying possible threats, it is recommended to analyze these threats based on their classification on a number of grounds. Each of the classification criteria reflects one of the generalized requirements for the protection system. Currently, when building a threat model, different versions of the models developed by experts in the field of information protection of public and private research institutions are used. Based on the analysis, all sources of threats to the security of information circulating in the corporate network can be divided into three main groups:

1. Threats caused by the actions of the subject.
2. Threats caused by technical means.
3. Threats from natural sources.

To ensure comprehensive security, it is necessary to make both organizational and technical decisions to counter situations that threaten information security. This approach allows a differentiated approach to the distribution of material resources allocated to information security. [6]

Each threat entails a certain damage - moral or material, and protection and counteraction to the threat are designed to reduce its magnitude, ideally - completely, real - significantly or at least partially. But this is not always possible.

The security system is ensured by the operation of such nodes as:

● Computer security. The work of this unit is based on the adoption of technological and administrative measures to ensure the quality of all computer hardware systems, which allows you to create a single integrated, accessible and confidential resource.

● Data security is the protection of information against careless, accidental, unauthorized or intentional disclosure or hacking.

● Secure software is a set of application and universal software tools designed to ensure the safe operation of all systems and secure data processing.

● Communication security is ensured by the authentication of telecommunication systems, which prevents the availability of information to outsiders, which can be transmitted by telecommunication request.

ImmuniWeb experts have studied the security of the world's 100 largest international airports. As a result, only three airports have demonstrated compliance with numerous researchers' requirements: Amsterdam Schiphol Airport, Helsinki-Vantaa Airport in Finland and Dublin International Airport in Ireland.

Security checks included tests of public sites, official mobile applications and the search for leaks of confidential data of the airports themselves or their passengers through cloud services, public repositories and the darknet. Yes, ImmuniWeb experts checked:

- correctness of HTTPS implementation;
- supports airport mail server SPF, DKIM and DMARC;
- updated or CMS site to the latest versions and do not contain vulnerable components;
- whether PCI DSS, NIST and HIPAA systems coexist;
- the presence of WAF in airport systems;
- correctness of cookie, header and so on settings;
- the presence in mobile applications of components that are vulnerable to known exploits;
- whether mobile applications rely on third-party libraries and frameworks;
- mobile applications use basic security settings and use dangerous coding techniques;
- whether airport-related data was available in public cloud storage services;
- whether airport-related data was available in public repositories;
- whether airport-related data was available on the darknet and on hacking sites.

As a result, the inspection showed that 97% of airports have some problem with cybersecurity. And most of the shortcomings were found on their sites. [3]

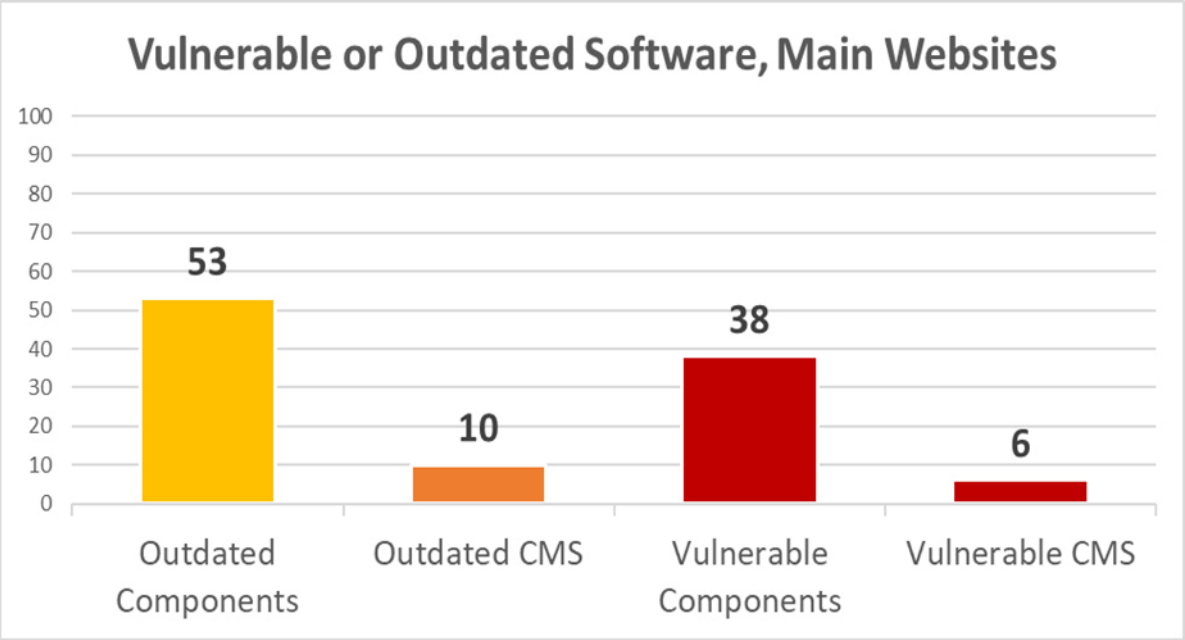

Figure 2: Disadvantages in the work of airport sites [6]

Site issues:

- 97% of sites work with outdated software;
- 24% of sites contain known vulnerabilities;
- 76% and 73% of sites do not comply with GDPR and PCI DSS;
- 24% of sites do not have SSL encryption or use outdated SSLv3;
- 55% of sites are protected by WAF.

Mobile application issues:

- 100% of mobile applications contain at least 5 external frameworks;
- 100% of mobile applications contain at least 2 vulnerabilities;
- on average, one application contains 15 different privacy issues;
- 33.7% of outgoing mobile application traffic is not encrypted.

Data leakage:

- data of 66% of airports can be found in the darknet;
- 87% of airports have data leaks in public storage;
- 503 of the 3,184 leaks have a critical or high risk that could potentially lead to breakage;
- 3% of airports operate with an unprotected public cloud with confidential data. [3]

The risks posed by the use of public WiFi hotspots should be considered as a source of danger, which allows the use of MITM-attack. If you follow simple safety rules, subject to a number of inspections, it is possible to reduce the risks to a minimum:

Carry out authentication - make sure that the access point belongs to the cafe / airport / shopping center, not the hacker. Legal asks to enter a phone number and sends an SMS to login:

- use a VPN connection to access the network. It was actually invented to safely access the Internet through dangerous access points;
- if you do not know how to perform paragraph 1 and paragraph 2, it is better not to transmit data through such a connection, and use the Internet only "in read mode" - to visit sites and services where you do not need to report anything. [6]

At the state level, a national cyber security strategy has been implemented since 2018. Currently, 5 national cybersecurity centers are being built, and sectoral and regional centers are being established. Also, in Ukraine, the State Service for Special Communications and Special Forces in law

enforcement agencies, such as the cyber police in the Ministry of Internal Affairs, deals with cybersecurity.

The Security Service of Ukraine comprehensively and operatively counteracts cybercrime and hybrid aggression against our country. And now SBU employees have reported on their activities in 2019. According to Informator Tech, referring to the SBU press service in 2019, SBU information security specialists neutralized more than 480 cyberattacks on public authorities and critical infrastructure. [5]

The Doctrine of Information Security of Ukraine stipulates that the national interests of Ukraine in the information sphere include such vital interests of the individual as:

- ensuring constitutional human rights and freedoms to collect, store, use and disseminate information;
- ensuring constitutional human rights to the protection of privacy;
- protection from destructive information and psychological influences.

Although modern approaches to airport security involve increasing the number of controlled borders and more sophisticated threat detection technology, airport services are both responsible for managing operational efficiency and passenger service, not to mention security at airport terminals and adjacent areas. Security professionals must be aware of technology, be prepared to prevent various threats.

Given the experience of world best practices, information security in Ukraine should be considered as a system consisting of four components: legal, technical, communication and educational.

Blockchain, a technology that links records using cryptography (secure communication), has already been tested in airline and airport operations. Perhaps the most important application of the blockchain is the storage of biometric data about passengers and ensuring the unimpeded movement of passengers. At the airport, technologies have a huge potential that allows you to create joint projects and share real-time data between stakeholders at airports.

Sensoryization and data analysis. The screening of passengers goes beyond the security checkpoint and will pass through the terminal (and beyond, linking with the vision of "Safe City"). The goal is to create a decentralized security model with sensors that analyze multiple datasets throughout the passenger's journey.

Now there is no doubt that the situation with cybersecurity is only getting worse. Experts believe that cybersecurity will be the main topic of 2020. According to the results of the report "Increasing cyber resilience in aviation: industry analysis" at the World Economic Forum (WEF) in 2020, emerging problems of cybersecurity in the aviation industry were considered. [3]

According to UATV, € 40 million for cybersecurity and medical rehabilitation has been provided to Ukraine by NATO.

Cloud services are one of the priority areas of investment in the next three years. Up to 95% of airlines and 85% of airports plan to invest in them, thus reinforcing the upward trend, which was pointed out in 2015 by SITA. The direction mentioned by both airlines and airports is self-service systems for passengers.

Providing mobile services is another area of airline activity. Ensuring uninterrupted service is of great importance for airlines: 94% of them assess the optimization of service on the basis of a single application as a priority, more than 97% of airlines plan to do so by 2021, and 58% - as a task with a high priority. Mobile applications are evolving rapidly, both in terms of functionality and ease of use, and more and more airlines are planning to turn mobile devices into a tool for passenger service, including service in times of downtime.

Airport operators pay great attention to improving the quality of service at all stages of the passenger's passage through the terminal and to solve this problem are constantly exploring the opportunities that open up some new technologies like the Internet of things, beacons and sensors. A study by SITA indicates that 80% of airports are already investing in these technologies or plan to make such investments in the next three years.Investment in the system of passenger orientation at the airport reaches up to 74%, and in the system of solutions individual service 68%.

Fortunately, airports and airlines have a chance to protect themselves by simply assessing cyber risks and taking appropriate measures to prevent leaks and intrusions into corporate networks. If

airline executives are satisfied that they have taken all necessary measures to protect the airline and its employees from the ever-advancing methods of cybercriminals, the "quality of airport services" can meet the system of socially significant services in strict accordance with ISO 9001 quality standards. current needs and environmental factors, it will protect operating systems and processes to ensure business continuity.

4. Conclusion

The system of protection of potential and real threats is not constant, as they can appear, disappear, decrease or increase. All participants in the relationship in the process of information security, whether human, state, enterprise or region, are multi-purpose complex systems for which it is difficult to determine the required level of security.

The basic conditions for the proper functioning of the airport information security system can be achieved by organizing the process so that the leakage of any information from the repositories was impossible and attackers could not use it for their own purposes, which will lead to an independent airport security system. Achieving this goal requires a lot of time, effort and resources, but the main task, without which the goal will be impossible, is to attract not just the security service, but in addition all personnel in the process of security and safety.

All protective equipment used must be accessible to users and easy to maintain. Each user should be given the minimum privileges needed to perform a particular job. The security system must be autonomous. It must be possible to disable the protective mechanisms in situations where they are an obstacle to the work. The maximum degree of hostility of the environment is taken into account, ie to assume the worst intentions of the attackers and the ability to circumvent all protective mechanisms. Also, the availability and location of safeguards should be confidential information.

In 2021, one of the main factors in the growth of IT costs will be the replacement of the airport's outdated IT infrastructure. The CORONAVIRUS-19 has been a catalyst for change that encourages spending more on the technology needed to maintain and ensure aviation safety.

Over the next two years, large airlines (over 1,000 employees) will implement selected new technologies 5 times faster than small businesses (1-99 employees). In addition, large enterprises will implement IT automation technologies, virtual reality, peripherals, containers, 5G and VDI, with increasing costs for airlines for cloud and managed services.

References

1. Ovchenkov N.I. Airport security threats: better prevented than eliminated. *Airport Partner, № 6, 2004.- p.4-6*

2. Ovchenkov N.I. Who is warned, is armed, or how to ensure the security of the airport. *Transport safety and technologies, №1, 2005.-P.72-74*

Websites:

3. https://tech.liga.net/technology/novosti/97-iz-100-krupneyshih-aeroportov-imeyut-plohuyu-kiberbezopasnost

4. https://www.securitylab.ru/news/512365.php

5. https://www.anti-malware.ru/analytics/Threats_Analysis/2018-cybersecurity-statistics

6. http://www.iksmedia.ru/news/5436874-.html#ixzz6UNI1cks1