DRAFT SECURITY SOLUTIONS THE AEROSPACE BUSINESS BEFORE CYBERCRIME

Michaela Bodnárová – Miroslav Štancl

Privacy is solved in SR Act. 428/2002 Coll. and is directed mainly against cybercrime attacks on information system. The development of information technologies brings new concomitant potential risks to information system attack. To prevent and elimination distortions system, each airline company sets security objectives and establishes a security project. The project involves safety regulations intended to safeguards privacy. For the event breach of the system specific security procedures are developed. Work with personal details may performed only the person responsible for compliance with the laws, regulations and internal security measures airline company. The issue is still current and extensive, creating open discussions.

Keywords: personal data, information system, security guidelines, security precautions, security project

1 INTRODUCTION

The importance of protecting personal data and other sensitive information in companies and firms increases with increasing amounts of applied information technology. The same time develops and grows the crime called cyber crime and its possible risk of distortion. There are several international and national norms, standards and regulations regarding data protection and information. The most important legislation in the Slovak Republic, which concerns the protection of information Act No. 428/2002 Law Code on the protection of personal data. Topic of information security and cyber-crime is still an interesting and current, raising questions regarding the security of information systems and areas of interference. After identifying the problem, an airline company starts drafting safety procedures and take measures to address the problems of the information system.

2 BASIC STANDARDS OF INFORMATION SYSTEMS SECURITY

Nowadays, every small company or large organization uses modern information technology for its operation. Information processing, distribution of information within the organization and beyond the use of updated information of a confidential or public character to all levels of management, it is only part of the use of information systems and information. This information may be in various forms, such as reasons. as electronic files, software files, data files, music recordings, photographs, conversation via e-mail, fax, etc.. All the forms in which the information might be, are threatened by a variety of risks. Due to the different possibilities of information security threats, any organization protects at least basic standards of safety information system. Standard technical term in the applicable standard expressed. It is usually formed as an official document of engineering or technical criteria, methods, processes or practices. Standards security of information system can be:

- National standardization organizations and professional organizations issuing standards
- International standardization organizations
- Private institutions

2.1 TRUSTED COMPUTER SECURITY EVALUATION CRITERIA (TCSEC)

In 1983 this document became the first attempt to create the conditions for the protection of sensitive data and information systems security under the name Orange Book U.S. Department of Defense. Safety of system according to TCSEC document prevents leakage of sensitive data and maintain confidentiality of data. Document does not concern individual components but the coherent information systems and distributed computer systems to four basic classes (A, B, C and D) and their subdivisions regard to the safety systems.

2.2 BRITISH NATIONAL SAFETY STANDARDS BS 7799

The emergence standards and implementation in validity since 1995 and it leading economic organizations. Is an effective tool for the evaluation of information security management systems. Development of new trends in the world in 1998 to adapt to the new requirements of the standard in 2000, the British standard was lifted up to the standards ISO standards. Standard of information security BS 7799 is divided into 2 parts:

- BS 7799-1: 1999 Handbook of procedures for information security management

- BS 7799-2: 1999 Information Security Management Systems - Specification with guidance for use

2.3 INTERNATIONAL STANDARDS ISO / IEC 17799

This International Standard deals with the general principles and the principles relating to the initiative, introducing and improving information security management in organizations. The standard provides general guidance for addressing information security management and control objectives of requirements provides guidance on the preparation and development of security standards in the organization. Gradually, in 2007, the name ISO / IEC 17799 as the name ISO / IEC 27002

2.4 INTERNATIONAL STANDARDS ISO / IEC 27000

ISO / IEC 27000 is very well known by the form of implementation of Information Security Management System, ISMS. This applies to all sectors of industry and commerce, it is not limited to data stored in electronic systems, but the security of information in any form. The standard provides a model how to create, implement, operate, monitor, examine, maintain and upgrade the ISMS. Then help protect the information assets and provide confidence to stakeholders, including the organization and customers.

2.5 INTERNATIONAL STANDARDS ISO / IEC 13335

This standard provides guidance relating to management of IT security resources, which should be familiar for workers who are in the organization responsible for IT security. It is a kind of guide for the organizations to create and implement a security system. Its aim is to identify the relationships of IT in general and IT security management. Offer several models to explain the IT security and create a general directive on the management of IT security. The negative is that it only focuses on addressing the security of information technology, so it is used mainly as a supplement to other standards.

3 SECURITY POLICY IN AIRLINE COMPANY

Ensure a stable, safe and efficient functioning of the airline company is currently are required ensure use all resources . Practically no current distributed security system was designed as an integrated whole. This creates a basis for compliance with applicable legislation and specified conditions.

3.1 LEGAL LEGISLATION AND IMPORTANT LAWS RELATING TO SECURITY OF AIRLINE COMPANY

Privacy and security in an company is devoted to a number of documents such as The Charter of the United Nations, European Parliament and the Council on the protection of individuals with regard to processing of personal data and on the free movement of such data, the Constitution of the Slovak Republic and other Slovak laws.

LAW No. 428/2002 LAW CODE OF PRIVACY

Is an important law at SR that deals with privacy issues in the processing of natural persons, the principles of personal data processing, security of personal data, the protection of the persons involved, the flow of personal data beyond the borders of other countries, as well as the registration and recording of information systems. Processing of personal data may only be a mediator with the consent of the operator and the person on exactly the intended purpose, which is not contrary to law. According to § 16 of this Act, the company prepares its security project.

Law no. 312/2010 Law Code of. on standards for information systems of public administration

The law establishes technical standards for information systems, standards for accessibility and functionality of websites, standardized terminology of electronic services, security, data standards and the standards of project management. Disruption of the above-mentioned standards may result in disruption of the entire information system in an enterprise or organization. In order to avoid disruption, the company has developed a security policy according to § 28 of this Act.

Criminal Law and Cybercrime

In spite of various safeguards and security procedures there is a distortion information system security and cyber crime, which is a modern crime. Differs from the classic crime offender and anonymity that can be committed in the distance. The Slovak law legislation is a law that deals specifically on Cybercrime, but some paragraphs in this modern form of crime is closely related to Criminal Law. 300/2005 law code. The object of the law is the responsibility for the offense, types of sentences and types of protective measures as are stored, and what elements of the crime and what penalties are imposed for commission of the offense. Under this Act, the cybercrime can be divided according to three aspects:

1. computer piracy - infringement of copyright

2. damage or misuse of the information at recording medium

3. Other computer-related crime - as a means to commit a crime

Ensuring normal operation and trouble-free IS, communication, transmission or storage of data without violation system, its task to each IS system administrator. There are several factors that may affect the safety IS with important activities and the fight against crime on the IS is primarily prevention, followed by the repression and the last step is to repair.

Copyright Law

According to § 6 of the Act. 618/2003 law code of. the author is a natural person who chose work or hosted his content. This law deals with relations associated with works of sound recordings, moving image, which are known through radio or television. The law is a special law designed to databases that can be used only with the consent of the author and for exactly the agreed purpose.

3.2 SECURITY STRATEGY AND BUSINESS OBJECTIVES

The concept of safety and security policy are the basic business documents of company that define the essential safety requirements and regulations to ensure the protection and security of data and information. Ignorance, wrong identification of the problem, but also suitable precautions are the cause of reducing the functionality of the information system, therefore is creating a security policy. It is a document in writing that answers the following questions:

- What company wants to protect
- Why company wants to protect
- How and in what way wants to protect
- How to verify that it is really protected
- How will management do if the discovery of vulnerabilities and subsequent failure, and tin order to avoid failure is neccesary to continuously review and improve the components.

Security policy is understood as a set of safety principles and rules that define how security and protection of sensitive data distribution, data and other resources of the organization. Ensuring safety, continuous and reliable operation of IS can be at three levels, namely organizational, logical and physical.

Security objectives, strategy and policy entail benefits for the overall effective functioning of the company. It is a way of information handling, quick recovery and renewal of IS from incurred problems, but also ensure not to repeat the known bugs. Security objectives indicate to the data routing, software, hardware, or documentation of people in the business, that form assets constituting security-by-security according to areas in the company. These objectives are to ensure the protection and are determined in two ways:

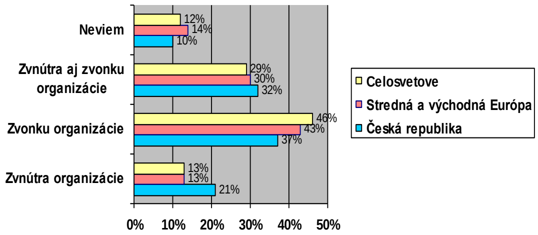
- minimization of disturbance of assets
- Minimizing potential losses by disruption assets

4. MOTION SECURITY DIRECTIVE OF INFORMATION SYSTEM BY MANAGER AIRLINE COMPANY FOCUSING ON CYBERCRIME

Proposal for information system security is not simple. The findings, which occurred companies dedicated to creating surveys in enterprises can help with design of security directive IS Manager airline company.

4.1 SURVEY OF INFORMATION SECURITY AND SURVEY THE FORMATION OF RISK FROM THE CYBERCRIME IN COMPANY

Cybercrime also addressed the Global Economic Crime Survey, conducted by PwC. The survey in 2011 highlighted the increasing risk of computer crime, impact and implications that entails. The following graph shows the results from approximately 4,000 respondents worldwide.



Graf. 1Where does the greatest risk in organizations

Based on the surveys, it was found that an understanding of the importance of information security should be a primary objective of business and should be given a higher importance. Solve problems with disruption of IS and computer crime can be based on safety measures and safety directives that will be respected company.

4.2 INFORMATION SYSTEM AND ANALYSIS ITS SECURITY

Information system is complex, consisting of people, technical tools and methods to ensure the collection, transmission and processing of data. IS usually contains information with at least one or more personal data may be processed in the form of card indexes, lists, registers, which mainly consists of writings, documents, contracts, evaluations, tests, etc.

The risk analysis

Define the term risk may be as danger, high degree of probability of failure and risk analysis can be defined as the probability that the insured event occurs in IS. The objective of risk analysis is to propose a system of such security measures that will be able to identify the assets company, determine their significance, to find potential threats, assess the current method of protection and measures to determine the extent of the risks and their minimize to the lowest acceptable level. With analysis risks are associated in particular the identification of assets and identification of threats and different methods to achieve the objective.

4.3 SECURITY DIRECTIVE AND SAFETY PRECAUTIONS FOR AIRLINE COMPANY

The increasing trend of crime in the IT field had a negative impact on many small companies as well as large organizations. Effects of these problems gradually began to notice governments around the world and started to pursue this issue. The result of solving computer crime problems for enterprises was achieved improving the security of their systems with which employees work every day, and which are exposed to danger. Component of any security project for the protection of personal data and sensitive information is a safety directive and other documents necessary for them to comply with the law no. 428/2002 law code of privacy.

Safety precautions are created especially to:

- Have prevented unauthorized access persons to personal data processing, manipulation with equipment intended for the processing of personal data and the handling of personal data carriers.
- Operator authorized persons have access to the necessary extent of personal data to perform their duties.
- Ensure IS ago by inappropriate modifications of system and adhere to a regular data backup.

Responsibility for the security of personal data

The person responsible for the security of personal data is dealt with in the Act. 428/2002 law code, § 15 Responsibility for the security of personal data. Part of § 33 of the Act is dealt oversight the protection of personal data carried out by the Office for Personal Data Protection. Safety of personal data under this Act, activities under the responsibility of the operator and facilitator. These people protect data against theft, loss, damage, unauthorized access and change through technical, personnel and organizational security measures.

Technical measures

Among the technical measures are includes all the technical resources (assets), which are intended for processing, handling, archiving, but also shredding of sensitive data. The focus of the technical security measures IS relates to the physical protection of IS through appropriate tools and appropriations.

Organisational measures

Organizational arrangements are legal standards, rules or regulations that govern the activities of individual departments. They focus on the processing, storage, handling, retention and disposal of personal information. The aim of these measures is to establish a file of conditions which determine the rules for access to sensitive data. The measure must be built on the basis of existing legislation.

Personnel measures

The objective measures of information system to ensure the protection of personal data in the airline company is to reduce the risk of human error in data protection. Processing of personal data or other sensitive information in an enterprise is permitted only to authorized persons for the job can use technical means or organizational means, according to Law no. 428/2002 law code of protection personal data. In the event of a leak or suspected leak of IS are required this to notify the responsible person.

Procedures at security incidents and other emergencies

The emergence of each of emergencies requiring safety procedures under which it is necessary to solve the situation. Individual procedures with preventive measures to help prevent, the spread of the problem and can provide IS to restore the original state which was before the crash. Solution proposal depends on the particular potential accidents that may occur.

5. CONCLUSION

Important significance of today time is information security relating to the protection of all information assets of the enterprise, technology, and the information system connected to the network. The businesses adopt safety measures mainly against modern crime, which is cybercrime. Efficient, safe and stable system must ensure the protection of its assets and ensure the development, robustness, security, stability and strength of the entire operations of the company.

Each company developes security policies, security objectives achieve a security project that ensures normal operation of IS. None of the ISare completeely safe and attack threats can occur at any of them. Tools to create a draft of solutions security airline company before illegal activity may serve different surveys from companies, current legislation, standards or regulations. The first and most important step in protecting IS is prevention. You need to know what to protect who or what it may jeopardize the safety and as a result design one how it will protect. In the wake of exceptional events the security project in companies established safety procedures that are accurate, staffed with responsible persons knowledgable of procedural steps to restore the system to its original state. With the development of the times it is necessary elaborate security measures and procedures in companies renew in order to eliminate possible risks of disruption.

BIBLIOGRAPHY

[1] GALANDA, J. Bezpečnosť IS [online]. Elektronická dokumentácia k predmetu, LF TUKE, 2010. Dostupné na internete: <www.moodle.leteckafakulta.sk>
[2] MEZINÁRODNÍ CERTIFIKAČNÍ A VZDĚLÁVACÍ SPOLEČNOST PRO INFORMAČNÍ BEZPEČNOST. BS 7799/ISO 17799. [online]. Dostupné na internete: <http://www.cis-cert.cz/iso-17799.php>
[3] THE ISO 27000 DIRECTORY. An Introduction To ISO 27001. [online]. Dostupné na internete: < http://www.27000.org/iso-27001.htm >
[4] ÚRAD NA OCHRANU OSOBNÝCH ÚDAJOV. Legislatíva. Právne akty. [online]. Dostupné na internete: <http://www.dataprotection.gov.sk/buxus/generate_page.php?page_id=902>
[5] Zákon č. 428/2002 Z. z. o ochrane osobných údajov
[6] Zákon č. 312/2010 Z. z. o štandardoch pre informačné systémy verejnej správy
[7] Zákon č. 300/2005 Z. z. Trestný zákon
[8] Zákon č. 618/2003 Z. z. – Autorský zákon
[9] Počítačová kriminalita pod lupou. [online] Česká republika, 2011. Dostupné na internete: <http://www.pwc.com/cz/en/hospodarska-kriminalita/assets/Crime_survey_CR_czech_ele.pdf >

AUTHOR ADDRESS

Michaela Bodnárová, misenkabodnarova@gmail.com
Department of aerodynamics and simulations,
Aviation faculty
Technical University in Košice,
Rampová 7,
041 21 Kosice

Ing. Miroslav Štancl, miroslav.stancl@tuke.sk
Department of aerodynamics and simulations,
Aviation faculty
Technical University in Košice,
Rampová 7,
041 21 Kosice