Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 104 (2017) 35 – 42

Procedia Computer Science

ICTE 2016, December 2016, Riga, Latvia

System Integration and Security of Information Systems

Andrii Boiko[a], Vira Shendryk[a,]*

[a]*Sumy State University, 2, Rymskogo-Korsakova st., 40007 Sumy ,Ukraine*

Abstract

The frequency of unauthorized actions to information systems (IS) in the process of their integration is steadily increasing, which inevitably leads to huge financial and material losses. According to statistics, internal users of IS, commit more than half of all violations. All of this forms "a dangerous group of risk ". Existing approaches for IS security are mainly provided by specialized tools of differentiation of user access to information resources. At the same time each user is assigned certain rights, in accordance with which it is permitted/prohibited local access to information is stored in PC, or remote access via communication links to information available on other PC.

After analyzing we identified 2 major vulnerabilities: tools of differentiation of local access are not able to provide protection against the actions of offenders are not directly related to obtaining unauthorized access to IS resources and tools of differentiation of remote access does not provide protection from network by internal users of the system.

The results of this research will lead to an improvement of the process of ensuring effective protection against threats to information security in the IS.

Keywords: Information system; Intrusion detection system; Behavioral method; Signature method; Security of information systems

1. Introduction

In recent years, the frequency of unauthorized actions into information systems (IS) is constantly increasing, which inevitably leads to huge financial and material losses. There is an interesting fact; more than half of all violations committed by the company’s employees, i.e. internal IS users.

* Corresponding author.
E-mail address: andrii.a.boiko@gmail.com

doi:10.1016/j.procs.2017.01.053

It is known that last few years, IS protection from insiders is mainly provided by specialized tools of the differentiation of user access to information resources. With the help of these tools to each user are assigned specific rights, in accordance with this it is permitted (or prohibited) local access to information are stored in computer, or remote access via communication links to information on other computers[1].

Still it must be noted that this approach does not solve the whole problem of information sources protection from intruders are operating inside IS. This is caused by two main factors:

- Tools of differentiation of local access are not able to provide protection against the actions of offenders who are not directly related to obtaining unauthorized access to information system resources. For example, the user can intentionally install and run the malicious software on own workstation that allows to capture and analyze network traffic in the IS. Another example of the unauthorized activity when protection can't be ensured by tools of access control is data recorded to external devices or the printing of confidential information to which the user has legally access. To identify such actions in IS should apply the system of workstation active monitoring
- The tools of differentiation of remote access does not provide protection from network attacks that can be performed by internal users of the system. Such attacks are based on vulnerabilities that may happen in software-hardware server and desktop stations of IS. Examples of vulnerabilities are unstable passwords, incorrect software configuration, errors are presented in the application software, etc. The success of the network attacks can lead to a breach of confidentiality, integrity or availability of information in the system. To timely detect and block such attacks should be used detection tools, known as IDS-system (Intrusion Detection Systems)[2].

On this basis, it should be highlighted the main tasks of research:

- The development of organizational measures are needed to meet the requirements of data protection, organizational and administrative documentation projects
- The ensure compatibility of hardware and software processing tools of data protection on the protected workstation with installable protection tools in compliance with the requirements for the configuration mechanisms of closed software environment, and flow control (mandatory access)
- The organization of complex schemes of information backup to external devices
- The development of the efficient schemes of the operational and centralized management of configuration
- The development of regulations to ensure continuity and rapid recovery of functioning of the object of protection in the presence of a complex server groups, including the secure server and domain controller, database, a management server anti-virus tools and file server

Thus, the effective protection from insiders of information security requires the use of additional forms of protection, such as workstations active monitoring, as well as intrusion detection systems

2. The main methods of ensuring the security of information systems

In order to counter threats are listed in the previous, modern information systems include security engines that implement the adopted security policy. Security policy in accordance with the purpose and conditions of operation of the system can determine the rights of access to resources and regulate the procedure of auditing of user activity in the system of network communications protection, to formulate ways of restore the system after a random crashes, etc. For the implementation of the adopted security policy, there are legal, organizational, administrative and engineering measures to protect information (see Fig. 1).

The legal maintenance of information security is a set of laws, legal documents, regulations, instructions, manuals, requirements which are required in the information security system.

Engineering measures are a set of special authorities technical tools and measures which are operating together to perform a specific task on the Data Protection Act. To engineering tools is included screening rooms, the organization of alarm, security facilities with a PC.