"HENRI COANDA"
AIR FORCE ACADEMY
ROMANIA

GERMANY

"GENERAL M.R. STEFANIK"
ARMED FORCES ACADEMY
SLOVAK REPUBLIC

INTERNATIONAL CONFERENCE of SCIENTIFIC PAPER
AFASES 2011
Brasov, 26-28 May 2011

THE SECURITY CONTROL OF THE INFORMATIONAL SYSTEMS

Loredana-Maria PĂUNESCU

Department for Economical Mathematics and Informatics, Petroleum&Gas University,
Blvd. Bucuresti 39, Ploiesti,Romania
loredana.paunescu@yahoo.com

Abstract: *In the present work there are presented the elements connected to the logical control, the identification, authentication and logical access to the informatics resources regarding the assurance of the informatics systems' security as well as the access to the systems, programes, and data only for the authorised users from the institution given as example.*

Mathematics Subject Classifications 2010: *68M12, 68M14, 90B20, 94C12.*
Keywords: *informatics system, control, procedure, access, information.*

1. INTRODUCTION

Security of information of any kind on the Internet and the first business information, is one of the barriers to electronic commerce development.

Processes to ensure the security of information systems function to protect systems against the use, publication or unauthorized alteration, destruction or loss of stored information.

Information systems security is ensured by logical access controls, which provide access to systems, programs and data only to authorized users.

2. CONTROL OBJECTIVES

Logical control elements that provide security systems are:

- data confidentiality requirements,
- the control authorization, authentication and access,
- user identification and authorization profiles,
- setting information required for each user profile,
- the control of encryption keys,
- incident management, futher measurements raport
- protection against virus attacks and prevention,
- firewalls,
- centralized security management systems, software,
- user training,
- methods of monitoring compliance with IT procedures, intrusion testing and reporting.

The organization must have an information security policy that covers:

- staff responsibilities,
- powers of security,
- clarification of data and security levels,
- control (audit) of national security.

Security policy relates to all employees, ie:

- internal standards and principles on security and, at the coarse level, by group (functions, departments) work,
- the code of ethics for employees and their preparation.

Ensuring security of information systems through the control provides security measures:

- including information about risk assessment at the organizational level of information security design,
- implementation and updating IT security plan to reflect changes in organizational structure;
- assessing the impact of changes IT security plans, and monitoring of security procedures,
- alignment of IT security procedures of the organization's general procedures.

Identification, authentication and access

- Logical access to computer resources should be restricted by the implementation of adequate identification, authentication and access by creating a link between users and resources based on access rights.

Secure online access to data

- In an online IT environment procedures to be implemented in accordance with the security policy, which requires security access control access based on individual needs, addition, alteration or deletion of information.

Managing user accounts

- Management organization must establish procedures to allow quick action on the creation, assignment, suspension and cancellation of user accounts.
- A formal procedure in relation to the management of user accounts must be included in the security plan.

Checking user accounts by management

- Management should have a monitoring procedure to check and confirm access rights periodically.

Checking user accounts to users

- Users must perform regular checks on their own accounts in order to detect unusual activities.

Security surveillance system

- Computer system administrators should ensure that all security-related activities are recorded in a diary system, and any indication of a potential security breach must be reported immediately to the persons responsible.

Data Classification

Management should ensure that all data are classified in terms of degree of privacy, a formal decision by the data holder.

Even data that does not require protection should be classified in this category by a formal decision.

Data should be reclassified in terms of modifying the degree of confidentiality.

Centralize user identification and access rights

Identification and control of access rights must be made centrally to ensure consistency and efficiency of global access control.

Reports on violations of system security

System administrators must ensure that activities that may affect the security of the system are recorded, reported and reviewed regularly, and incidents involving unauthorized access to data are resolved Force.

Logical access to information should be granted based on stringent needs of the user (it must have access only to information which is necessary).

Incident Management

Management should implement procedures for managing system security incidents so that the response to these incidents to be efficient, quick and adequate.

Confidence in third party

The organization shall implement procedures to ensure control and authentication of third parties with whom they come into contact with the electronic media.

Authorization of transactions

Organization's policy should ensure implementation of controls to verify the authenticity of transactions, and user ID that initiated the transaction.

The system must allow transactions can not later be denied by any one participant.

This involves implementing a system of confirmation of the transaction. Sensitive information should be submitted only considered secure communication channel between the parties, that does not allow interception of data.

Protection of security functions

All functions of the organization for security must be protected in particular, to maintain their integrity. Organisations must be kept secret for security procedures.

Encryption key management

The leadership must define and implement procedures and protocols for the generation, modification, cancellation, destruction, certification, encryption keys used to protect against unauthorized access.

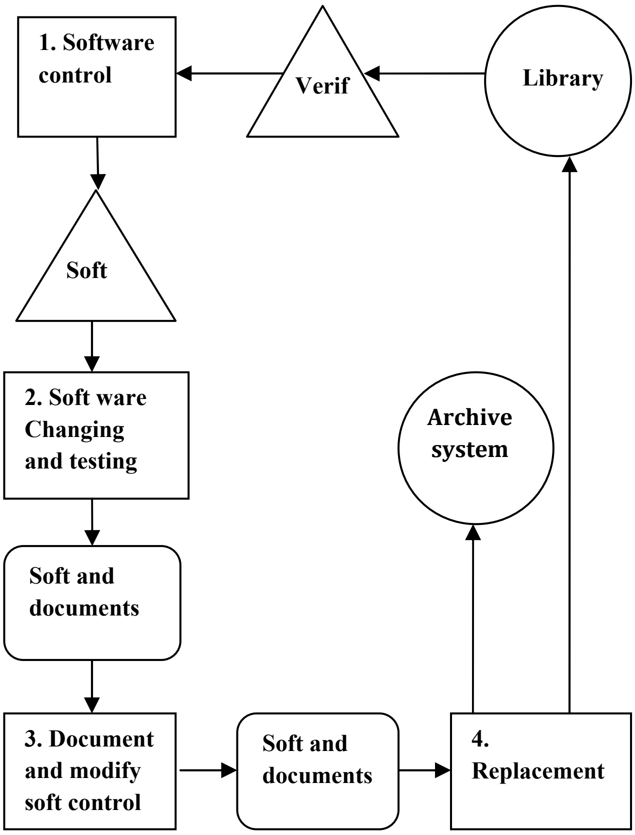

Fig.1. Protecting a system against viruses

Prevention, detection and correction of destructive programs

In order to protect the system against destructive software (viruses), have implemented a procedure that includes prevention, detection, action, correction and reporting of incidents of this kind.

Limits of a firewall

- restricts access to some services block external low protection for attacks from inside
- low protection against viruses,
- reduces the speed of communication with the outside,
- poor reliability due to centralization

Users' Authorization

a. Identification: PC to recognize a potential user of the system,

b. Authentication: establishing the validity of the identity function claimed ;

c. Authorization: user recognized and permitted access to system resources.

Access control

The risk of an unauthorized access refers to:

- reducing privacy,
- data theft,
- unauthorized disclosure of information,
- reducing data integrity,
- interruption of the system.

Control access to public environments using firewalls require access control policy between two networks and we show that:

- the whole data traffic passing through it,
- passing is allowed only as authorized by local security policy,
- the system itself is immune to penetration;
- communications monitoring TCP / IP,
- can record all communications,
- may be used for encryption.

REFERENCES

1. Bobolea, D., *Retele de calculatoare*, Editura Teora, Bucuresti, 2000.
2. Deac M., Lacrama D.-L., *Baze de date in aplicatii comerciale*, Editura Mirton, Timisoara, 2004.
3. Ivan, I., Apostol, C., *Certificarea produselor program prin amprente,* Revista Română de Informatica si Automatică, vol. 13, nr. 1, 2003, p. 28 – 31.
4. Ivan, I., Pocatilu, P., Ivan, A. A., Toma, C., *Data and Control Structures Oriented Software Testing, Master of International Business Informatics Handbook,* Bucureşti, Editura ASE, 2003, p. 41 – 62.
5. Ivan, I., Mijache, L., *Design Patterns – Cale de creştere a fiabilității software,* Revista NET Report.
6. Lacrama D.-L., *Securitatea bazelor de date*, Editura Teora, Bucuresti, 2003.