ASPECTS CONCERNING THE INFORMATION SYSTEMS SECURITY

Col.prof.eng. Gelu ALEXANDRESCU[*], Ph.D.
„Carol I" National Defence University

Security policy of information systems must take into consideration the following domains: equipment (hardware); software and firmware; procedures; communications, computer networks and physical environment; staff; stray radiation; natural disasters.

Keywords: information systems; security; communications; computer networks; information technology and communications.

The information vulnerabilities are a part of security systems vulnerability, generated by state of affairs, processes or phenomena of internal organization life (military structures), that diminish the reaction capacity to real or potential risks of any kind, including informational or that favor their appearance and development, with consequences concerning fulfilling the established objectives.

Generally, the informational vulnerabilities are even higher as the informational networks and information structure are of a higher complexity and with a higher degree of privacy, being harder to organize, manage and protect. Also, the vulnerabilities increase in direct proportion with the implemented technological level in equipment building and functioning (especially digital) of informational systems.

Management activities of informational system's security must allow:

- minimizing the possibilities of unauthorized entry in the communications system by using some layered protection solutions based on combining of policies, hardware and software solutions, for creating some secure barriers against unauthorized users;
- ensuring calculus equipment's security, of software and supervision system, and also of the relation and/or distribution data base system;
- detection of unauthorized use and determining the original entry point, concerning the fraudulent access.

[*] e-mail: *alexandrescugelu@yahoo.com*

The procedures security is a integrated part of the general security program of informational system and must assure a higher level of equipment protection that use software, by continuous survey of exploiting parameters and equipment, by protecting the hardware and software components against destruction or intentionally or unintentionally change, preliminary determination of probable implications that can appear to equipment configuration change, organizing a serious control to the generation, managing and use of passwords and keys concerning the access in different facilities offered by the informational system.

The security management of an informational system has an ensemble of measures destined to ensure the protection under all aspects of *the communication system* and *its components*, including: system entries, application access, information transfer, management components protection by analyzing and minimizing the risks, implementing the security plan and monitoring the application of used criteria (strategy). Special measures concern: supervision of security indicators, partitioning the information access, administrating passwords, generating notifications and alarm messages to security infringement.

Communications security includes the measures ensemble that assures the stable and uninterrupted networks functionality, own lines and communication means in conditions of executing by the opponent of some intense research actions, of jamming or of neutralization. It has the purpose to ensure preventing of emissions intercept, unauthorized electronic access and information change during transmitting it, assuring the use only by the authorized personnel. Also, it must prevent the unauthorized personnel access to equipment, services, material and documents, by discovering, confirming and counteracting the espionage, sabotage and destroy actions. The adopted security system must ensure a secure information circulation with any category of classification and by any transmission mean.

Networks computer security contains the techniques ensemble that realize the control concerning the fraudulent use and changing in computer or in held information and takes in consideration ensuring authenticity, confidentiality, integrity, availability and nonrepudiation of the processed and memorized information in the computers (servers and work stations). Security domains in information technology concern: computers, data, information, application and networks. For ensuring the security in computer networks it has a special importance also the content hiding of information by using data encryption.

The multilevel[1] hardware and software security concept associates different access control levels, to protect as good as possible a source, no matter its nature, without producing the performance degrading of informational system, taking into consideration: hardware and software resources to protect, access control at each subsystem and system in its ensemble, detecting the unauthorized penetrations (access) and preventing personnel penetration that don't have access right.

Hardware security contains:

- Fulfilling necessary controls to prevent the unauthorized access to equipment and connections, facilities, materials and documents;
- Ensuring protection against espionage, sabotage and deterioration of technical means actions;
- Providing distance access to be allowed only based on authorization by legal entities, and the used devices to be secured;
- Forbidding the physical threats against computer networks components, establishing if the firewalls and routers have the security assured;
- Blocking, with specific technical devices, the networks' entries and exits against the unauthorized access, confirming that the computer network is protected by a firewall;
- Keeping the computers and external magnetic supports in an electromagnetic protected environment;
- Having physical or even logical doubling of the files server;
- Using coaxial cables or optical fibers for reducing parasite radiations;
- Using systems of firewall, detection and prevention of intrusions.

Software security contains:

- Establishing the requirements concerning the detection and attacks prevention to software security, and also of controlling it;
- Establishing security standards that must be applied and used;
- Determining the software products from computers (source programs, libraries and filled modules) to which must be assured protection against unauthorized access;
- Ensuring unique identification of users access and labeling files with the persons list that have authorized access;
- Ensuring permanent accounting of all the used software products, continuous and round the clock control of software components functioning

[1] T. Bajenescu, *Telecommunication modern networks management*, Teora Publisher, Bucharest, 1998, pp. 123, 124.

of application and of software products existence to security (antivirus software and firewall software to identifying and blocking the unauthorized access of hackers, eventually and other nontechnical services);

- Ensuring that all the software products are rated and checked by authorized entities from the point of view of security criteria (confidentiality, integrity, availability, authenticity) before giving them to exploitation;
- Ensuring protection against compromising and deteriorating software products of application and informational through evil software (viruses, worms, trojan horses, logical bombs, zombies, vampires), checking and permanent using of antivirus programs, antispams, antispywares and for protecting against unauthorized access;
- Protecting the programs of automated encryption of information against subtracting and modifying, to keeping the unauthorized persons to know the clear content of memorized data in the calculus systems;
- Ensuring software products to saving some involuntary damaged files or restoring of some previous versions, and also of hiding some files;
- Using the documentation concerning the software design and performances of application and informational only by programmers and authorized operators, each of them having shared access only to programs that officially respond to;
- Keeping the authorized software products versions in 2-3 copies, realized on different magnetic supports, being forbidden to execute unauthorized copies from any source documentation;
- Archiving periodically the information from the data bases (deposits), after a pre-established program;
- Establishing the content and a way to realize the alarm against unauthorized access.

Computer networks security is mostly based on using firewall devices, through which it must confirm that:

- The computer network is protected;
- Translating the network address (Network Address Translation-NAT) and the server's domain name (Domain Name Server-DNS) are being used to hide internal names and addresses towards external users;
- Evil (codes) programs are filtered;
- Devices' work of detection intrusions (IDS) and the ones of preventing intrusions (Intrusion Prevention Systems-IPS) must be coordinated with the firewalls activity.

The computer networks security is vital to forbid the opponent to exploit the vulnerabilities of an information environment against allied forces.

Using information technology and communication has created the possibility of realizing some modern informational systems in which informatics and communications have a decisive role.

BIBLIOGRAPHY

Alexandrescu C., Alexandrescu G., Boaru Gheorghe, *Sisteme informaţionale – fundamente teoretice*, „Carol I" National Defence University Publishing House, Bucharest, 2009.

Alexandrescu C., Alexandrescu G., Boaru Gheorghe, *Sisteme informaţionale militare – servicii şi tehnologie,* „Carol I" National Defence University Publishing House, Bucharest, 2010.

Băjenescu T., *Managementul reţelelor moderne de telecomunicaţii*, Teora Publishing House, Bucharest, 1998.

Ilie Gheorghe, Stoian Ion, Alexandrescu G., *Reţele de calculatoare – soluţii de realizare şi administrare*, „Carol I" National Defence University Publishing House, Bucharest, 2004.

Ilie Gheorghe, *Securitatea sistemelor militare,* Military Publishing House, Bucharest, 1995.

Oprea Dumitru, *Protecţia şi securitatea informaţiilor*, Polirom Publishing House, Iaşi, 2003.