Trakia Journal of Sciences, No 3, pp 251-255, 2016

Available online at:
http://www.uni-sz.bg

ISSN 1313-7069 (print)
ISSN 1313-3551 (online) **doi:10.15547/tjs.2016.03.009**

Original Contribution

ADDITIONAL COSTS FOR SECURITY IN HANDLING CLASSIFIED INFORMATION

G. Pavlov[1], J. Karakaneva[2*]

Department of National and Regional Security, University of National and World Economy, Sofia, Bulgaria
Department of National and International Security, New Bulgarian University, Sofia, Bulgaria

ABSTRACT
The costs for information security are mandatory to provide so-called "industrial security", i.e. the ability of the company or organization to work on contracts related to classified information. However, because the information security is ensured by a set of measures at each stage of the information system life cycle it is possible to solve the problem in stages. Generally in the value of specialized security system are included: design work, purchase and setup of hardware and software products, incl. firewalls, encryption tools, antivirus systems, authentication, and authorization, and administration instruments. It is necessary to add the costs to sustain of physical security, personnel training, management, maintenance and regular updating of the system and finally – for security audit.
The paper analyzed some possible alternatives for the implementation of security system, as a result of the assessment of the information resources value.

Keywords: information security, classified information, security system, costs for security.

INTRODUCTION

The problem of information security is vital for governmental administration in the Republic of Bulgaria (Ministry of Defense, Ministry of Interior) and recently for the Council of Ministers and other ministries and agencies (Ministry of Finance, the Bulgarian Telecommunications Company, etc.).

Over the last 25 years the public research in the field of information security increased. In connection with the mass usage of Internet and e-commerce, many manufacturers offer high-tech software and hardware security solutions. With commercially available products and equipment it is possible to build a security policy to protect the information of powerful adversary.

There are three key concepts used in discussions of computer system security: vulnerability, threat and countermeasure (1, 2). The possible vulnerabilities and threats must be considered very carefully for each information system in order to decide how to protect the system and its information. Computer security is interested in identifying vulnerabilities in the systems and means to protect the systems against the threats. For each type of threat can be applied to one or more countermeasures. In connection with the ambiguity of the choice of countermeasures should use appropriate criteria to ensure protection of information at a given price.

The effectiveness of protection was assessed by the reduction of the probable loss. From an economic perspective the acceptable measure to counteract is when the value of the security tools is less than or equal to the value of probable losses.

It can be determined the maximum levels of risk in ensuring the protection of information and on that basis to choose one or more economically feasible countermeasures to reduce the overall risk to a value less than the maximum acceptable level.

The potential intruder would expect to get more profit from attack than the cost of funds invested in it. Therefore, it is necessary to maintain the price of violation of protection at a level that exceeds the expected profits of the infringer.

APPROACHES

Basically there are two approaches: The first is scientific, when it was first examined and

***Correspondence to**: *Assoc. Prof. Dr Juliana Karakaneva; New Bulgarian University, Sofia, Bulgaria; E-mail:ykarakaneva@nbu.bg*

subsequently implement in practice the necessary tools to determine the level of protection. In this case it is recommended the senior management to engage in the process of assessing the value of information resources and defining of potential losses from a breach of the security rules. This assessment is essential for the continued operation of the security team.

If the information is not valuable, in practice there is no threat to the information assets of the company, the potential losses are minimal and you can forget about security systems. However, if the information has a particular value and the threats and potential losses are clear, then the budget should include funds for security subsystem. The senior management must be aware and to support the security project.

The second approach is more practical. In this case the experts find the optimal value of corporate protection system based on a comparison with the best practices. International experience shows that the rational decision is the security system to costs about 10-20% of the value of the information system. In Bulgaria, this is basically the proportion of funds allocated in the financial sector security investigations shown IDG Bulgaria back in 2003.

In this approach, the justification of the budget is relatively easy – the authors cite the good practice formalized in a number of standards such as ISO 27001 for example. In both cases however, the realization depends on factors such as the maturity of the organization and the specifics of its activities.

Information security is ensured by a set of measures at each stage of the life cycle of the information system (3, 4) the costs are direct and indirect. The direct ones include those like software-technical means, labor costs, which are reported in the categories of operations and administration, as well as funds for services for remote users and others related with the activities' maintenance of the organization.

The indirect costs reflect the impact of communication and information systems and security subsystem on the company's employees through measurable indicators, such as downtime, "denial of service", "hang" the system and others. They often play a significant role, as it is usually not initially reflected in the budget for information security, appear subsequently and ultimately lead to an increase of planned expenditure.

The company management should engage in the evaluation process of the necessary funds for the protection mechanisms. One successful tactics is with the management team to speak with obvious business categories and arguments.

SOME PRACTICAL RECOMMENDATIONS AND SOLUTIONS

It is noted that the most developers of computer systems examine any hardware protection mechanism as additional costs that do not conform to the desire to reduce overall system costs. The decisions at the level of project manager include the issue of the development of hardware and it is necessary taking into account the ratio: the cost of procedures' implementation and reaching the level of information security. Therefore, every developer needs a formula linking the level of protection and the costs of its implementation (security costs-effectiveness). So, you can determine the cost of hardware's developing for previously defined level of protection. In general terms such dependence is introduced by Hoffman taking into consideration the following definitions.

Definition 1

Let's define the cost of the protection as proportion of the amount of resource used for the creation of a mechanism to manage access to the total amount of this resource.

Let's assume that R is a set of resources $\{r\}$,

M - set of system mechanisms $\{m\}$,

A - set of mechanisms of access control $\{a\}$.

Assuming that $U\ (m,\ r)$ is a quantitative measure of the use of the resource r by a mechanism m, the cumulative cost of the protection system for access control will be the sum of these costs.

In such of dependencies the developer can define various options and determine the mechanism of protection and what equipment to use. Unfortunately there is not such a flexible architecture of microcomputers that can easily be modified to achieve a certain balance between the cost and level of protection.

There are two possible factors that determine the value of the ratio "cost/level of protection" for mechanisms implemented with the hardware tools:

1) Creation of security mechanism using the existing or new technologies within the eligible costs;

2) Implementation of proper planning of security project. The basis of this approach is

the clarification of the need to perform protective measures. On the other hand, the design and protection mechanisms should be adequate to meet the requirements of minimizing the cost of development taking into account the possible attempts to breach the system.

In the process of identification and access management has become necessary the registration of the user to "system for access" (SA). Usually registration function is implemented by the operating system (OS) and the additional costs for programming and backup of devices and recording and storage of registration's information (logs) must be small. Preferentially this information is encrypted. If there is a reliable means of data protection by registration journal we may not need a different device for it, but in any case this journal must be separated from the controlled system. Deleting the information from such a device is allowed only for certain people and after the written permission.

During the discussion of economic problems in the information's protection, particular issue is the costs associated with such transformations as temporal coefficients of encryption. This coefficient is defined as the ratio of the time T_1 of *selection, encryption and data transfer* to the time T_2 of *selection and transfer* (without encryption) ($K = T_1/T_2$). It allows regardless of the computer's type to measure the temporary cost of information's protection.

For comparison of the different methods of encryption for different computers and programming languages are performed five tests with different encryption keys:

• Zero conversion – the test data is moved from one section of memory to another. The speed of encryption is the basis for the comparison of the two times (with and without encryption).

• The key contains one word – the data is selected from memory and to each word is applied a logical operation "OR" with key and the result is transferred to another section of memory;

• Long key − the action is similar to the previous test, but the key contains 125 words;

• Dual key − two keys consists of 125 and 123 words are added by logical OR to the source text.

• Random key of infinite length − as a key is implemented the set of symbols derived from pseudorandom numbers generator.

A comparative evaluation of the effectiveness of these transformations can be made on the basis of these tests.

The speed of encryption is different, but as a rule, the difference is not significant if the coefficient of efficiency defined above is used. This difference would be important in certain amount of speed of the CPU (engine time is a measure that is used by machines with powerful processors from the last century).

If it is necessary to include instruments for information's protection, additional costs are determined by the cost of programming. The costs are determined by the following operations:

1. Developing of program tools for support of hardware instruments for protection;
2. Adding of function of messages' generation for limiting printing of information;
3. Compulsory completion of the job when there is an attempt of security breach or attempt for execution of privileged commands;
4. Forming and reporting a signal in the case of attempted breach of the security functions;
5. Automatic activation of the protection system during startup;
6. Removing the information within the memory's block in the return of the resources in the system;
7. Full double recording of data for limited use;
8. Clearing the hardware buffers on stopping devices.

CPU cost in such systems grew by 2% and about 10-15% is reduced the capacity of the system to process data.

COSTS RELATED THE DESIGN AND DEVELOPMENT

Obviously, the determination of the value of information is the basis for decisions on the level of protection. There are many attempts to formalize this process based on the methods of information theory, but the evaluation process today is too subjective (5, 6).

The organizations are vulnerable to risk in a different way. Their security policies should reflect the vulnerability of the particular organization for different types of security incidents and require priority investments in the area of greatest vulnerability.

There are two factors determining the vulnerability of the organization (7).

First factor is the consequences of a security incident. All organizations are sensitive to financial losses. The aftermath of an incident safety may require significant investments,

even if they suffered only non-critical services. An important step in determining the potential impact is the generation of a register of information resources. Although it seems easy to maintain an accurate list of systems, networks, computers, and databases used in the organization, it is a complex task. Another important objective is the categorization and classification of the information resources, according to their value and potential risk.

More serious effects of incidents appear when the work of the organization is impaired, which lead to losses of missed opportunities, loss of time and work to restore the activity. The most serious consequence is the interrupting of the external functions. Such consequences directly cause financial losses as a result of impaired operation of services or the potential loss of customer confidence in the future.

A second factor captures the political and organizational consequences. In some corporation or governmental institutions the penetration on the network is the serious accident, even if such organization has no financial losses. In open environments, such as universities or research centers as a result of the incident the management may decide to introduce the restrictions on access.

These factors should be considered when determining the vulnerability of the organization in terms of security incidents. To ensure the protection of all information resources, so that the computing environment of the organization can be quickly restored after security incidents, every network administrator should keep a register of information systems in its area of responsibility. The list must include the existing hardware of the computing environment, programs, electronic documents, databases and network channels.

For each information resource to be protected a description of the following information can be carried out:
1. Type: equipment, program or data;
2. Usage in the system: general-purpose or critical application;
3. Responsible people for the information resource (owner);
4. Physical or logical location;
5. Catalog (register) number.

General purpose system is "interconnected set of information resources that are under a single administration, allowing the solution of general (non-specific) tasks or ensure their implementation". Usually the tasks of general purpose systems are providing treatment of information or interaction between applications. General purpose system incorporates computers, networks and programs providing the work of significant number of applications, and is usually administered by the department of automation in the organization.

Security policy for general purpose systems as a rule is also applicable to the Internet components because the server, communication programs, and gateways providing Internet connectivity, typically are located under one management.

Critical applications are these that can lead to large losses of the organization in case of security incident.

Technology can contribute much to protect corporate resources, but it is not enough. The rest depends on the people. The hard work of security officers to turn employees into the responsible owners of corporate data is very important to be the company more secure.

CONCLUSIONS

The considered financial issues in designing a data processing complex for classified (secure) information can be arranged in the following sequence:
• Initial (investment) costs associated with the security system;
• Ongoing operating costs.
The investment costs include the costs for risk analysis and formulation of system's security requirements, development and implementation of programming procedures to protect information and the costs for physical security.

Operating costs include the costs associated with maintaining the operability and stability of security system. They include the additional costs of the system processing, for allocation of additional memory for protection programs, but also for system registration log, additional personnel costs and other current expenses.

It should be noted that while there is not enough reliable standard methods for measuring the degree of information security in the design of the protection system, remains paramount requirement to provide a given level of security at an affordable price realization.

REFERENCES

1. Pavlov, G., J. Karakaneva, Information Security Management in Organization,

Trakia Journal of Sciences, vol. 9, n. 4, 2011.
2. Karakaneva, J., Architecture Design of Security System, *Trakia Journal of Sciences*, vol. 8, n. 3, 2010.
3. Pavlov, G., Protection of the Information, University Press "Economy", UNWE, Sofia, 2010 (in Bulgarian).
4. Pavlov, G., Information and Security, Avangard Prima Publishing, Sofia, 2012 (in Bulgarian).
5. Pavlov G., Information security policy of the firm business transactions, *Trakia Journal of Sciences*, Vol 1, No 4, pp 13-18, 2003, available on line at: http://www.uni-sz.bg
6. http://kiev-security.org.ua.
7. Karakaneva, J., Каракънева, Ю., Aspects of the organization's security in time of crisis, Scientific Conference "Economics of Defense and Security", UNWE, Sofia, 2011 (in Bulgarian).