AUDITING THE SECURITY OF INFORMATION SYSTEMS WITHIN AN ORGANIZATION

STEGĂROIU CARINA-ELENA,
LECTURER PHD, „CONSTANTIN BRÂNCUŞI" UNIVERSITY, TÂRGU JIU, ROMANIA
carinastegaroiu@yahoo.com

Abstract
The safety provided by a well configured firewall is no excuse for neglecting the standard security procedures; setting up and installing a firewall is the first line of defense and not a full proof solution, auditing being only one component of the system, whilst the other is protecting the resources and when we consider auditing as being the process of recording certain events that take place on a computer or within a network, we must come to the conclusion that this is the only technique that allows us to identify the source of a possible issue within the network.

Information security is used as a means to protect the intellectual property rights, whilst the main objective in setting up an information security system is to enlist the confidence of prospective business partners. In accordance with the legal requisites and the principle of maximizing one's investment, regardless of the many forms it could take, or the means through which it is stored, transmitted or distributed, information must be protected.

Information security is not only a technical problem, but mainly a managerial issue, as the security standard, ISO/IEC 17799 meets the needs of any type of organization, be it public or private, through a series of practices related to the management of information security.

This paper aims to present the process of taking entry data from a plethora of programs and storing it in a central location. Due to its flexibility, this process can be a useful auditing instrument, as long as we are familiar with the way it works and how the events are recorded.

Key words: *information security, auditing, internet, firewall*

Clasificare JEL : *A10, B23, C61*

1. Introduction

By connecting to the Internet, be it from home or the office, we become members of a community which is wired to an enormous system that is superior to any one individual and where time and distance are rendered almost obsolete in favour of the interconnectivity which creates unprecedented links between all members.

The security of such a network is seen as an activator of services as well as an element of competitive advantage on the market – as the trend evolves, security incidents can have a significant impact on stock quotations and can affect customer services within many a companies, a fact which can damage the bond of trust between clients and businesses.

Inevitably, the dangers generated by cyber attacks will continue to grow and pose a viable threat as companies continue to rely on the Internet for transactions and business management and expansion.

The greatest risk is that of damaging the company reputation as a result of a security breach and therefore affecting the client/business partner confidence. Such a breach can be catastrophic for the business and unfortunately, as virtual networks and the services related to them expand, no domain is spared this plague. Therefore, information loss and contamination has become an integrated part of a business's risk management plan and it – should – also factor as one of the key elements of any contingency plan given the insidious type of danger it poses in a market dominated by the strength of trust bonds and powerful image branding.

Consequently, the process through which events that can generate losses are identified and quantified is dealt with by risk management by cataloguing risk factors in the following form:

- the inherent general risk, which is made up of the management risk, the accounting risk and the business risk;
- the control risk, which is represented by an error or a group of errors with a significant impact, which have not been prevented, detected or corrected on time by the accounting system or by the internal auditing.
- the non-detection risk, in which the basic auditing procedures fail to detect a significant error or a group of errors with a cumulative negative effect;
- the risk of sampling.

By categorizing various types of information related risks, greater control over the way the information load operates can be enforced. The difference between the security within a local network of computers and a widespread one such as the Internet is made by control, for in a local network if we know the used protocols we can configure the monitoring and the auditing in order to prevent abuses. Moreover, separating the incidents by their probable source can help isolate prospective breaches of security and thus, maintain a semblance of stability within the network. Such procedures usually make up the security policies of an organization, the structure of which we will further analyze in order to better identify the optimal design that would benefit the safety of sensitive information.

2. The policies of the information security program

By analyzing several security policies a general structure can be inferred, with the mention that no two organizations have identical security policies.

When one implements an information system security program, one must first devise a policy for such a program. This is the umbrella concept under which security techniques, norms and standards are devised and applied. In a given unit, special policies for Internet and email use, for remote access to the system, for the ways of using the information system, for data protection etc. are required.

Therefore, such a policy defines the overall company policy in the information field, as well as the responsibilities within the system, the objective being that of offering the management the necessary support for securing the data within the organization. It is our aim to present an overview of the key elements of a security policy, in order to provide a springboard for understanding and embetterment of information safety.

Consequently, the policies which should be generated are essential components of the program and must answer to five major objectives:

- prevention: the ability to prevent unauthorized access to the patrimonial values of the organization;
- assurance: making sure that the policies, standards and norms are in accordance with the intentions of the organization regarding the protection of its patrimonial values;
- detection: the ability to detect intruders in a system and to launch the necessary counter-measures;
- investigation: the ability to use adequate techniques to obtain information about possible intruders in the system;
- continuity: the possibility to guarantee uninterrupted functioning through the development of a action plan in case of disaster.

Once these objectives are set, met and put into practice, the policy can be further refined by means of implementing an efficient code of good conduct in regards to the way information is handled.

Therefore, the policy of adequate use must analyze and define the corresponding use of information technology within the organization. Users should read it and sign it whenever they are about to set up a user account. The responsibilities of the users must be formulated explicitly, as should be the levels of Internet and email use. The policy should also provide an answer to the following questions:

- Should users read and copy files that are not theirs, but to which they have access?
- Should users modify files that support this option, but that don’t belong to them?
- Should users make copies of setting up kits for personal use?
- Should users have shared access to their open accounts?
- Should users have the right to make copies of licensed software?

At first glance, such steps may appear self-explanatory, but the simplicity of the statements should not leave room for leniency when it comes to mishandling information at the workplace. A clear and concise policy should help and guide users and at the same time prevent misinterpretations and incidents caused by ignorance and/or lack of proper guidelines. Another policy that deals with the norms for opening system accounts and maintaining them is the user account policy. This is very useful in large organizations, where users have accounts in different systems. As in the previous situation, reading and signing such a policy is advisable and the policy should provide answers for the following set of questions:

- Who can authorize new user accounts?
- Who (employees, spouses, relatives, children, visitors etc) is allowed to use the company’s information resources?
- Can a user have multiple accounts in the same system?
- What are the rights and responsibilities of the users?
- When is an account deactivated and stored?

Again, we reinforce the idea that assigning clear roles and dealing with problems according with their source of origin is paramount when it comes to establishing a viable information security policy. Although eminently intangible, data and information should be treated like one would any other company asset, if not when even greater care considering the role they play in forging trust between clients and businesses and building reputable images on the market. As such, as we move forward with our analysis, the issues of remote access and data sensitivity inevitably arise. The remote access policy defines the ways of connecting form outside the internal network. Such a policy is necessary when we are dealing with organizations in which the users and networks are not geographically aligned and it must answer the following questions in order for it to be applicable and functional:

- Who has remote access rights?
- What methods are accepted by the organization (dial-up, modem)?

- Is modem access from an external source to the internal network allowed?
- Are certain security conditions imposed, such as having an antivirus software, for remote access?
- Can family members access the network?
- Are there any restrictions regarding the kind of data that are accessible from an external source?

Inextricably linked with access is, naturally, access sensitive information. Information security policy sets the conditions for processing, storing and transmitting sensitive data and protects against unauthorized modifications and access. Such a policy must be signed by all employees and it must answer at least the following questions:

- What are the data sensitivity levels?
- Who has access to sensitive data?
- How are sensitive data stored and transmitted?
- What levels of sensitive data can be printed on public printers?
- How should sensitive data be deleted from external supports (shredding papers, erasing disks etc.)?

We note that, in the last two instances, attention to detail must prevail when designing such policies. Breaches of security often occur due to loops in the system that are not covered during the design and implementation phases. Once these issues are taken care of, firewall can be installed in order to add an extra layer of protection.

Therefore, the firewall management policy describes the way in which hards and softs are managed and how change requests within the system are handled. It answers the following set of questions:

- Who has firewall access?
- Who should receive the requests for operating changes within the firewall?
- Who should approve such requests?
- Who can see the regulations and access lists to the firewall configuration?
- How often should firewalls be audited?

One more element is, at this stage, necessary in order to regulate access to the system. Password management policy is often the heart of security policies within an organization. Usually, it regulates issues regarding expired passwords, password length and check ups. Here follows some recommendations for such a policy:

- Minimal password length should be at least 8 characters;
- Passwords should not consist of words found in a dictionary;
- It should be a combination of characters and specific symbols;
- Passwords should expire after a predermined period of time;
- Passwords belonging to network administrators should expire faster and be longer;
- Passwords in the organization should be different from the ones used in other systems;
- A list with old passwords should be kept in order to prevent re-use (the last 6 passwords should not be repeated);
- New user passwords should be new and difficult to guess.

Of course, these recommendations are by no means inexhaustible. Levels of difficulty can be set higher, according to the internal demands of the company. That is why companies often regulate not only the way in which the system works, but also how permissive and “user-friendly” it should be. The Internet use policy, or I-AUP (Internet Acceptable Use Policy), is the document through which the ways in which the users of an organization network can navigate the Internet are described.

The policy approves the software used for filtering and blocking, the specific activities which are allowed as well as the beneficiaries of the access rights. It should also include authentication methods before accessing the Internet from outside the organization/country in order to prevent illegal use.

The protocols covered by such a policy are as follows:

- Electronic mail includes all the forms of email used by an organization, all that is accepted for use and the software used to filter and scan. The policy for this area should emphasize the specific requirements regarding data that cannot be transmitted via email and the procedures that should be followed when a user receives an email containing such data. The policy should also contain the measures that ought to be implemented in case of email misuse.
- **Web**. The policy will define the specific conditions for web trafficking. As long as the WWW (World Wide Web) uses HTTP (HyperText Transport Protocol) to transfer information, this policy will clearly define the types of sites that are strictly forbidden (pornographic sites, gambling sites etc.)

By the Internet policy we mean the following:

- Accepting the use and the conditions for:
- File download;
- newsgroups
- sensitive data communication;
- type of attached files;
- message size;
- unlicensed software;
- unapproved soft kits;
- exporting sensitive data;
- folder protection;

- antivirus protection;
- management of system changes;
- data storage;
- safety and availability;
- data protection through classification;
- access control;
- e-mail and data that can be stored in an unit;
- monitoring;
- exceptions and amendments to the Internet policy.

Regulated use of the Internet, in addition to the stipulated access and use to the Intranet, are by no means the least of the issues a viable information security policy and program should take into consideration. The details and layers of security such issues provide can only help strengthen the security program past designing an impregnable firewall.

3. Using the site security policy to design the firewall

The term firewall was first used in constructions as a non-flammable barrier between apartments in a building, and then it was adopted by security experts in order to describe a method of preventing intruders from entering a network connected to a larger network.

Before devising a firewall strategy we must first consider the elements which we want to protect and the way in which we want to do so, and also keep in mind the company's security policy and then we can make decisions as to the types of services that can be allowed to pass through the firewall.

After revising the security issues, we can develop a firewall policy by using two fundamental methods: allow all access except that which has been specifically forbidden or forbid all access, except that which has been specifically allowed. The second strategy shall be used as it is easier to specify a small list of things we will allow than a larger loust of things we will forbid.

As the Internet network continues to grow and new protocols and services are developed, we will not have to add new rules to exclude possible new problems, at least until we have the time to revise security elements and decide if we should allow the protocol or service through the firewall.

The safety provided by a well designed firewall should not be an excuse for neglecting the usual security procedures, as a firewall cannot protect against all damages coming from an external network.

Auditing, seen as a process of recording certain events that occur on a computer or network, allows us to detect the source of a possible breach and the infiltrator that is capable of destroying important data.

In order to do so, there are operating systems that have extended auditing abilities – see syslog, which takes entry data from a variety of programs and stores them in a central location and which, due to its flexibility, can be a valuable instrument for auditing as long as we understand the way in which it is configured and the events it records. Syslog must be turned on when booting, and this operation is done through one of the rc files - /etc/syslog {-mN] [-ff*ilename*] [-d]

Syslog: syslog.conf is an ASCII file which we can modify by using a standard text editor. We can use the /etc/syslog.conf file or we can use a different file by opting for such a file when opening the syslog. The file contains a recording in two parts:

- a selector that defines the event which should be recorded
- an action that defines what syslog should do when the event occurs

The selector part is made of two data areas, separated by a dot. The first part is the name of the system function that generated the event message. The second part indicates how severe the event is. On a single line, more than one selector can be placed, but they must be separated by a semi column (;).

Syslog runs as a background process, listens to messages and decides when to act based on the rules set up in the configuration file. These messages come from 3 sources: from /dev/log that receives messages from the processes that run on the local computer, from /dev/klog that receives messages from the core of the operating system and from the UDP 514 port that receives messages from other computers on the network.

As we have done so throughout the course of this paper, we reinforce the fact that when the safety and security and information are concerned, there is no such thing as an overkill. It is often the "backup for the backup" and the attention paid to the details of information access and use that help protect a business's information load from exposure, corruption or contamination.

4. Conclusions

Nowadays, information is composed of mostly processes, as it is transferred and stored using information systems and equipments (means, facilities for automatic processing of data - MPAD).

We can safely state that transmitting information all over the world is done by using information systems, such as electronic mail, mobile phones, photo and video cameras and that people are downloading all types of data from the Internet, even specialized programs, in stark contrast to years past when such access was unattainable.

The audit of information systems is not unlike the quality audit for other systems when it comes to planning, implementing and reporting, and it only differs in the set objectives and the aspects that need to be included in the audit questionnaire and also in the way the auditing proofs are presented, meaning that most of these cannot be handed over on paper to be evaluated and the auditors' access to the system in a large organization can be a big threat, and the organization must take measures to offer all the auditing proofs required while also keeping secret information protected within the systems.

This paper has dealt with 5 key elements that ensure the viability of any security strategy for an organization, and they cannot be dissonant lest they should add prejudice to the final goal of information safety. The 5 key elements are as follows:

1. Security policies in accordance with the activity of the organization, a written policy with clear objectives and firm measures and corresponding resources. These policies should be made known to the employees, collaborators, third parties and to all other parties the organization deals with.

2. Security plans that set up strategies for implementing policies and that consider all elements of the organization's activities and existing technologies, and also the future directions for development.

3. Key products/services that are necessary for the execution of the plan and the achievement of the set objectives. How should levels of security, performance and quality be achieved.

4. Monitoring and managing processes to ensure the set security level. The measures and methods used to analyze the processes and performances and align them to the development of the organization.

5. Trained personnel for implementing security policies, plans, products and processes.

These 5 key elements, if applied correctly and effectively, may serve as a springboard for developing a full proof information security system, which, in effect, is a prerequisite when it comes to protecting sensitive data and the influence it has on building bonds of trust and good reputation on the current business market.

5. References

[1] **Oprea D.**, Protecţia şi securitatea informaţiilor, Ediţia a II-a, revăzută şi adăugită, Editura Polirom, Iaşi, 2007.

[2] **Mihai I. C., Popa I. F.**, *Securitatea în Internet*, Editura Sitech, Craiova, 2008.

[3] **Popa S. E.**, Securitatea sistemelor informatice, note de curs şi aplicaţii pentru studenţii Facultăţii de Inginerie, Universitatea din Bacău, 2007.