INFORMATION SECURITY RISK AUDIT IN ORGANIZATIONS

Ion Ionuț Bratu, Valahia University, Romania

ABSTRACT

Information protection has become a significant concern for many organizations. Establishing a security program is the process by which security is provided to the company. It involves five steps: establishing the main steps and the staff responsible for ensuring security, defining the requirements for improving security, informing staff about the security measures imposed, auditing and monitoring security. The auditor should verify the extent to which existing controls in the organization ensure the confidentiality, integrity and availability of information resources. This paper focuses on the importance of the audit service from the perspective of determining security risks and compliance with the minimum security requirements imposed by industry standards.

JEL: M42, M48, O33.

KEYWORDS: security risks, audit, cyber threats, risk factors.

INTRODUCTION

The problem of security is felt today as an acute need, although its implementation often occurs as a result of significant data loss, fraud or information theft (Bozkus Kahyaoglu & Caliyurt, 2018). In this context, it is necessary to realize that the security of information systems is primarily a human problem and not a technical one, which requires awareness and motivation of the human factor in this regard.

Security control ensures the protection of the organization against unauthorized access to the organization's resources, both by its employees and by the people outside of it (Hong, Chi, Chao & Tang, 2003). Thus, the audit follows the existence of concrete measures regarding: the confidentiality and integrity of communications and data; confidentiality and non-repudiation of transactions; preventing, detecting and monitoring unauthorized access to the system; management and administration of the computer system or any other activities or technical measures undertaken for the safe operation of the system.

In most cases, the information presented in the audit report represents aspects that lead to the danger of the security state of the system and that can lead, under certain conditions, to the non-observance of the optimal security conditions. The preparation of the audit opinion and of the audit report is performed by documenting the operations undertaken within the audit mission and performing the tests undertaken as well as the results obtained.

GENERAL REFERENCES REGARDING SECURITY RISK AUDIT

Security is not perfect, no matter what measures are taken. There will always be an unthinkable loophole through which the system can be attacked. Security is a protection of the information and processes of an information system against disasters, human error and fraudulent manipulation so that the impact on the organization is minimized (Onwubiko & Lenaghan, 2009). The requirements of information technology security are often reflected in the following terms:

- assurance: the fact that the system works as expected, meets the requirements of users;
- identification / authentication: the process by which the computer recognizes the presence of a potential user of the system;
- responsibility: users are responsible and must justify their actions;
- access control: access to information resources may be restricted to different categories of users;
- securing the electronic transfer: by ensuring the confidentiality, integrity and authenticity of the transmitted message and its non-repudiation;
- continuity of services: ensures the availability of data and processes of system users.

All these properties can be accomplished by using public cryptographic keys (Hong, Chi, Chao & Tang, 2003). Today, special attention is paid to the development of legal standards and rules for resolving the main weakness of public key encryption systems – joining a public key of a user with that user's identity.

The auditor should verify the extent to which existing controls in the organization ensure the confidentiality, integrity and availability of information resources (Pereira T. & Santos, 2010). Confidentiality is intended to protect information against unauthorized access. The most important aspect in this case is the identification and authentication of system users. The integrity of the information refers to its protection against unauthorized changes (accidental or intentional); unauthorized access to the organization's strategic information often leads to fraud. But availability means ensuring the accessibility of the computer system whenever authorized individuals within the system request it.

Another important activity carried out by the auditor during the missions is penetration testing at the level of the internal infrastructure and of the one exposed in the Internet (Frost & Choo, 2017). Thus, the purpose of an external penetration test is to identify, evaluate and fix security vulnerabilities that could affect the external interface of the IT infrastructure, which could lead to compromise of access control systems in the system and implicitly allow unauthorized access to data and company internal information. At the same time, the internal penetration test reveals vulnerabilities in the internal infrastructure and offers recommendations to counteract them in order to create a solid and secure internal network, without compromising its use.

The auditor will also verify the system of restrictions imposed by the network administrator – a system that must ensure an adequate filter of users in data processing and last but not least, will analyze the network design and security tools used within it. It refers to the methods by which an authorized user accesses files, directories, ports and even protocols. In this sense we can speak

on the one hand, of an access control in the system (physical control), and on the other hand of an access control to its resources (logical control).

In order to meet current and future cyber security challenges, good user access management requires knowing at all times who has network access, what is it doing, how long has it been accessing system resources. Users' access to a system requires its identification, authentication and authorization in the system. The auditor will check that procedures are established for their periodic change, and that the confidentiality and transparency of the passwords, plus the access to encrypted files is being protected.

CONCLUSIONS

The integrity of the information held by a company is vital for that company to survive, to develop and, at the same time, to ensure a closed and secure circuit of the flow of information within the organization.

During the audit missions, a number of vulnerabilities were found, such as incorrect management of user rights by the network administrator, failure to disconnect users after a number of failed logins, incorrect password management, inefficiency of the user control mechanism, lack of a logbook, lack of memorizing the last successful or unsuccessful login, the lack of a file access control system depending on the level of authorization that can lead to unauthorized access, and improper access to network resources.

Internet network vulnerabilities can also lead to surprise attacks by network users leading to unauthorized access to the private network with the necessary consequences. The auditor of such an organization, who uses Internet services, will verify the existence and configuration of specific tools such as: firewalls, VPN (Virtual Private Network), intrusion detection tools (Intrusion Detection System), encryption techniques and PKIs..

REFERENCES

Bozkus Kahyaoglu, S. & Caliyurt, K. (2018) “Cyber security assurance process from the internal audit perspective”, Managerial Auditing Journal, 33(4), 360-376.

Frost, R.B. & Choo, C.W. (2017) “Revisiting the information audit: a systematic literature review and synthesis”, International Journal of Information Management, 37(1), 1380–1390.

Hong, K., Chi, Y., Chao, L.R. & Tang, J. (2003) “An integrated system theory of information security management”, Information Management & Computer Security, 11(5), 243-248.

Onwubiko, C. & Lenaghan, A.P. (2009) “Challenges and complexities of managing information security”, International Journal of Electronic Security and Digital Forensics, 2(3), 306–321.

Pereira, T. & Santos, H. (2010) “A Security Audit Framework to Manage Information System Security”, In: Tenreiro de Magalhães S., Jahankhani H., Hessami A.G. (eds) Global Security,

Safety, and Sustainability. ICGS3 2010. Communications in Computer and Information Science, vol 92. Springer, Berlin, Heidelberg.