Ghibanu, Ionuț Adrian

Article

Vulnerabilities and threats of information systems and communications

Academic Journal of Economic Studies
Vol. 5, No. 4, December 2019, pp. 151–155
ISSN 2393-4913, ISSN On-line 2457-5836

Vulnerabilities and Threats of Information Systems and Communications

Ionuț Adrian Ghibanu

Valahia University, Romania, E-mail: ghibanu.ionut.adrian@gmail.com

Abstract

In the economic-financial life, risk is a component of any activity, being found in the daily agenda of company managers. This article presents an overview of the existing vulnerabilities and threats in information systems and communications. The results show the information security policies determine the dynamics of the security threats and vulnerabilities towards information handled in communication and information systems.

Keywords

Information systems, risk, network, threats, vulnerabilities, communications

JEL Codes: D80, D81

Received: 10 November 2019 **Revised: 26 November 2019** **Accepted: 13 December 2019**

1. Introduction and literature review

Information is a product that is of value to an organization and therefore needs to be properly protected. According to the specialized literature, information security comprises procedural (administrative) security and computer security (computer security and communications security) (Willems, 2011; Gandino *et al.,* 2017). As the number of computers under attack is increasing, it is not surprising that people have begun to take computer security seriously (Arukonda and Sinha, 2015). But despite this growing interest, many computer users still do not really understand what computer security is and why it should be important to them.

If a computer is connected to a computer network or can be accessed by phone or otherwise, the risks of someone being able to penetrate the system increase accordingly. Messages can be intercepted, redirected or modified. The financial behaviour of the economic agents is influenced by the level of development of the financial market by its credibility and by the way in which the resources can be purchased or the economies placed through the financial companies (McQuade, 2006).

People running the system or just using the computer are the biggest vulnerability for its security. System security is most often in the hands of a system administrator (Kshetri, 2014). Also, regular users, operators, programmers, or people who support the system may be corrupted or forced to disclose passwords, information, or access paths, in other words, compromising the security of computers (Chen and Zhang, 2014). In the most general sense, the security of the computer systems ensures the protection of the information stored in these systems, prevents the loss, accidental or willful modification and their unauthorized reading, that is what is expected from them, even if the users do not do what they should do (Winkler, 2010; Dor and Elovici, 2016).

Although it is not just about securing security and confidentiality, the key to the success of an e-banking system is largely represented by this important aspect. Major frauds or smaller attacks, due to breaches in the security systems, have shaken the image and functioning of the banking companies that have been hit by this new type of offenders specialized in electronic banking offenses (Arukonda and Sinha, 2015). The technology of electronic payments should allow individuals to transfer important funds, instantly, anywhere in the world, and at the same time remain anonymous, but it will be very difficult for authorities to collect taxes and fight against those who break the law (Krombholz *et al.,* 2015).

Analyzing the rate of attacks statistically, it was found that the nodes where the lines meet are the most vulnerable, and the communication equipment is vulnerable to both natural disasters and errors, as well as to the human factor. It is extremely important that unauthorized persons are kept away from them. Communication lines and network connections are highly vulnerable to attack. Often it is easier to get into a system through the network than from the inside (Arukonda and Sinha, 2015).

For each method of attack there are identified vulnerabilities that could be exploited (Arukonda and Sinha, 2015). Subsequently estimated vulnerability level could be very unlikely / not feasible (low probability, requires expensive

equipment and a very high level of experience), quite likely (requires a high level of expertise and/or expensive equipment), with high probability (requires standard equipment and experience), certain (can be done by anyone).

To achieve identification and information security risk assessment is essential to identify threats and vulnerabilities in the system they can exploit (Da Veiga, 2016). For each pair threat / vulnerability, determine the severity of impact on the organization's information assets (loss of confidentiality, integrity or availability thereof) and determine the likelihood that vulnerabilities exploitation in conditions of security controls implemented at the system level. Therefore, vulnerabilities are based on understanding the functions and capabilities that are available in the operating environment of the system through which information is managed (Karim, 2007). Assessment of threats and vulnerabilities lead to qualitative conclusions about the threat (in terms of very low, low, medium, high, very high) and vulnerability (in terms of low, medium or high).

2. Overview of the existing vulnerabilities and threats in the information society

The complexity of the new economic systems involves more and more information exchanges between its elements - companies, government agencies, associations, institutions, even simple individuals. These processes create an increased need for digital telecommunications networks and new media (Hjortdal, 2011).

Risk management involves a cyclical activity that begins with the risk analysis that will have to lead to the formulation of the risk management policy and will result in a protection plan and an insurance plan. Then the results obtained are used in the feedback loop to control the entire process (Singh and Fhom, 2017).

Minimum security measures in the judicious use of computer systems should be implemented to allow the reduction of risks related to computer infections, to an acceptable level. Among the measures against infections we can mention: preventive measures, protective measures, detection measures, elimination measures, repair measures (Eastin *et al.,* 2016).

The degree of vulnerability to attack of the environment depends, in a decisive way, on its type. Network cables are possibility vulnerability for a computer system and this also results in certain measures that must be taken even from the design phase of a computer network (Arukonda and Sinha, 2015). Threats that must be considered include:

- threats communicative nature, such as interception of communications and incorrect routing messages;
- threats logical type, such as hacking, unauthorized use of an application, malicious software;
- threats related to technical failure of equipment or applications related to information systems and communications.

In accordance with the specialized literature (Broadbent and Schaffner, 2016; Andress, 2003; Fenz *et al.*, 2014 Strang and Sun, 2017), Table 1 presents a list of examples of vulnerabilities and threats that can exploit these vulnerabilities, along with the types of goods that may be affected system.

Table 1. The list of examples of vulnerabilities and threats

Vulnerability	Threat	Affected assets
Lack of back-up files	Operations without interruption of power supply; unauthorized software, unauthorized modifications	Date
Improper configuration management	Technical malfunction; Unintentional human error; Programming errors	Hardware; Software
Inadequate control of software distribution	The use of unauthorized software	Software
Absence of audit records	Unauthorized access to resources	Date
Management inadequate communication network	Failure of communications services	Date
Inadequate supervision programmers work	Unauthorized changes to software components	Software; Date
Facilities improperly configured security applications	Unauthorized access to data; Theft and fraud	Date
Security measures implemented improperly	Unauthorized access to data and software components	Software; Date
Absence of intrusion detection software	Unauthorized access	Software; Date
Lack of physical security of premises communications equipment	Destruction of data and facilities; unauthorized access to data	Installations hardware
Lack of policy to use only licensed software components	Using pirated software	Date
The absence of regularly updating antivirus software	Malicious code	Software; Date

Vulnerability	Threat	Affected assets
Lack of use of digital signatures	Denial of service	Date
Locating system in an area susceptible to voltage fluctuations	Fluctuation of the supply voltage	Installations
Sending unencrypted classified data	Unauthorized access to data	Date
Unauthorized copying data/software	Use of pirated software	Software; Date
Unencrypted passwords of users	Unauthorized access	Date
Unsuitable for Firewall Policies	Unauthorized access to data	Date
Absence Firewall	Unauthorized access to data; unauthorized changes to software; data destruction	Software; Date

On the other hand, threats to computer systems fall into two main categories: intentional and accidental. Intentional threats have a great diversity, permanently enlarged over the last few years and are aimed especially at computer-specific products. Attacks can come from inside or outside. Some types of attacks can only come from certain types of attackers. Intentional attacks can only be organized by those who have significant resources (Chen *et al.,* 2015).

Accidental threats may be due to administrators and poorly trained users, who have not been properly trained, who have not read the required documentation or who do not understand important to comply with the security measures in place (McQuade, 2006). A system administrator may change by accident or complete ignorance of the protection mechanisms, certain rights to files and software subsystems, which determine either the inaccessibility of an application or data, or the public exposure of confidential data domains. Specialists appreciate that much more losses are recorded because of ignorance than bad intentions.

Communication interception is another problem in computer networks. It can be active and passive. Passive interception affects the confidentiality of the transmitted information but does not change it. With a simple connection or a loop for connecting to the communication lines, several types of communication can be successfully intercepted. Active interception already involves coupling to the communication lines used in the respective network and deliberately modifying the information, affecting their authenticity (Kshetri, 2014).

The refusal of a service is not only a problem of networks, but also of operating systems. If someone interrupts the power supply, fills the disks, or creates as many processes as the system can withstand, no one will be able to work and the system crashes (Singer and Friedman, 2014).

Controlling access to the system ensures that unauthorized users cannot enter the system and encourages (sometimes even forces) authorized users to be aware of the need for computer security. The control of access to the system is implemented by periodically changing their own passwords, notifying unauthorized entries in the system or attempts to open a file, notifying the use of special privileges in case of sensitive connections, notifying access to a local network from a system independently, or even from a workstation on another network (Fischbacher-Smith, 2016). Data access control ensures the monitoring of the persons who have access to data, the type of data accessed and the purpose of the access. The system must support selective access control, allowing a user to determine whether others can read or modify their data (Hong *et al.,* 2010).

The administration of the system and the implementation of the security policy consist in the development, planning and carrying out of independent procedures that make a system secure and follow the delimitation of the responsibilities of the system administrator, proper training of the users and their control, to be sure that the security policies are respected. There are many standards and sets of rules set in large organizations and institutions that regulate most aspects of network management and networked workstations (Hadžiosmanović *et al.,* 2012). The architecture of the computer systems and the computer networks, as a result of the system design (especially in a computer system that handles confidential data) is based on, besides the performance criteria and possibly cost, clear criteria and rules regarding the security of the respective system (Malatras *et al.,* 2016).

Encryption is another important method of protecting sensitive information stored in computing systems, but also of those transmitted over communication lines. Encryption of e-mail messages transmitted over the network protects the information in case an intruder enters the network (Broadbent and Schaffner, 2016). The information that is encrypted remains secure even if transmitted through a network that does not provide strong intrinsic security because even in the case of interception it cannot be understood directly.

3. Results and discussions

Networks create serious security concerns because the exploitation of even a small vulnerability can have serious consequences and damage can spread quickly to other systems or interconnected networks. Against the background of the

current and growing trends of development on a global scale of the information society, specialized applications are accessed, modified or destroyed by generating and disseminating viruses that may harm the interests of particular companies and individuals (Cho *et al.,* 2018). Although most security systems target intruders from outside, studies show that most attacks come from within. It has been estimated that 80% of successful attacks on an institution's computing systems come from authorized users who abuse their rights to perform unauthorized operations (Zikopoulos *et al.,* 2011).

In network communications, a variant of integrity called authenticity, offers a way of verifying the origin of the data, by determining the one who introduced or sent them, by recording the sending and receiving data. In the financial environment, accuracy is usually the most important aspect of security (Renwick and Martin, 2017). For banks, for example, the confidentiality of financial transactions is often less important than verifying the accuracy of these transactions. The increasing use of electronic payment technology for commercial transactions involving large sums of money is the main cause of computer fraud used by computer networks (especially the Internet) to "launder" money. Massive thefts from banks by entering their private networks, commercial espionage and other possible computer crimes. In the network projects, the following aspects must be taken into account, during the physical placement of all the equipment:

- the location of the equipment to meet the maximum technical criteria functionality, as well as the existing physical protection norms imposed by each equipment and not only some norms imposed by an organizational structure of the moment, the structure subject to changes, more often than the structure of the computer network;
- the operation of placing the equipment must comply with the existing internal regulations;
- to consider the opportunity of using only the equipment modern, very well protected.

A computer system must ensure the accessibility of information for all its users. Accessibility means that all the hardware and software components of the computing system work efficiently and that the system is capable of rapid and complete self-recovery in the event of disasters. The opposite of accessibility is the refusal of services. This means that users can no longer access the resources of the computing system.

The systematic evaluation of the informational structure of the organization assume to determine the effectiveness of current information security solutions and to identify weaknesses and vulnerabilities (vulnerabilities classified as conceptual, implementation and configuration). In general, the weaknesses of the system are determined based on a variety of automated tools, including tools for testing the integrity of files, antivirus, and system efficiency by limiting access passwords, security communications, and many other instruments.

4. Conclusions

The protection methods specific to the information technology of today are varied, depending on the type of vulnerabilities they protect. There is a border between the different forms of security: technical, civil, people and goods, etc., as there are delimitations between the measures aimed at prevention or intervention with repressive tendency. However, to be successful in today's market, we must have a reliable, robust e-business structure with high availability and scalability.

Companies operating in the online environment will have to pay extra attention the web applications and web sites that its develop. Criminals will try to exploit any vulnerability in web applications present to take possession of information about users (name, accounts, passwords, email addresses) for later use in activities phishing or spam. Periodic auditing of websites and web applications will be essential for companies online.

In addition, policies and products that provide computer security can reduce the likelihood that an attack will penetrate defense systems, or force those interested, to invest so much time and so much resources that they would rather give up. Also, the own assessment of the type of security required by the protected system will influence the choice of particular security techniques or products, necessary to meet the imposed requirements.

The next period will be marked by a number of economic challenges that companies will have to face in a most professional and least cost. Securing IT infrastructure on all levels will be crucial to the smooth running of any company activites in the period ahead.

Acknowledgement

This work is supported by project POCU 125040, entitled "Development of the tertiary university education to support the economic growth - PROGRESSIO", co-financed by the European Social Fund under the Human Capital Operational Program 2014-2020

References

Andress, A. (2003). Surviving Security: How to Integrate People, Process, and Technology. Auerbach Publications, Boca Raton, FL, USA.
Arukonda, S., & Sinha, S. (2015). The innocent perpetrators: reflectors and reflection attacks. Advanced Computer Science, 4, 94–98.
Broadbent, A., & Schaffner, C. (2016). Quantum cryptography beyond quantum key distribution. Designs, Codes and Cryptography, 78(1), 351- 382.
Chen, C. L. P., & Zhang, C. Y. (2014). Data-intensive applications, challenges, techniques and technologies: A survey on big data. Information Sciences Journal, 275(1), 314-317.
Chen, H., Ge, L., & Xie, L. A. (2015). User Authentication Scheme Based on Elliptic Curves Cryptography for Wireless Ad Hoc Networks. Sensors, 15, 17057-17075.
Choi, Y., Lee, D., Kim, J., Jung, J., Nam, J., & Won, D. (2014). Security Enhanced User Authentication Protocol for Wireless Sensor Networks Using Elliptic Curves Cryptography. Sensors, 14, 10081-10106.
Da Veiga, A. (2016). Comparing the information security culture of employees who had read the information security policy and those who had not: Illustrated through an empirical study. Information & Computer Security, 24(2), 139-151.
Dor, D., & Elovici, Y. (2016). A Model of the Information Security Investment DecisionMaking Process. Computers & Security, 63, 1–13.
Eastin, M. S., Brinson, N. H., Doorey, A., & Wilcox, G. (2016). Living in a big data world: Predicting mobile commerce activity through privacy concerns. Computers in Human Behavior, 58(1), 214-220.
Fenz, S., Heurix, J., Neubauer, T., & Pechstein, F. (2014). Current challenges in information security risk management. Information Management & Computer Security, 22(5), 410-430.
Fischbacher-Smith, D. (2016). Breaking bad? In search of a (softer) systems view of security ergonomics. Security Journal, 29(1), 5-22.
Gandino, F., Celozzi, C., & Rebaudengo, M. (2017). A Key Management Scheme for Mobile Wireless Sensor Networks. Applied Sciences, 7, 490.
Hadžiosmanović, D., Bolzoni, D., & Hartel, P.H. (2012). A log mining approach for process monitoring in SCADA. International Journal of Information Security, 11(4), 231-251.
Hjortdal, M. (2011). China's use of cyber warfare: Espionage meets strategic deterrence. Journal of Strategic Studies, 4(2), 1–24.
Hong, J., Kim, J., & Cho, J. (2010). The trend of the security research for the insider cyber threat. International Journal of Future Generation Communication and Networking 3 (2), 31–40.
Karim H. V. (2007). Strategic security management: a risk assessment guide for decision makers, Elsevier Inc.
Kshetri, N. (2014). Big datas impact on privacy, security and consumer welfare. Telecommunications Policy, 38(11), 1134-1145.
Malatras, A., Geneiatakis, D., & Vakalis, I. (2016). On the efficiency of user identification: a system-based approach. International Journal of Information Security, 15(1), 1-19.
McQuade, S. (2006) Understanding and Managing Cybercrime. Boston, MA: Allyn & Bacon.
Renwick, S.L.; & Martin, K.M. (2017). Practical Architectures for Deployment of Searchable Encryption in a Cloud Environment. Cryptography, 1, 19.
Singer, W.P., & Friedman, A. (2014). Cyber Security and Cyber War: What Everyone Needs to Know, New York: Oxford University Press.
Singh, A., & Fhom, H.C.S. (2017). Restricted usage of anonymous credentials in vehicular ad hoc networks for misbehavior detection. International Journal of Information Security,16(2), 195-201.
Strang, K. D., & Sun, Z. (2017). Scholarly big data body of knowledge: What is the status of privacy and security? Annals of Data Science, 4(1), 1-17.
Willems, E. (2011). Cyber-terrorism in the process industry. Computer Fraud & Security, 3, 16 – 19.
Zikopoulos, P., Eaton, C., DeRoos, D., Deutsch, T., & Lapis, G. (2011). Understanding Big Data: Analytics for Enterprise Class Hadoop and Streaming Data. McGraw-Hill Osborne Media, NY.