Advanced Engineering Days

aed.mersin.edu.tr

Security in the components of information systems

Fatmir Basholli [*1], **Rezar Mezini**[2], **Armand Basholli** [3]

[1]*Albanian University, Department of Engineering, Tirana, Albania, fatmir.basholli@albanianuniversity.edu.al*
[2]*Vodafone Albania, Head of Corporate Security, Tirana, Albania, rezar.mezini@vodafone.com*
[3]*Vodafone Albania, Head of Property, Tirana, Albania, armand.basholli@vodafone.com*

Cite this study: Basholli, F., Mezini, R., & Basholli, A. (2023). Security in the components of information systems. Advanced Engineering Days, 7, 185-187

Keywords
Systems
Technology
Integrity
Security
Information

Abstract

The security aspects of information systems in the public and private sector are very important, because these are often part of critical national security infrastructures. Although the size of the public sector varies in different countries, it usually includes all government infrastructure and various levels of local government, which consist of many smaller organizations scattered throughout the country. Today, even in the private sector, is being invested in the use of technology and security aspects. The purpose of this paper is about the processes, policies, procedures, and other documents that public and private sector organizations possess and use in the field of security and information systems. Through this paper, I think we contribute to understanding how these institutions or private companies stand against national and international standards and best practices in the field of security of components in information systems.

Introduction

We emphasize that information systems planning, development, operation and management by organizations and sectors takes place in a very specific context that presents special challenges. Institutions, public and private sector organizations are often tasked with procurement, employment, property management, remuneration procedures with inflexible salaries and operate within an institutional framework that is not easily changeable. These factors contribute to a variety of issues and difficulties related to the security of information systems components. Today, even in the private sector, is being invested a lot in the use of information technology, where personnel enjoy the advantages offered by technology in performing their daily work. Confidential information, company technology secrets, financial data, computer equipment and security issues are at risk if security procedures are not followed properly. The main responsibility of each user includes the data security and the telecommunications network used. The paper aims to address some other aspects in the field of information security, focusing on the issues of physical security of the facilities where these organizations operate, bearing in mind the possible limitations in human and financial resources [1-3].

Material and Method

Reviewing the literature related to the concept of information security, the history of security and its principles, we keep in mind:

The concept of Information Security, which includes the application of measures to ensure the security and privacy of data by managing their storage and distribution. Information security has both technical and social implications. Information security system is the process of data protection from unauthorized access, disclosure, or destruction [4-5]. The history of Information Security begins with security in telecommunication networks. The need for information systems security, i.e., the need to secure physical sites from threats, hardware, and software, was addressed as early as World War II, when the first analog computers (mainframes), developed to help in the calculations for breaking communication codes, were used. Access to sensitive military sites and security facilities

is initially controlled by means of personal cards, keys and facial recognition of personnel authorized by security personnel. The growing need to maintain national security eventually led to more complex and sophisticated defense measures utilizing today's technological advances [6-7]. The principles of Information Security, the CIA triangle, can be found in almost every security book today. The CIA triangle (**c**onfidentiality, **i**ntegrity, and **a**vailability) is useful in helping people think about security in direction of the most important aspects of information protection. The CIA concept is not perfect. The CIA focuses on three aspects of information protection that really are important, but this is not a comprehensive model. Alternatives to the CIA triad that include other aspects of security have been proposed by dissenters in the security profession (Figure 1).

Figure 1. The triangle CIA (**C**onfidentiality, **I**ntegrity, and **A**vailability)

The purpose of security in the components of information systems is to prevent unauthorized access (confidentiality) or modification (integrity) of data while maintaining access (availability). From this we conclude that the value of information consists of the characteristics it has. When a characteristic of information changes, the value of this information either increases or decreases. Some characteristics affect the value of information to users more than others. Confidentiality refers to restricting access to data only to those who are authorized to use it. In general, this means that a single set of data is accessible to one or more authorized people or systems, and no one else can see it [8-10]. Integrity means that the information is useful and reliable only if it is correct and has not been modified without the author's consent and approval. "Integrity" must be adequately protected by means such as appropriate authentication, routing protocols, proper configuration of systems and application security. ISO 27000 - ISO 27006 refers to integrity as the ability to maintain the accuracy and completeness of assets (data). Availability has to do with the systems (place) where the database is stored, on disk or more recently in the cloud. The rapid developments in information technology, the speed of decision-making is important, where the availability of important information at any time has become very necessary. Unlike confidentiality and integrity, which deal with the context of the data contained in computer systems, availability refers keeping the service of computer information technology systems functioning by ensuring that the service will be available when it is needed. Availability is one area where developments in technology have significantly increased the challenges for information security professionals.

Results and Discussions

Information systems are collections of interrelated elements that work together for a specific purpose. Information systems (IS) are defined as a set of interrelated components that work together to perform input, processing, output, storage, and control operations to obtain information from data conversion, which can be used to support forecasting, planning, control, coordination, decision-making and operational activities in an institution or facility. Hardware and software are usually mentioned as part of information systems, but apart from these there are also other important components. The software component of includes applications, operating systems, and various software tools. Software is probably the most difficult component to secure. Exploiting errors made during software programming constitutes a significant part of information attacks. Hardware is the physical technology that carries and executes software, stores, and transports data, and provides the means for inputting and outputting information from the system. Physical insurance policies deal with hardware as a physical asset and with the protection of physical assets from damage or theft [11]. The application of traditional physical security tools, such as locks and keys, restrict access and interaction with the hardware components of an information system. Securing the physical location of computers and securing the computers themselves is important because a breach of physical security can result in information loss. Hardware components have always played a major role in computer security. Over the years, this role has grown exponentially, due to increased processing power, communication capacities and capabilities, as well as decreased cost and component size. Inexpensive, powerful, easily accessible network devices present significant challenges to computer security. Data stored, processed, and transmitted by a computer system must be protected. Data is often the most valuable asset

possessed by an organization and is the main target of deliberate attacks. Another important aspect is data classification.

Information classification, related to information security, is about placing information into categories that indicate how this information should be handled in relation to access control and maintaining confidentiality. Although often overlooked in aspects of computer security, humans have always been a threat to information security. It is often thought that people can be the weakest link in an organization's information security system. The information security culture must support all activities so that information security becomes a natural aspect in the daily activities of every employee (user), that the development of the information security culture must result in changes in employee behavior. Developing information security culture can lead an employee to act as a kind of "human firewall" to protect organizational assets (information). This means that employees must perceive safety practices as part of their daily work routine. Without proper employee security perception, an organization will remain highly exposed to security threats and deficiencies. The information security procedures are instructions for carrying out a process. The computer networks are components of SI that are used by increasing computer and information security. The latest challenge has been created by the increasing popularity of wireless networks [12-13].

Conclusion

The organization of trainings with users of information technology equipment is an aspect that has room for significant improvement in the field of cyber hygiene, where risk management should be more than a simulated control exercise. Information security isn't something you buy, it is something you develop, and you must have talented people to do it right. Security in the components of information systems is a social responsibility. We all have a role to play. Trust in technology is a good thing, but controlling it is even better.

References

1. Fred, B., Schneider, G., Mark, K., Hill, D., & David J. F. (2019). Challenges and Opportunities in Cybersecurity Research.
2. Dawson, J., & Thomson, R. (2018). The future cybersecurity workforce: Going beyond technical skills for successful cyber performance. Frontiers in psychology, 9, 744. https://doi.org/10.3389/fpsyg.2018.00744
3. Basholli, F. (2022). Cyber warfare, a new aspect of modern warfare. International Scientific Journal Security & Future, 5(2), 72-75
4. Perwej, Y. (2019). The hadoop security in big data: a technological viewpoint and analysis. International Journal of Scientific Research in Computer Science and Engineering (IJSRCSE), 7(3), 1-14. https://doi.org/10.26438/ijsrcse/v7i3.114
5. Aslan, Ç. B., Sağlam, R. B., & Li, S. (2018, July). Automatic detection of cyber security related accounts on online social networks: Twitter as an example. In Proceedings of the 9th international conference on social media and society (pp. 236-240).
6. Škrjanc, I., Ozawa, S., Ban, T., & Dovžan, D. (2018). Large-scale cyber attacks monitoring using Evolving Cauchy Possibilistic Clustering. Applied Soft Computing, 62, 592-601.
7. Mittal, S., Das, P. K., Mulwad, V., Joshi, A., & Finin, T. (2016, August). Cybertwitter: Using twitter to generate alerts for cybersecurity threats and vulnerabilities. In 2016 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM) (pp. 860-867). IEEE.
8. Foroughi, F., & Luksch, P. (2018). Data science methodology for cybersecurity projects. arXiv preprint arXiv:1803.04219.
9. Apruzzese, G., Colajanni, M., Ferretti, L., Guido, A., & Marchetti, M. (2018, May). On the effectiveness of machine and deep learning for cyber security. In 2018 10th international conference on cyber Conflict (CyCon) (pp. 371-390). IEEE.
10. Boussi, G. O., & Gupta, H. (2020, June). A proposed framework for controlling cyber-crime. In 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO) (pp. 1060-1063). IEEE.
11. Daberdini, A., Basholli, F., Metaj, N., & Skenderaj, E. (2022). Cyber security in mail with Fortiweb and Fortinet for companies and institutions. Advanced Engineering Days (AED), 5, 81-83.
12. Williams, C. M., Chaturvedi, R., & Chakravarthy, K. (2020). Cybersecurity risks in a pandemic. Journal of medical Internet research, 22(9), e23692.
13. Wu, S., Chen, Y., Li, M., Luo, X., Liu, Z., & Liu, L. (2020). Survive and thrive: A stochastic game for DDoS attacks in bitcoin mining pools. IEEE/ACM Transactions on Networking, 28(2), 874-887.