j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 6, No:4. 2023

The Impact of Information Security Processes on Providing Secure Digital Systems

[1]Balsam A. Mustafa, [2]Fadhil .A. Al-Qirimli

[1&2] *College of Engineering Technical, Uruk University, Baghdad, Iraq.*

Babidah331@gmail.com

Abstract With the increasing use of the internet, a global network, Information security is a substantial issue in today's business. Information security has become one of the most important aspects of modern electronic society. Security of information, networks, and systems is vital to make information systems work satisfactorily and enable people to safely get the information they need. Security is the practice of defending information from unauthorized access. This paper discusses the essential characteristics of secure communication and the important processes used by administrators to protect data and systems.

10.36371/port.2023.4.4

Keywords: *Security attributes, Authentication, Authorization, User identity, Access control*

1. INTRODUCTION

Today's society is aware of the threats associated with the internet, a global network that connects millions of computers to enable communication and quick access to information from anywhere. The possibility of information being altered, stolen, or used improperly is one of the major concerns. Cybersecurity is seen as occurring whenever unauthorized access is made to a system or network with the intention of damaging that system's data. Information security is described as "protecting information and its vital parts, including the systems and hardware that use, store, and transport that information" by the Committee on National Security Systems (CNSS) in the United States [1]. Common logic dictates that as technology develops, humans will be responsible for both the benefits and the harm.

Personal information, contact details of staff, customers, secret business plans for the foreseeable future, trade secrets, **Confidentiality**: When unauthorized individuals can read or copy data from a system, confidentiality is compromised. This includes information about health and patients, personal bank and credit card information, information about intellectual property, inventions, and patents, exam results, names of people or organizations that provide services like drug rehab or psychological counseling, as well as contact information for employees, clients, and students. Because it fosters respect and trust in the workplace, stops information from being misused, and safeguards people's and organizations' reputations, confidentiality is crucial [3].

inventions, and other information that gives the company a competitive edge are among the crucial information that needs to be kept private for people and organizations.[2]

Through a variety of methods, such as hacking, viruses, worms, denial of service attacks, spamming, mobile malware, etc., attackers may gain access to computer systems without the knowledge of the person or organization using them [2]. This severe damage could prevent the systems from functioning properly and deny service to authorized use

2. ESSENTIAL SECURITY ATTRIBUTES

Confidentiality, integrity, and availability are the core security requirements in relation to online information. Authentication, Authorization, and Nonrepudiation are ideas pertaining to information users to ensure the above security features. The primary needs for safe communication and security management are these security features which will be discussed [4].

Integrity: It can be described as the characteristic that data hasn't been changed without authorization [5]. When information is accessible across an insecure network, it can be perverse. Loss of integrity is the term used to describe when information is transformed in unanticipated ways. This indicates that information is altered by uninvited parties.

Balsam A. Mustafa, Fadhil. A. Al-Qirimli, 2023. The Impact of Information Security Processes on Providing Secure Digital Systems. *Journal port Science Research*, 6(4), pp. 344-347. https://doi.org/10.36371/port.2023.4.4

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 6, No:4. 2023

Errors in hardware, software, human interaction, and invasions all have an impact on integrity [6]. In order to preserve information security, access permission is a crucial issue. Integrity is crucial for crucial financial and safety data utilized in processes like air traffic control, electronic fund transfers, and financial accounting.

Availability*:* "Timely, dependable access to data and information services for authorized users" is how availability is defined by [7]. One threat to information security is the denial of service (DoS) attack, which aims to make a user-accessible information resource inaccessible [8].

In contrast, the availability attribute indicates that authorized users can access information and related resources whenever they need to. [9] stated that a number of factors, including system software, hardware, and network, affect the availability of information. Dependency on the network is crucial because users who are unable to use the network or particular services it offers will be subject to "denial of service." In service-oriented industries that rely on information like (airline schedules), availability is crucial.

Organizations use authentication and authorization because the permission should only be granted to those who can be trusted with the information in order to offer users access to the data they need to utilize.

3. AUTHENTICATION AND AUTHORIZATION

The two vital information security processes to safeguard systems and data are authentication and authorization. "The technique that enables recognition of a user described to an automated data processing system" [10] is the definition of authentication. This indicates that a user authenticates themselves to a computer system by providing certain information, such as a user name and password, in order to log into a system. The system validates the submitted identification and grants access to the user. The research of [10] highlighted various issues with this authentication mechanism, one of which is that passwords are difficult to remember, particularly when they are long and unpredictable, and become harder to remember over time. It becomes more challenging if users must memorize unique passwords for every service offered by a system, particularly if the system offers several services. Using single sign-on on the network, which enables users to sign on once to a system throughout the session even if they are using multiple services of the system, is one solution offered to address this issue [10].

Various identity-providing techniques in the context of computer security make advantage of the user's biometric traits. The user can be verified if the attributes are distinct for each individual. Think about voice, face, and fingerprint recognition as examples. Despite the fact that fingerprint automation technology is widely used in biometric-based authentication systems due to its convenience and low error rates, research [11] revealed that there are a number of issues with this technique, the most significant of which is the quality of the fingerprint image, which has a significant impact on the performance of the entire system. More research is still required to accurately capture a fingerprint digitally without distortion or a low-quality partial image in order for the device to function as intended.

Simply put, authorization is the right of access to network services and applications. After a user has been authenticated, authorization is the next stage. Based on rules and access policies for particular user types, authorization enables users to access various levels of information and execute functions. Verifying the files, data, and programs a user is authorized to access is the process of authorization [12]. Access to users should be restricted to those who are authorized to do so. A individual working in an organization's financial department, for instance, shouldn't have access to personnel information and records.

Authorization limits access to a secured component based on a user's access privileges, i.e., they are unable to access files or information that is prohibited by their position within the organization. According to [13], there are various methods for defining access rights, or the necessary elements and how they work together. Three main elements describe an authorization model: Object is the system entity that needs protection (such as a file, database table, or record), Subject is the active entity (such as a user, group, or organizational position) that requests access, and Action specifies what the Subject can do with the Object (e.g. access right, type of activity).

Both, authentication and authorization are security processes that prevent unwanted access to a secured system.

3.1 How Authentication Works

The basic objective of authentication is to demonstrate the user's identity through authentication techniques such usernames and passwords, biometric data like fingerprint or facial recognition scans, and phone or text confirmations [14]. The procedure for identity authentication using a login and password (the most popular type of authentication) is as follows:

1. The user sets up a username and password to access the desired account. The server then stores those logins.
2. The server compares the user's login credentials to those stored in its database as the user begins to log in using his unique username and password. The user can access the system if they match.

3.2 Types of Authentication

1) Single-Factor Authentication

To access a system, single-factor authentication (SFA) or one-factor authentication utilizes a login and password. Although this is the most widely used and recognized type of authentication, it is regarded as having low security [14]. Single-factor authentication just offers one barrier, which is

Balsam A. Mustafa, Fadhil. A. Al-Qirimli, 2023. The Impact of Information Security Processes on Providing Secure Digital Systems. *Journal port Science Research*, 6(4), pp. 344-347. https://doi.org/10.36371/port.2023.4.4

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 6, No:4. 2023

its fundamental flaw. To access the system, burglars merely need to take the login information. Moreover, employing weak passwords, exchanging admin credentials, and reusing passwords all make it much simpler for hackers to guess or discover them [15].

2) Two-Factor Authentication

The usage of two-factor authentication (2FA) adds an extra degree of security to users' capacity to access networks and systems. Two factors of authentication from the three categories are needed with 2FA rather than just one:

- Something you know (i.e., username and password)
- Something you have (e.g., a smart card)
- Something you are (e.g., biometric credentials)

With two-factor authentication, it is also essential to add a factor from the other two categories as a second tier of security on top of providing a user name and password as a first line of defense [15].

3) Three-Factor Authentication

The use of three independent authentication factors—one from something you know, one from something you have, and one from something you are—is known as three-factor authentication (3FA) [15].

4. EMERGING AUTHENTICATION TRENDS

It is apparent that when cybercrime and malicious assaults rise, security threats do as well, growing in complexity. To offer more security against damaging attacks, authentication techniques must be continuously improved. To guarantee secure access across industries, it is anticipated that newer and more sophisticated authentication mechanisms will be used. The ability to improve and enhance biometric authentication capabilities will be one of the key developments [3]. This is crucial because, according to "Statista" [16], a statistics platform for industry data, the global biometric system market is anticipated to grow dramatically over the next several years, reaching a value of $83 billion by 2027.

Adaptive authentication will be a significant area of expansion. The next iteration of multi-factor authentication (MFA) makes use of machine learning and artificial intelligence (AI) to recognize additional user data, such as location, time, and device, to monitor login attempts and lock any questionable access activity [12]. AI has also been crucial in developing automated security systems and enabling threat detection systems to foresee new assaults and promptly alert admins to any data breach.

5. CONCLUSION

As a result of the digital transformation that is affecting all businesses, big and small, corporations, organizations, and even governments, are becoming more and more reliant on computerized systems to manage their daily operations. In today's world, securing data from numerous online risks and any illegal access has taken precedence, making cyber security an imperative necessity.

Authentication and authorization processes, which are essential for protecting data and networks against malicious attacks and preventing unauthorized access to a secured system, were reviewed in this article together with the essential components of secure information.

REFERENCES

[1] National Security Telecommunications and Information Systems Security (1994). National Training Standard for Information Systems Security (Infosec) Professionals. File 4011

[2] The Importance of Information Security, https://pecb.com/article/the-importance-of- information-security-nowadays accessed on 14/02/2023

[3] Dutta,N. , Jadav, N. , Tanwar, S., (2022). Cyber Security: Issues and Current Trends, Springer publisher

[4] Siponen, M. T., Kukkonen, H., (2007). A review of information security issues and respective research, The DATA BASE for Advances in Information Systems, 38(1)

[5] Nieles, M., Dempsey, K., Pillitteri, V., (2017). An Introduction to Information Security, NIST Special Publication 800-12 Revision1

[6] Talha, M., Abou El Kalam, A., Elmarzouqi, N., (2019). Big Data: Trade-off between Data Quality and Data Security. The 9th International Symposium on Frontiers in Ambient and Mobile Systems (FAMS2019), Leuven, Belgium

Balsam A. Mustafa, Fadhil. A. Al-Qirimli, 2023. The Impact of Information Security Processes on Providing Secure Digital Systems. *Journal port Science Research*, 6(4), pp. 344-347. https://doi.org/10.36371/port.2023.4.4

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 6, No:4. 2023

[7] Martin, A., Khazanchi, D., (2006). Information Availability and Security Policy, Proceedings of the 12th Americas Conference on Information Systems, Mexico, 2006

[8] Whitman, M.E. (2003). Enemy at the Gate: Threats to Information Security, Communications of the ACM, 46, 91-95

[9] Qadir, S. and Quadri, S.M.K, (2016). Information Availability: An Insight into the Most Important Attribute of Information Security. Journal of Information Security, 7, 185-194

[10] Alenius, F., (2010). Authentication and Authorization, Achieving Single Sign-on in an Erlang Environment, UPSALA UNIVERITET, Independent thesis Basic level

[11] Uliyan, Diaa M., Sadeghi, S., Jalab, H., (2020). Anti-spoofing method for fingerprint recognition using patch based deep learning machine. Journal of Engineering Science and Technology, 23(2), 264-273

[12] Kizza, J.M. (2020), Access control and authorization. Kizza, J.M. (Ed), Guide to Computer Network Security Texts in Computer Science, Springer Publishing, pp. 187-206, ISBN 978-3-030-38140-0

[13] Mohamed, A.K.Y.S., Auer, D., Hofer, D., Küng, J. (2022), A systematic literature review for authorization and access control: definitions, strategies and models, Journal of Web Information Systems, Vol. 18 No. 2/3, pp. 156-180

[14] B. Madhuravani, P. Bhaskara Reddy (2013). A Comprehensive Study on Different Authentication Factors, 2(10), ISSN: 2278-0181

[15] Matt, B. (2018), Computer Security: art and Science, Addison-Wesley Professional, ISBN 978-0-13-409714-5.

[16] Statista Report, https://www.statista.com/statistics/1048705/worldwide-biometrics-market-revenue/ accessed on 14/02/2023

Balsam A. Mustafa, Fadhil. A. Al-Qirimli, 2023. The Impact of Information Security Processes on Providing Secure Digital Systems. *Journal port Science Research*, 6(4), pp. 344-347. https://doi.org/10.36371/port.2023.4.4