Journal of Computer and Engineering Technology 7 (1)
© Nabu Research Academy, 2020

Information Security Protection and Threats vulnerabilities: A survey

Sarah Ali Abdulkareem , Israa Mishkhal, Haider Ali Jasim Alshamary

SaraAli@sport.edu.iq , iamishkhal@gmail.com, haider.alshamary@uodiyala.edu.iq

Abstract

The development of worldwide web and the use of internet in all modern live branches developed the amount of information extracted from different types of networks. Information security is one of the most used scientific term in protecting collected information and using them in researches to develop theories and extract useful information by mining the collected data. The use of information through internet in multiple life branches like social live, learning, medical clinics and hospitals, militaries, industries, business and agricultural led to develop threats and vulnerabilities. In this research, the researcher surveyed different types of risks and threats on information's that we need to secure. Detected some information levels of security. Explained types of threats and how to choose the level of security according to the importance of data and data types that needs to be protected. The researcher concluded by the main data protection purposes, Information security zones, Patterns and levels of information security.

Introduction

According to the development of information, the term information security became one of the most used in using, processing and interaction with data through multiple types of networks. Researches and studies that contribute to maintaining the confidentiality of various type of information, including military, medical, agricultural and industrial information that presented through information technology. Information security is the science that researches the theories and strategies of information to provide protection for important information from threats and attacks, such as penetration, manipulation and theft [1].

The development of information security from a technical or performance point of view for protecting information security[2] has accompanied the tremendous development in the development of informatics with the development in information mining and its importance in several aspects such as:
* Confidentiality or Privacy: It is the privacy of information related to clients or the organization in order to ensure that information is not penetrated or accessed by un authorized.
** Complementarity and integrity of the content: to ensure that the information content is correct and has not been modified or tampered with, and in particular the content will not be destroyed, altered or tampered with at any stage of processing or exchange, whether in the stage of internal dealing with information or through illegal interference .
*** The availability of information or service: - Ensure that the information system continues to operate and the ability to interact with information and provide service to informational sites, and that the information user will not be prevented from using it or entering it.
****The copyrights for the information: Not to deny the sources of the information quoted and what is intended to ensure that the person who quoted the information does not attribute it to himself and he must mention what is related to the information and its locations in order to preserve intellectual property.

The information security

Ensuring all or some of the information security elements depends on how the information and its uses are protected and on the services related to it. Not all information requires confidentiality and ensuring non-disclosure and not all information of high importance in terms of access to it or ensuring that it is not tampered with. This is why information security plans start from the answer to a series of consecutive questions[3],[4] : -

What should we protect?

What should we protect? [5] The answer to this question determines the classification of data and information in terms of the importance of protection, as the information is classified according to each case separately, from information that does not require protection, to information that requires maximum protection.

What are the risks that require high information protection?

The risk identification process begins with visualizing every risk that may affect the protected information or threaten its security, from cutting off the electricity source to the computer to the risks of penetrating the system from the outside with one or more means of penetration through vulnerabilities[6]. Employees misuse of their passwords. These risks are classified in lists according to the basis of classification, and they are classified as risks in terms of their source, means of implementation, purpose of those responsible for these risks, their impact on the protection system and on information.

What are the best protection measures?

Here, each facility and each agency find its own way to provide security from risks and within the limits of the specific information protection, requirements that have been identified, the limits of its financial capabilities and the budget allocated to protection. Security measures should not be lax and weak and do not guarantee protection or exaggerated to an extent that affects the performance element of the system Subject of protection[7]. If we imagine a person who wanted to protect the money in his home. It is acceptable to place it in an iron clipper, for example, and put a protective iron on the windows of the house, or set an alarm bell for any intrusion into the house, and perhaps these three means can be accepted to provide security from the activities of stealing. [8] However, it is not logical, but it is an exaggeration for this person to protect his money by placing guards on his home, and this is what we call the effect on the health and effectiveness of performance. Therefore, the protection measures are based on the appropriate protection needs. In case of increasing limits, they will have a negative impact on performance, so the site or system becomes slow and ineffective in the performance of its normal tasks, and if it falls below the required limit, weaknesses increase and become more vulnerable to internal and external penetration [9].

Threats detection when they arise?

It includes successive stages, starting from the stage of the technical, administrative, media and legal procedures necessary when the threat occurs, and the stage of analysis procedures for the nature of the risks that occurred, the reason for their occurrence, and how to prevent their occurrence later. Finally the procedures for recovery and return to normal before the danger occurs, taking into account the implementation of what the analysis showed about how the risks occurred and ensuring that they did not happen.

When some information are required such as national security and military secrets, for example, the two elements of secrecy and complementarity are given the utmost attention. [10] For banking securities, in addition to the two advanced elements, the system itself must give an element of continuity the same importance, if banks work in the field of electronic banking or electronic banking services, the element of non-repudiation is just as important. Internet sites for example, require the element of continuity to be given the greatest attention. However, e-commerce sites are among the Internet sites require diligence to provide the four elements protection of equal importance, as they need to ensure confidentiality. With regard to customer data, such as credit card numbers, require integrity and safety in relation. [11] For data exchanged via e-mails between the customer and the site, the purchase order does not arrive, for example, it has been altered or corrupted, and requires the continuity of the site in providing its services and the customer’s ability to access it throughout the validity of the browsing and purchase process. But, at any time the user wants to enter the site, and requires a guarantee that it will not The customer’s denial that the behavior he performed on the site (such as a purchase order) was issued by him, or the site’s own denial that he had contracted with the customer in a certain matter.

Risks and attacks in the information environment

[12],[13] Risks and attacks in the information environment affect four basic aspects, which are the components of information technology in its most recent manifestations:

• Devices: - They are all the equipment and physical tools that make up the systems, such as screens, printers, their internal components, physical storage media, and others.

• Programs: These are the orders that are arranged in a specific order to accomplish the work. They are either independent of the system or stored in it.

• Data: - It includes all entered data and information extracted after processing it, and extends in a broad sense to the software stored within the systems. The data may be in the process of input, output, storage, or exchange between systems over networks, and it may be stored inside the systems or on external storage media.

• Communications: - The communication networks that connect technology devices include each other locally, regionally and internationally, and provide an opportunity to penetrate the systems through them as well as being in themselves a place of attack and a real danger. The focus of danger is the human being, whether the user or the person assigned to him with certain technical tasks related to the system. This person's perception of the limits of his powers, his awareness of the mechanisms of dealing with danger, and the safety of control over his activities within the limits of respecting his legal rights, are major issues concerned with the comprehensive security system, specifically in the work environment based on computer systems and databases.

Key information operations related to information security

There are many processes for dealing with information in the systems environment, processing techniques, communication and data exchange, but in general the following main processes can be identified[14],[15]:

Information classification: It is a basic process when building any system or in the environment of any information-related activity and the classifications differ according to the entity under study, for example the information may be classified into available, reliable, confidential, and highly confidential information or information may be accessible to access and others prohibited from accessing and so on.

Documentation: The information operations basically require a written documentation system to document the structure of the system and all means of processing and exchange and their components. Mainly, documentation is necessary and necessary for the identification and authorization system, information classification, and application systems. In the context of security, the documentation requires that the security strategy or policy be documented and written and that its procedures and components be fully documented, in addition to plans for dealing with risks and accidents, the responsible authorities and their responsibilities, recovery plans, crisis management and emergency plans related to the system when the danger occurs.

Administration and Personnel Responsibilities: The tasks of those connected to the information security system starts mainly from the good selection of qualified individuals and the depth of their theoretical and practical knowledge. provided that the user is aware that practical qualification requires continuous training and does not stop at the limits of the knowledge and experience.

Mainly, the administrative or organizational tasks consist of five elements Or major groups:

- Analyzing risks

- setting a policy or strategy

- developing a security plan

- setting up the security technical construction

- employing devices, equipment and means

- implementing plans and policies.

It is important to realize that the success of the administrative or collective duties of the facility depends on the awareness of all stakeholders in management with their technical, administrative and financial tasks like strategy, plan, duties of security, the organization's commitment to consider security issues as one of the issues that all are aware of. Everyone can deal with what concerns his or her duties from among the elements of security[16]. At the personal level or the level of the users, the institution must put adequate guidance to ensure public awareness. In addition, meticulous about security issues, but what is required is to build a culture of security among workers, which is divided between the necessity of observing the ethics of using technology and the required procedures. Everyone should notice any defect, and the institution must specify to the users what they must do and, most importantly, what they are forbidden to do while using the various technical means.

• **Means of identification and authentication of users and the limits of identification and authorization**:

Access to computer systems, databases, and informational sites in general can be restricted by many means of identifying the user's personality and determining the scope of use, which is known as identification and authorization systems. Identification or identity is a matter consisting of two steps; the first is the means of identifying the user[17],[15]. Second is the acceptance of the means of identification, or the so-called authentication of the validity of the presented identity. The means of identification differ according to the technology used, and are the same means of security of accessing information or services in the sectors of using the systems or networks. Alternatively, e- business sectors, and in general, these means are divided into three types: -

1 - Something that a person owns, such as a plastic card or otherwise.

2 - Something that the person knows, such as passwords, code, personal number, etc.

3- Something related to the person’s self or present in it, such as a fingerprint, eye print, voice, etc.

The means of identification and documentation are the most powerful means that combine all of these methods in a way that does not affect the ease of identification and its effectiveness at the same time.
Whatever the method of identification that will entail is documented by the authentication system, it is by itself and by means of which it will reach it is subject to a security system and security instructions that must be taken into account. Those words that can be easily guessed or investigated. [18] Along with, the use subject to the rules of non- disclosure, non-disclosure, and preservation of them. When appropriate means of identification are used to provide access to the system. When the documenting and matching process is achieved and ensuring the correctness of the definition (identity). The next stage is to determine the scope of use Authorization, which is known as authorizing or authorizing. The use of a sector of information in the system, and this issue is related to access control or access control of information or parts of the system.

Logging: Various types of computers contain some kind of records that reveal the device and its software and access to it uses, which are known as performance records or system access records. Performance records take exceptional importance in the event of multiple users. Specifically in the case of computer networks whose components are used by more than one person. in this The specific case, there is more than one type of performance records and documentation of uses, and performance records vary in terms of their type, nature and purpose, there are historical performance records, temporary records, exchange records, system records, security records, database and application records, maintenance records or what is known as records of technical and other matters. In general, the performance records are mandated to specify the person of the user, the time of use, the location, the nature of the use (its content) and any other additional information depending on the activity itself.

Back-up operations: Preservation operations relate to making an additional copy of the materials stored on one of the storage media, whether inside or outside the system, and the preservation operations are subject to rules that must be predetermined, documented and written, and they are adhered to to ensure the standardization of preservation standards and the protection of backup copies. Numbering and categorization, the mechanism of retrieval and use, the place of preservation and its security, and the encryption of copies that contain private and confidential data, are major issues that clear and specific standards must be taken regarding.

Technical security means and the intrusion prevention system: There are many technical means of security that must be used in the computer environment and the Internet, as are their purposes and scope of use. We have dealt with the above issues of identification and authentication, specifically passwords and other means of identification. Firewalls, in addition to cryptography, as well as access control systems, Intrusion Detection Systems (IDS)[21], and anti-virus systems and software are increasingly important, but they do not all represent the security methods used, but rather they are in addition to the means of advanced identification and documentation. The most important technical security means now, and we will review these methods to the extent available with an indication of their most important issues through internationally approved security guides and some prevailing standards and measures regarding them in Clause 1-5 of this chapter.

Incident Handling System: Regardless of the size of the technical security means used, the security standards and procedures followed, an integrated system must be available to deal with risks, accidents and attacks, and it is considered a major requirement for business enterprises as in the case of banks and financial institutions[19].

The first thing to be understood in this regard is that dealing with accidents is a process and not just a project or a single step, meaning that it is an integrated process related to continuous, progressive performance subject to predetermined rules that are followed with precision and discipline. Whenever incidents are dealt with as a mere case that arises when the accident we are before A deficiency that is, in itself, one of the weaknesses in the security system.

The components, stages and steps of the accident handling system differ from one institution to another depending on many factors. It is related to the nature of the risks analysis process has revealed. [20] The security strategy in the institution has revealed depending on the system under protection. Whether the system is closed or open computer systems, databases or networks or a combination of them, and whether we are talking about a specific service system or public services over the network. whether private or international, and depending on the function of the application being protected. As the steps, content and elements of accident handling plans for Internet banks, for example, differ from those of information sites, however, and in general The system for dealing with accidents usually consists of six stages (step by step), which are: - **Pre-preparation, investigation, observation, containment and eradication, recovery and return to normalcy, and follow-up**.

Risks, threats, vulnerabilities, types of attacks and attacks, and their technical methods in concepts and conventions

The purpose of this presentation is to try to provide a disciplined definition of the conventions used in the world of computer and Internet crime, in terms of distinguishing between many conventions that are confused between them, as there is a difference between electronic crime, electronic terrorism, information warfare, risks, accidents, weaknesses, errors, breaches Information war ... And others[22],[23].

Threats: It means the potential danger that the information system may be exposed to and it may be a person, such as a spy, a professional criminal or a hacker, or something that threatens devices, programs or data, or an event such as a fire, power outage and natural disasters.

Vulnerabilities: It means an element, point, or location in the system through which the aggressor is likely to implement or achieve the breach. For example, people who use the system are considered a weakness if their training is not sufficient to use and protect the system and the Internet connection may be a weakness, for example if not Not encrypted. The spatial location of the system may be a weak point, such as if it is not equipped with means of prevention and protection, and in general, weaknesses are the driving reasons for achieving threats or risks. Countermeasures related to this term: the technique used to protect the system, such as passwords, locks, and means of control, firewalls, and others.

Risks: They are used synonymously with the term threat, although it is a fact related to the impact of threats when they arise. A successful information security strategy is based on risk analysis, and risk analysis is a process and not just a restricted plan. It starts with questioning about threats and then points Vulnerability and finally the appropriate prevention methods to deal with threats and means of preventing vulnerabilities.

Incident: It is a broad term that includes risks and includes errors, and it is in the sense used in technical information security studies, it refers to intended or unintended acts, and covers technical attacks and errors. However, an accurate description of this concept in the administrative - administrative and legal framework, it is necessary to He is responsible for unintended accidents, which may be risks due to nature and without an intentional factor, or unintended technical errors.

Attacks: it is a term for describing the attacks by their results or by the location of the target. We say denial of service attacks, terrorist attacks, software attacks, malevolent employee attacks or humor attacks. The term "breaks" is used as a synonym for attacks, which is a term used to describe various types of technical attacks, and thus is synonymous with attacks.

Legal conventions: it is important in this regard to define the difference between three terms used in the field of legal studies. The first is the term cybercrime, which is indicative of various computer and Internet crimes at the present time despite Its use in the beginning was limited to cybercrime alone, which is what we will deal with in detail later in the course of explaining the legal conventions indicating computer crimes.

Cyber terrorism or cyber terrorism: attacks targeting computer and data systems for religious, political, intellectual or ethnic purposes that are part of cybercrime as crimes of destroying systems and data or crimes of disrupting websites and systems work. but they are distinguished from them by many features.

Information warfare: which is a term that appeared in the Internet environment to express attacks of disrupting websites, denying service, and seizing data. They are often attacks with a political dimension, or attacks by malevolent competitors in the business sector, which makes them synonymous here with acts of cyber terrorism.

Physical security breaches or Dumpster diving: which means that the attacker searches the corporation’s remnants of garbage and leftover materials in search of anything that helps him penetrate the system, such as papers with passwords, or computer outputs that may contain useful information, or discarded hard disks after replacing them. Alternatively, other written materials, discs, notes, or anything inferred from it on any information that contributes to the penetration.

Wiretapping: It is the physical wired connection with the network or the system connections in terms of eavesdropping or stealing and seizing data exchanged over wires, which are activities that are carried out in easy or complex ways depending on the type of network and the methods of physical connection.

Eavesdropping on Emanations: This is done by using technology to collect the waves emitted from the systems of various kinds, such as capturing the waves of optical computer screens or capturing the sound waves from communication devices.

Software piracy: It is achieved by copying it without permission or physically exploiting it without authorization for this exploitation, or its imitation, simulation and material use of it in a way that violates copyright.

Communications and Security Breaches of: it includes unauthorized copying of data, Traffic Analysis Covert Channels, Theft, and Attacks via tunneling manipulation.

Conclusion

What we are experiencing in terms of the overlapping of several generations, classifications, or strategies of current information, its multiplicity and the multiplicity of its patterns, is something we all touch, and everyone user has to have the Knowledge in the multiplicity of techniques for dealing with information. The speed of information development and its importance in conducting research from various aspects of modern life necessitated finding special methods and algorithms to encode it and preserve it from manipulation from different perspectives.

.The researcher concluded the main data protection purposes with the following:

.Confidentiality: Ensuring that the information is not disclosed or viewed by unauthorized persons

Integrity and integrity of the content: to ensure that the information content is correct and that it has not been .modified or tampered with, and in particular the content will not be destroyed or changed by illegal interference

Continuity of availability of information or service: - Ensure that the information user will not be subject to denial of .his use of it or his access to it

Information security zones

Communications security: Communications security means protecting information during the data exchange process from one system to another

Computer Security: It is intended to protect information within the system of all types and patterns, such as protection of the operating system, protection of application programs, protection of data management programs, .and protection of databases of all kinds

Information security cannot be achieved without providing integrated protection for these two sectors through security standards that guarantee the provision of this protection and through multiple levels of security that are .different in nature

Patterns and levels of information security

Physical protection: It includes all means that prevent access to information systems and their rules, such as locks, .barriers, bunker rooms, and other physical protection methods that prevent access to sensitive devices

Personal protection: It relates to the employees working on the relevant technical system in terms of providing the means of identification for each of them and achieving training and qualification for those dealing with security .means, as well as awareness of security issues and the risks of information attacks

Administrative protection: It is intended to control the management authority over the management of information systems and their rules, such as controlling external or foreign software from the facility, questions of investigation of security breaches, matters of supervision and follow-up of control activities, in addition to carrying out control .activities within higher levels, including issues of controlling external contributions

Media-cognitive protection: such as controlling the reproduction of information and the process of destroying sensitive information sources when deciding not to use them

References

1- Bidgoli, H. (2006). *Handbook of Information Security, Threats, Vulnerabilities, Prevention, Detection, and Management* (Vol. 3). John Wiley & Sons.

2- Winn, J. K. (2009). Are better security breach notification laws possible? *Berkeley Tech. LJ*, *24*, 1133.

3- Schumacher, M. (2003). *Security engineering with patterns: origins, theoretical models, and new applications* (Vol. 2754). Springer Science & Business Media.

4- Beckers, K., Heisel, M., & Hatebur, D. (2015). Pattern and Security Requirements. *Pattern Secur. Requir. Eng. Establ. Secur. Stand*, 1-474.

5- Ehrlich, M., Trsek, H., Wisniewski, L., & Jasperneite, J. (2019, October). Survey of Security Standards for an automated Industrie 4.0 compatible Manufacturing. In *IECON 2019-45th Annual Conference of the IEEE Industrial Electronics Society* (Vol. 1, pp. 2849-2854). IEEE.

6- Barreto, C., Andersson, D., & Reimers, K. (2014). Post-Secondary Education Network Security: Results of Addressing the End User Challenge. In *Proceedings INTED 2014 Conference* (p. 6018).

7- Ransome, J., & Misra, A. (2018). *Core software security: Security at the source*. CRC press.

8- Jouini, M., Rabai, L. B. A., & Aissa, A. B. (2014). Classification of security threats in information systems. *Procedia Computer Science*, *32*, 489-496.

9- Baker, W. H., & Wallace, L. (2007). Is information security under control?: Investigating quality in information security management. *IEEE Security & Privacy*, *5*(1), 36-44.

10- Samonas, S., & Coss, D. (2014). THE CIA STRIKES BACK: REDEFINING CONFIDENTIALITY, INTEGRITY AND AVAILABILITY IN SECURITY. *Journal of Information System Security*, *10*(3).

11- Aminzade, M. (2018). Confidentiality, integrity and availability–finding a balanced IT framework. *Network Security*, *2018*(5), 9-11.

12- Aminzade, M. (2018). Confidentiality, integrity and availability–finding a balanced IT framework. *Network Security*, *2018*(5), 9-11.

13- Kumar, M., Meena, J., Singh, R., & Vardhan, M. (2015, October). Data outsourcing: A threat to confidentiality, integrity, and availability. In *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)* (pp. 1496-1501). IEEE.

14- Cherdantseva, Y., & Hilton, J. Information Security and Information Assurance. The Discussion about the Meaning, Scope and Goals.(May, 2012).

15- Newsome, B. (2013). *A practical introduction to security and risk management*. SAGE Publications.

16- Fischer, R., Edward Halibozek, M. B. A., & Walters, D. (2012). *Introduction to security*. Butterworth-Heinemann.

17- Al-Dhahri, S., Al-Sarti, M., & Abdul, A. (2017). Information Security Management System. *International Journal of Computer Applications*, *158*(7), 29-33.

18- Sauerwein, C., Sillaber, C., & Breu, R. (2018). Shadow cyber threat intelligence and its use in information security and risk management processes. *Multikonferenz Wirtschaftsinformatik (MKWI 2018)*, 1333-1344.

19- Abbass, W., Baina, A., & Bellafkih, M. (2016, October). Improvement of information system security risk management. In *2016 4th IEEE International Colloquium on Information Science and Technology (CiSt)* (pp. 182-187). IEEE.

20- El-kenawy, E. S. M. T., Saber, M., & Arnous, R. (2019). An Integrated Framework to Ensure Information Security Over the Internet. *International Journal of Computer Applications*, *975*, 8887.

21- Haider, W., Creech, G., Xie, Y., & Hu, J. (2016). Windows based data sets for evaluation of robustness of host based intrusion detection systems (IDS) to zero-day and stealth attacks. *Future Internet*, *8*(3), 29.

22- Kumar, R., & Goyal, R. (2019). On cloud security requirements, threats, vulnerabilities and countermeasures: A survey. *Computer Science Review*, *33*, 1-48.

23- Rot, A., & Olszewski, B. (2017, September). Advanced Persistent Threats Attacks in Cyberspace. Threats, Vulnerabilities, Methods of Protection. In *FedCSIS (Position Papers)* (pp. 113-117).