ISSN (Print) 2794-**7629**
ISSN (Online) 2794- **4549**

Received 03/03/2023
Accepted 25/04/2023

FULL PAPER

Information Security and Network Protection Measures

Prepared by

Aouragh Karim
Cyber Security Management
Charisma University – UK
Aouragh.karim@yahoo.com

Abstract

The Internet is one of the information and communication technologies in the current era, because of its great role in disseminating information among people all over the world, and with the diversity of the use of the Internet, new criminal patterns began to appear on this network, and these criminal patterns are viruses and theft of political and commercial secrets. In this article, we study information security concepts, network protection measures, virus prevention, and overcoming vulnerabilities.

key words : Information security, network protection, vulnerabilities, viruses

1- Introduction:

Despite the benefits that have been achieved and continue to be realized every day thanks to the tremendous development of the electronic field at all levels in various areas of contemporary life, so that all different sectors have become dependent in their work primarily on the use of the computer in the first place, the world has become a small village connected by information networks.

In this era, enterprises have relied on information technology, which has proved to contribute to the work being done with great speed and precision. Data and information are stored in information stores linked to the institution's computers through the communication network and are often available online to facilitate work processes and reduce time.

Therefore, data-processing methods for compatibility with the computer environment have evolved from manual to automated electronic workflow systems to the e-government concept. Thus, information technology has facilitated medical, engineering, industrial and banking work, library systems and the work of educational institutions and has even become a weapon in military establishments for use in hostilities.

These networks need protection to ensure the integrity of their content and the continuity of their work. It has been concluded that business in enterprises is interrupted if their information networks, such as airlines and large companies around the world, are disrupted. Indeed, the short interruption of such networks has taken a heavy toll on their owners or beneficiaries. The short interruption of government and national information networks has led to the disruption of their work, which is reflected in the low level of services provided to citizens and the confusion in State institutions related to broken-down networks. The suspension of business networks causes significant financial losses that may often lead to bankruptcy and business quality and success depend on the quality and functioning of communication networks and the continuity of databases.

The issue of network security has become the cornerstone of the building of any network system of any size, owing to the increasing and diverse new threats such as infection with viruses, malware, and attempts to penetrate for the purposes of stealing information, sabotage, modification and tampering, which we always find in a state of rapid development and progress. To confront these threats, we need sophisticated security solutions that are no longer available through traditional protection methods, which has been a fundamental challenge in securing the necessary protection of any network system.

2. The problem of study:

The proliferation of electronic information networks with all the positive features has led to new risks that were not previously known, including the security of the electronic information network linked to access to networks, the theft of secrets of companies, Governments and security and defence institutions, the promotion of sabotage, espionage and piracy programmes, the theft of sites and their vulnerability to viruses and harmful programmes.

Accordingly, the problem of studying can be summarized in the lack of adequate means and procedures to counter electronic penetration and protect networks.

3. Study hypotheses:

There are no statistically significant differences between the security gaps in information networks and the preventive actions taken to prevent them from being exploited.

There are no statistically significant differences between actions to avoid threats and actions taken.

4. The objective of the study is:

1. Identification of information security
2. Identification of risks, gaps and threats
3. Identification of viruses
4. Identification of weaknesses in the networks considered and measures to redress them
5. Identification of actions needed to achieve high protection of information networks.

5. Importance of the study:

The theoretical importance of the study stems from the importance of maintaining and protecting the security of corporate computer networks from the potential for hacking, piracy or sabotage, which has an impact on their future strategy and plans and thus their growth and development in their respective sectors.

6. Information and network security concepts:

Until the late 1970s, the field of information and network security was known as communications security (COMSEC) ,defined by the Information and Communication Systems Security Recommendations of the Agency United States national security:

Standards and precautions to prevent access to information by persons not authorized through communications and to ensure The authenticity and validity of these contacts included the specific activities of communications security in four areas:

1. Security encryption
2. Dispatch Security
3. Radiation Security Emission
4. Physical Security

The definition of telecommunication security has two characteristics:

1- Confidentiality [3] : This means ensuring that the information is not revealed or accessed by anyone else.

2- Risk: A concept that refers to negative and potential impacts on assets and valuable property that may result from a current process or future event. It began in the 1980s, with the steady growth of personal computers and their use, a new era of security, namely, COMPUSEC, Computer Security, defined by the United States National Security Agency (USNSA) Information and Communication System Security Recommendations:

Standards and procedures that ensure confidentiality and completeness and provide components of information systems, including hardware and software The integrated software and information is processed, stored and transported.

Computer security has two additional features:

Integrity and content integrity: it means ensuring that the content of the messages (information)

It has not been modified or tampered with. In particular, the content has not been destroyed, altered or tampered with at any stage. from processing or exchange stages, both in the internal handling of information and through intervention

Illegal during transmission.

2- Continued availability of information or service: ensuring the continued operation of the information system Networks and their continued ability to interact with information and users, not to stop or block service. The lack of access as a result of attack, destruction and sabotage.

Later in the 1990s, the concepts of telecommunication and computer security were combined to shape what became.

It's known as Information Systems Security (INFOSEC). It includes a concept of security.

Information systems are the four aforementioned features of the concepts of communications security and computer security, namely confidentiality.

And reliability, completeness and availability, as added to it is the new characteristic of combating denial or preventing denial of conduct. The purpose here is to ensure that the person who did the non-repudiation is not denied it. By acting in connection with the information or its location, it is he who has done so in such a way that this characteristic provides the ability to prove that the conduct of a person has taken place at a given time.

6.1. Risks, gaps and threats:

Security is known as protection from danger and loss. In general, the concept of security is similar to that of safety. Variance the precision between the two concepts is the additional focus of security on protection against the external risks of individuals and activities that violate protection and are directly responsible for breach of security. The term security is generally used.

As a synonym for safety, but technically, security means not just safety, but working to provide Safety too.

Specific concepts are recurrent in different areas of security, including:

1- Risk: the risk of a particular event having an impact on the achievement of objectives. In engineering science, the risk is known quantitatively as the probability of an accident and the loss of a single incident.

Risk is seen as an indicator of threats and depends on threats, gaps, impact on operations and uncertainty. There are many ways and means of assessing and measuring risk.

In information security and networks, the risk is determined using three variables (factors):

1. There could be a threat.
2. There may be gaps.
3. Potential impact of the threat.

If any of these variables become zero, the total hazard to the system or network is close to zero Also.

2- Gaps: (or lack of immunization) and generally known as sensitivity to harm or attack Physical or psychological. It also means that property and valuable assets are not adequately protected. In computer security. Networks use the term gaps to refer to the weaknesses of these systems that allow the attacker to attack. And it could cause gaps, short software, or design malfunctions, as a result of programmer neglect or designer, or the attacker's use of malignant programs like virus programs.

Computer and network security gaps can be classified into two categories:

1. Technical gaps: As a result of poor immunization resulting from systems and network techniques, a network attack is known as a technical attack.
2. Administrative gaps: They are the result of non-technical reasons and, in this case, the attack on the network or computer is known as a social engineering attack..

Gaps in terms of difficulty and ease can also be divided into two categories:

a- **High-level Gaps**, which are easy to exploit, and an example of his book

A program code to exploit that gap.

b. **Lower-level gaps,** in vulnerability and this type of gaps that are difficult to exploit and require a lot of effort and resources by the attacker.

3- Threats: Potential intrusion into assets and property (information) without the permission of the owner and forced and through a potential loophole in the system to steal or sabotage it, and in case of its occurrence, threats pose a danger to the system.

There are three essential components of the threat:

1. **Objective:** Represents in computer security and networks information stored or sent through networks for violation Her confidentiality, her safety, her presence.
2. **Client:** The programs and objects that are formed and created for the threat require access to the computer or networks, as well as information on their operating characteristics and the security mechanisms used in them, in order to search for a gap in access to the system or network.
3. **Event:** The quality of the impact represents the state of threat and is used in many ways, most importantly, authorized abuse and unauthorized to information or system. And he put on malignant blades, Like virus blades in systems.

Figure 1 illustrates the relationship between the components of the information security system and the networks and their impact on each other.

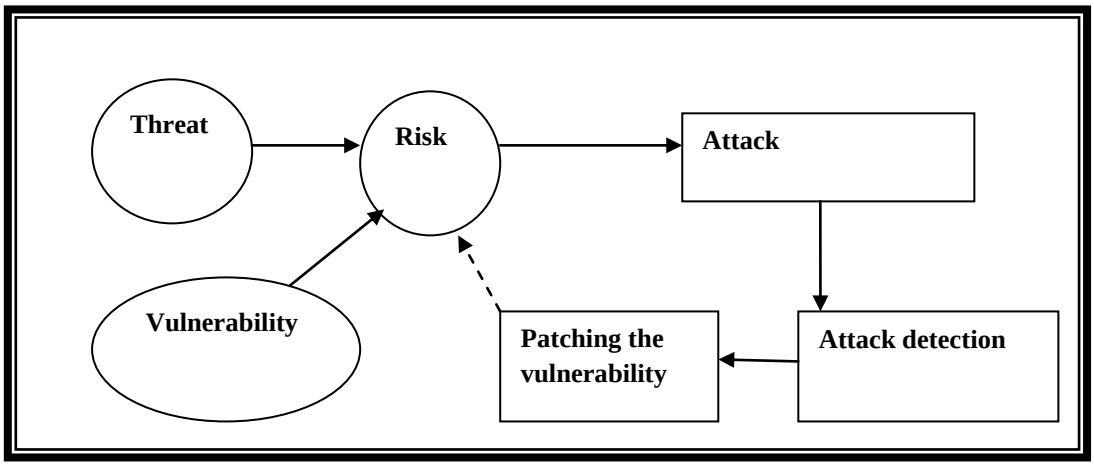

Figure 1 illustrates the relationship between the components of the information security system and the networks and their impact on each other.

6.2. Elements of information security:

The elements of information security are organized in several areas, including:

- **Security of data and information storage sites:** this area is concerned with many scientific and practical mechanisms. Related to data preservation sites and surrounding environment to ensure that information is in secure locations like data centres, which should be subject to strict control and physical security procedures. It's so high in access that it can only reach those who are authorized and through a secure gate that may be able to access the device.Sometimes it depends on advanced techniques, such as reading the fingerprint of the finger and the iris, (Printyee) or voice frequency or through serial numbers or magnetic cards,etc..
- **Security of data archiving:** this is done through the use of advanced information encryption techniques Saved (Encryption) with various types of symmetry or asymmetric encryption, whether internationally accredited Or a locally developed encryption method.
- **Data-conservation media security:** this axis is achieved through the most appropriate preservation of hard drives (HDD),memory cards (CASH), (CD) and other appropriate preservation media.
- **Information protection security:** various mechanisms are used, such as firewalls or firewalls. To protect against hacking network devices, use filters to ensure that unauthorized information is not transmitted, and use anti-Virus to protect against various viruses and copies.Backup to address the problem of missing non-written digital data that is more vulnerable than Others for damage, damage or loss are done with a number of mechanisms.
- **Information and data transfer security:** in the past, direct physical data transfer mechanisms were used and surrounded In confidence and protection of these mechanisms are relatively slow, and the current reflection is that this method has been safer than the roads. Modern e-networking. After technical advances, modern transport

mechanisms have become what they have been characterized by. The speed and accuracy of the transfer are best suited when taking the necessary security precautions in data transfers. We therefore believe that this area is concerned with the safe environments for the transmission of and access to data and information through networks.

- **Security of communications systems and transportation environments used:** when direct connection is by lines telephone or satellite on-line, and when data are relatively medium. The risk here lies in the presence of sniffing intruders on the lines of communication, highlighting the importance of robust and efficient data encryption and maintaining the integrity of the communication line from the presence of interceptors or spyers.
- **Security of applications used and protocols:** when communication is indirect and through an intermediary such as internet or data transfer to a high-security service site, such as expenses or direct purchase with electronic credit cards, spying and hacking are the most obvious security problems that can't be eliminated. It's completely on it, and it can be significantly reduced by using safe protocols on... the level of the application or network layer shows the importance of digital signatures and electronic certificates. To secure sites and other protections.
- **Searching for potential sources of danger for information to combat:** sources of danger and security threats data and networks are too many, and perhaps the most important of them is the risk of access to data by people who are not allowed to do so, and thus information is leaked, destroyed or altered.that connects them to the data or enables them to destroy it or change it in a number of ways.

7- Computer viruses:

7.1- Definition of Viruses:

Computer viruses spread widely and evolve rapidly due to the technological advancements we witness in our daily lives. Thousands of computer devices are infected daily by these viruses, causing significant financial and emotional losses to their users. Personal information is stolen, and users are often blackmailed for financial gain to regain access to their files.

A computer virus is an external program deliberately created to alter the properties of the files it infects [6], executing various commands such as deletion, modification, or sabotage. Computer viruses are programs written by skilled programmers with the intent to harm

another computer, take control of it, or steal important data. They are characterized by their ability to replicate and spread. The virus attaches itself to another program called the host; viruses cannot generate themselves. They can be transmitted from an infected computer to a healthy one.

The virus is a program designed to spread itself among files and integrate or attach itself to programs. When the infected program is executed, it may infect the other files present on the hard disk or floppy disk. Therefore, the virus requires intervention from the user to spread. Typically, this intervention involves executing it after being downloaded from email, downloaded from the internet, or through exchanging floppy disks.

7.2- Components of the virus: [6]

The virus program generally consists of four main parts:

1. **The Replication Mechanism:** This part allows the virus to copy itself.
2. **The Protection Mechanism:** This part hides the virus from detection.
3. **The Trigger Mechanism:** This part allows the virus to spread before its presence is known, such as using the computer's clock timing, as in the Michelangelo virus, which activates on March 6th of each year.
4. **The Payload Mechanism:** This part executes the virus when activated.

7.3- How Viruses Work:[6]

The creator of the virus programs it and directs its commands, determining when and how the virus becomes active. Typically, the virus is given enough time to spread freely without drawing attention to infect as many users as possible. Viruses vary in terms of when they become active; some start at a specific date or time, others activate after executing a certain command in the infected program, while some start their activity after replication and reaching a certain number of copies. After activation, the virus engages in various destructive activities depending on its purpose. Some may display messages mocking the user or issue warnings about memory overflow, while others may delete or modify files. Some viruses replicate and copy themselves to fully disable your device, while others are more devastating, wiping all data from the hard drive."

7.4- Reasons for the Spread of Computer Viruses:

The reasons for the spread of viruses on users' computers around the world vary, and among the most important are:

- Viruses spread through programs downloaded from the internet, especially when relying on sources of unknown origin. Once the user installs the program on their device, these viruses activate to damage the device.
- Some users resort to using what is called "cracks,"[6] a small tool used to activate paid software for free. However, these cracks often carry viruses that infiltrate the computer.
- Infected file exchange between users by connecting two devices, one of which is infected with viruses, naturally affects the healthy device, easily transferring the viruses to the other device.
- Clicking on links sent to the user without knowing the sender can result in downloading viruses directly to the device.
- Viruses spreading through email attachments, as today, viruses often find their way to personal computers through email attachments. Once you open the attached file, the virus infects your device and may replicate itself, spreading the infection to all email addresses in the Address Book.

7.5- The Major Damages Caused by Viruses:

With the diversity and continuous proliferation of viruses, the damages inflicted on your computer system vary. However, the damages caused by viruses can be summarized in several points:

Viruses that infiltrate your computer system work to completely destroy it by corrupting files on the hard disk, affecting random-access memory, and manipulating device settings, ultimately causing the system to slow down and eventually leading to its complete destruction. Additionally, viruses that infect installed programs on the computer cause malfunctions in the programs, preventing them from performing their essential functions.

Viruses that infect websites you browse steal your personal data and intercept what you send through various websites. These viruses target vulnerabilities in your device, preventing antivirus programs from detecting and combating them, thus making your device susceptible to viruses."

8- Results:

The research and preceding studies indicate that the following measures should be taken to protect the network from threats, risks, and vulnerabilities:

1. Installing a firewall [2].
2. Installing antivirus protection systems.
3. Installing internet usage monitoring software.
4. Using a password with a minimum length of 8 characters [5].
5. Updating operating systems.
6. Updating antivirus software.
7. Updating firewalls.
8. Conducting periodic tests to detect weaknesses within and outside the network.
9. Using a variety of techniques to assess vulnerabilities [1].
10. Implementing self-protection for programs [4].

9- Conclusion:

Some companies in practical reality have faced problems due to weaknesses in their electronic information security systems, leading to data breaches, fraud, or data destruction, resulting in significant financial losses. To compensate for this, some companies may struggle to provide the requirements for controlling the security of their information due to weaknesses in their internal control systems. Hence, this study aims to contribute to understanding this issue. It is hoped that this study will provide useful results and recommendations for companies or professionals in various security sectors, whether military or civilian, and those working in industrial, commercial, governmental, or non-governmental fields. This will help identify some weaknesses within the components of electronic information systems to preserve their information security."

10- Recommendations:

The internet has become massively utilized and relied upon, carrying millions of communications. It has become a serious threat to the safety of data flowing through networks. Knowing how to protect the privacy of your information and devices while using the internet reduces the likelihood of exposure to risks of unauthorized use, which can cause material or moral harm to you."

11- References:

1. G.Saba (2018)."**Network Security and Information Infrastructure**", published by the Syrian Virtual University in 2018.
2. Nawaf Saleh Al-Munj: "**Information Security for Small and Medium Networks**."
3. Yousef Khalil Yousef Abduljabbar:(2014) **"The Effectiveness of Internal Control Measures in Providing Electronic Information Security in Jordanian Industrial Companies."** Master's Thesis in Accounting, Accounting and Finance Department - College of Business (Middle East University, 2014).
4. Naeem, Mamoun: (2004).**Maskless Program Pirates**: "Theoretical and Practical Foundations for Breaking Program Protection and Anti-Piracy Prevention Methods" - Dar Shuaa for Publishing and Sciences, First Edition 2004 - Aleppo, Syria.
5. Thomas Toum: (2004)."**The First Step Towards Network Security**," translated by the Arab Center for Arabization and Translation, (Beirut: Dar Al-Arabiya for Science, 2004).
6. Anwar Abu Bakr Abu Madin:(2018) **."The Internet and Virus Protection",** Research, Postgraduate Studies in the Computer Department, University of Tripoli, 2018."