Journal for Research in Applied Sciences and Biotechnology

www.jrasb.com

ISSN: 2583-4053

Volume-2 Issue-1 || February 2023 || PP. 186-190

https://doi.org/10.55544/jrasb.2.1.26

Analysis of Threat Risk and Vulnerability in Network Security Along with Countermeasures to Overcome the Damages in an Enterprise Network

Maroof Khan[1] and Gulab Jan Sajjad[2]

[1]Lecturer, Department of Computer Science, Paktia University, AFGHANISTAN.

[2]Dean of Computer Science, Information System, Paktia University, AFGHANISTAN.

[1]Corresponding Author: hamdard181208@gmail.com

www.jrasb.com || Vol. 2 No. 1 (2023): February Issue

Received: 21-01-2023	**Revised:** 11-02-2023	**Accepted:** 21-02-2023

ABSTRACT

The research is conducted based on analysis of threat, risk and vulnerability in an enterprise network along with countermeasures to overcome the security incidents in an enterprise network. It is clear that most of the businesses are running using internet to store and share data between employees and customers, because data are precious and an asset for an organization. So, there is a high chance of losing data due to threat, risk and vulnerability in an enterprise network. However, there is a need of awareness and understanding between threat, risk and vulnerability including countermeasures to protect data in rest and data in motion in a network. As well as information security aim to protect organizational data from unauthorized access, manipulation and destruction.

Keywords- Threat, Risk, Vulnerability, Security, countermeasures.

I. INTRODUCTION

The network consists of a group of systems connected to one another for making a communication network through any wired or logical wireless medium, as well as a communication network include the devices like computers and printers. In an enterprise network a node is any devices used to communicate with each other's and share resources as computer, printer and server. Network protocols, a comprehensive collection of rules governing the interaction between two systems, including security, are the basis for communication between nodes.

Individuals and corporate organizations send, receive, and electronically store their secret data through an enterprise network. It is obviously common that unauthorized can access or attack these networks to intentionally or nonintentional access and destroy the business data. In this developing stage of information technology protecting our data, systems, hardware and software's from malwares or internal and external hacker are ever important for our enterprise network data. So, Threat risk and vulnerabilities are more common than our thinking in this evolving network in the world, which can cause to obtain access to our data in rest and data in motion in an enterprise network. This access to our confidential data can damage, destroy. Manipulate our business data.

Securing an enterprise network is a complex employment and need a qualified professional to develop a framework to reduce the challenges. Therefore, there is a need of individuals who understand the essentials of network security to legitimate the threats, risk and vulnerabilities in the network. All enterprise network requires various level of security countermeasure to protection their business data, resources and infrastructures, both the individual and organization must ensure the security by using the approaches of

ISSN: 2583-4053

Volume-2 Issue-1 || February 2023 || PP. 186-190

https://doi.org/10.55544/jrasb.2.1.26

analysis, assessment, planning, implementation and maintenance. As well as the countermeasure will be provided for the threats, risks and vulnerabilities to reduce the breaches of network security from inside and outside hackers.

II. METHODOLOGY

To deliver the research goals which is the analysis of security threats, risks, vulnerabilities and the countermeasures to overcome the loss in enterprise network. A library-based research methodology will be applied in this research for collecting data regarding the analysis and countermeasure related to my research a review of literature will be done for collecting relevant data. According to George 2008, stated that library research involves finding sources that offer factual data or a person's or an expert's belief on a research issue; it is an important step in conducting all other research. The resources include books, articles, journals, magazines and bibliographies.

III. PROBLEM STATEMENT

With the huge development of network in the world, security issues are increasing to manage and control the enterprise networks. There is a believe that security issues are encountered both internally and externally and are concerned about business computer systems, resources that have important and sensitive data. Therefore, there is a less awareness about network security threat, risk and vulnerabilities as well as comparison of disclosure of theses security breaches. The countermeasures will be an asset which will support and help in reducing the damages in enterprise network.

IV. LITERATURE REVIEW

Network security is one of the most important aspects for enterprise network because it is the security which overcome the damages and lose of data in network infrastructures. Security threat and their vulnerabilities are the essential aspect to be discussed while risk is critical that can breech security in an organization. As well as countermeasure for reducing the barriers in an enterprise network will be take in consideration.

Literature review is the approach of collecting previously published data in a specific arena from different books, articles, thesis and journals. Literature review ensures understanding with and comprehension of the most recent research in the topic, with the help of literature analysis we will be able to find out what research has already been done on your problem and identify what is unidentified.

A literature review is an important aspect of a research or article. Literature review is an analysis or discussion of the most recent published information on a given subject. It makes an effort to recap and assess the data and material in accordance with the research topic. A literature review investigates other people's perspectives on the topic at issue and synthesizes and delivers an argument, not only a list of research that have been summarized. This makes it possible for your readers to understand what various sources have to say about the issue at hand (Cantero, 2019).

Afghanistan is suffering from a decade of conflict which have destroyed many educations, agriculture, industry and ICT based infrastructures. After international intervention in Afghanistan many development projects are implemented for quality development and education including ICT infrastructures. We have ICT based center in many universities and education enters but less awareness about threat, risk, vulnerabilities and countermeasures to overcome the level of damages in enterprise network in Afghanistan the study will elaborate the goal of this article.

Threat

A network threat is an attempt to access someone data through network breaching. Network threat are in different forms someone using DDoS attacks to bring down your network or services while some attackers using malwares to stole your data or theft your credentials which may cause danger to your enterprise network.

According to (Yassir and Nayak, 2012) stated that, Hacker attacks for a variety of reasons, such as fraud, extortion, data theft, revenge, or simply the challenge of breaking into a system. Internal staff members who misuse their access privileges or outside attackers who remotely access or intercept network communications can both achieve this. The development and propagation of malicious computer code, also known as "viruses," is another typical method of attacking a computer system. Computer viruses are malicious software programs designed to harm other computers. A "Trojan horse" is a harmful program that can occasionally be found inside of another application and be copied by a user without their knowledge.

In order to protect against attacks and respond to breaches when they happen, it is essential to understand the biggest threats and the security mechanisms that has to take in consideration. As (Rathore et. al, 2017) indicated that, malware is the software’s designed to infect and interfere the processes of computer and enterprise network. Malware is the threat that commonly used by unauthorized users to potentially damage organizations data and infect the systems. Mostly malwares are transmitted to enterprise networks using email mechanism, during downloading attachments or using other communication sources to reach the target to destruct the system infrastructure and steal the confidential data. The most common threats in malware are the Trojan horse, phishing, spyware, viruses and worms.

ISSN: 2583-4053

Volume-2 Issue-1 || February 2023 || PP. 186-190

https://doi.org/10.55544/jrasb.2.1.26

As Yassir & Nayak, (2012) indicated that, Threats to network security are not limited to businesses; they can be seen across the world in various nations and the quantity to which each is vulnerable to risk, some of the threats are listed below.

- Malicious insiders
- Malicious code
- Web based attacks
- Denial of services
- Stolen devices
- Phishing and social engineering
- Malware
- Botnets
- Viruses, worms and Trojans

In the advanced development of internet Securing a computer network, network devices and network infrastructures from unauthorized access is complex. According to Friedberg et al. 2015 stated that, when discussing advanced persistent threats, it is common for the attack to originate inside the network. Previously, comprehensive attacks frequently took place to count and track different people. The actual harm is then secretly done when more sensitive information is extracted. Another popular tactic is to disable or tamper with logging systems in order to hide harmful behavior.

Risk

In network security risk is the likelihood that a cyber-threat will result in the loss and destruction of assets or data. It means in the presence of risk the organization lose the confidentially, integrity and availability of information and has possible adverse effect to the organization processes. As (Chen, 2009) stated that, Confidentiality, integrity, availability, and accountability are often seen as components of information security. Information is protected against theft and eavesdropping through confidentiality. Integrity is the defense of data against unwanted alteration and covering. In the context of cyberattacks like denial of service against information systems, availability refers to users' dependable access to permitted information. Whereas, accountability is the transmission of duties and the capacity to track a person's activities to all parties concerned.

According to Andersson (2010), stated that risk is a term which are more frequent in normal conversation and others of which are more formal. In common usage, risk can be seen as either the possibility that an undesirable event will occur but need not. As well as risk is an unfavorable event's likelihood and its potential effects are harmful for organization assets, sensitive information and infrastructures.

Data that are stored in an enterprise network are under risk both data at rest in servers and computer and data in motion which travel from source to destination. As Lakshmanan (2020), stated that, data is more valuable to an organization business, so hackers and other attackers are always targeting it. Data security risks exist whether it is kept on local servers, computers or on the cloud, but moving data from one place to another makes it much more vulnerable to hacker attacks between computers, servers, the cloud, etc. As there is a lot of data transit within a network. Data and applications are more vulnerable to data breaches because diverse connection technologies are used in such data flows.

Vulnerability

The development of networking in the world bring the complexity in systems whereas the number of vulnerabilities are increasing and securing the large enterprise network are more complex which bring the attention of securing the enterprise network more protected. A network vulnerability is a flaw or weakness in administrative processes, hardware, or software that, if exploited by a threat, could lead to a security break. Vulnerability in an enterprise network may be both physical or non-physical through which hacker can exploit the network system and harm the entire network. According to Lai and Hsia, (2007), indicated that the design flaws in the network, software, hardware, and firmware, as well as improper configuration or setting on these systems, are the cause of vulnerabilities. The vulnerabilities have unpredictable effects that can harm system data or lower system performance. In some situations, the "sensitive" data may be recreated or exposed by exploiting these systems weaknesses. System vulnerabilities have various properties and diverse effects on the systems.

As vulnerability is the weakness in enterprise network which can be exploited easily by hacker leads an organization to potentially harm or destroy data. The vulnerability may be in hardware or software and in most attacks, vulnerability is involved. According to (Lakshmanan, 2020) indicated that, Various attacks can be carried out against the edge devices when they are booting up. This is due to the fact that the built-in security processes are not active at that time. Attackers may try to attack the restarting node devices by getting the benefit of this vulnerability. It is necessary to protect the boot process in edge devices since they frequently run on low power and suffer sleep-wake cycles. As well as indicated that distributed denial of services, man in the middle attacks, botnet attacks, routing attacks, data transit attacks, access attacks, booting attacks, malicious attacks and phishing attacks are come into existence due to vulnerability in an enterprise network.

Countermeasures for mitigation of threats risk and vulnerability in an enterprise network

In computer network a countermeasure is a process that is used to mitigate the threat, risk and vulnerability in an enterprise network in organization.

A countermeasure is a technique taken by the organization to mitigate a threat, often by security experts. Or an action or technique used to minimize, prevent, or reduce potential threats to computers, servers, networks, operating systems (OS), or information

ISSN: 2583-4053

Volume-2 Issue-1 || February 2023 || PP. 186-190

https://doi.org/10.55544/jrasb.2.1.26

systems is known as a countermeasure (IS). Firewalls and antivirus software are examples of countermeasure tools. (Hamid, 2005).

Countermeasure in network security is an act against reducing the threat, risk and vulnerability in an enterprise network which mitigate the harm to information. Regarding this Aliero and Ibrahim (2012), indicated some common countermeasures for reducing security attacks are listed in the following statements:

Countermeasures against social engineering attacks:

- Business data classification and employees' level of access to business sensitive information.
- Never allow strange person to access confidential or sensitive business information as user name and passwords.
- Never allow using fake devices as unauthorized hardware or software on a computer network.
- Never open unsolicited emails, only open communications from reputable sources. Never react to, access, or forward such emails' attachments or links.
- Always scrap enterprise network documents as well as noticeable resources as network hardware and software holding devices as computer hardware.
- Always provide security training for enterprise network employee for internal and external threats, risk and vulnerabilities awareness to protect sensitive information and assets from unauthorized access.
- Protection against unauthorized physical access to maintain and implement policies and credentials to avoid access to sensitive area and data.

As protection and security control of information in an organization is necessary and need to be protected due to the importance of information for organization. According to Samonas & Coss (2014), indicated that the three key terms are important in understanding and shaping the information security in an organization which mainly focused on technical protection of confidentially, integrity and availability of information sensitive data. therefore, to protect information physical and nonphysical unauthorized access a countermeasure of implementing CIA is needed in an organization.

1. Confidentiality

Confidentially is the essential concept of securing information. Confidentially means to have a complete reliability in information security confidentiality implies that data and information must be protected from unauthorized access by unauthorized individuals. According to (Samonas and Coss, 2014) stated that, confidential means to have a complete faith and reliability on the data protection that there is no access to unauthorized individuals to access the system and information in an enterprise network because confidentiality is the essential concept of information security. As well as Gibson (2017) indicated that confidentiality is used to avoid unauthorized expose of information. Confidentiality means the information and system can be accessed by authorized individuals but unauthorized individuals cannot access the information and system in an enterprise network. As well as indicated that different methods are used for implementing confidentiality as encryption data to make the data unreadable in the form of ciphertext, access controls which includes identification, authentication and authorized which together provide access controls and avoid unauthorized people to access the information and systems.

2. Integrity

As integrity is the process of keeping and guaranteeing the accuracy and steadiness of data in information security. It means there should be no modification in information. As (Samonas and Coss, 2014), declared integrity is the prevention of information from alteration or destruction and guarantee the authentication and repudiation of information in an enterprise network. Actually, this non repudiation of information guarantees the authenticity and medication of data in an enterprise network. Similarly, Gibson (2017) said integrity is another factor that guarantee the accuracy and modification of data. It ensures that data is not corrupted only authorized person can modify the data in an enterprise network. However, if illegal attempt or unexpected modification take place it could be malicious or unauthorized users.

3. Availability

In information security availability means timely and accurately access to information. According to Samonas & Coss (2014) stated that an enterprise network or a system is available and useable when it is effective and efficient, and customers are satisfied when the performance of a system is available. As well as Gibson (2017) indicated availability is the process where data and services must be available to someone or organization as it is needed. In an enterprise network availability come with the implementation of redundancy and fault tolerance and using of uses of patches software which do not affect the availability of an enterprise network.

V. CONCLUSION

Analysis of threat risk and vulnerability are the key concepts in information security. Therefore, we have tried to analyze the theory of threat, risk and vulnerability which is an essential aspect to avoid an enterprise from this kind of attacks. Threat is the potential damage to information or information technology resources in an organization. Actually, threat is the likelihood to harm a system but there is no assurance to harm. Risk analysis provide the understanding to be proactive against the threats and attention for the domains for less and more security as Internet, malwares, spywares and adware are the source to create problems for an enterprise network. Vulnerability in network security is the weaknesses in an

ISSN: 2583-4053

Volume-2 Issue-1 || February 2023 || PP. 186-190

https://doi.org/10.55544/jrasb.2.1.26

enterprise network. Vulnerability gives us the opportunity to evaluate the possibility of risks and the best countermeasure is the implementation of vulnerability assessment which point out the summary of risks details for an organization. As well as in our analysis to keep the integrity of an organization information CIA concept is the best countermeasure to protect the confidentiality, integrity and availability of an enterprise network and unauthorized access to organization data both intentionally and unintentionally.

REFERENCES

[1] Cantero, C. (2009). How to Write a Literature Review. Qualitative Research Reports in Communication, 10(1), 55–60. https://doi.org/10.1080/17459430902839066.

[2] Yassir, A., & Nayak, S. (2012). Cybercrime: a threat to network security. International Journal of Computer Science and Network Security (IJCSNS), 12(2), 84.

[3] Chen, T. M. (2009). Information Security and Risk Management. Idea Group Publishing, 15.

[4] Lai, Y. P., & Hsia, P. L. (2007). Using the vulnerability information of computer systems to improve the network security. Computer Communications, 30(9), 2032–2047. https://doi.org/10.1016/j.comcom.2007.03.007.

[5] Rathore, S., Sharma, P. K., Loia, V., Jeong, Y. S., & Park, J. H. (2017). Social network security: Issues, challenges, threats, and solutions. Information Sciences, 421, 43–69. https://doi.org/10.1016/j.ins.2017.08.063.

[6] Friedberg, I., Skopik, F., Settanni, G., & Fiedler, R. (2015). Combating advanced persistent threats: From network event correlation to incident detection. Computers and Security, 48, 35–57. https://doi.org/10.1016/j.cose.2014.09.006.

[7] Andersson, O. (2010). analyses during the development of IT systems in the Swedish Armed Forces. Science.

[8] Lakshmanan, A. (2020). Literature Review on the latest security & the vulnerability of the Internet of Things (IoT) & a Proposal to Overcome. no. April.

[9] Gibson, D. (2017). CompTIA Security+ Get Certified Get Ahead: SY0-501 Study Guide (A. and C. C. Karen (ed.)). CompTIA.

[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] Aliero, H. M., & Ibrahim, S. S. (2012). Network Security Attacks, Impact and Countermeasures. International Journal of Marketing and Technology, 2(3), 1–13.