Network Security in Organizations

Narmeen Ijaz, Nadia Iftikhar & Sidra Anwar

Narmeen Ijaz, CS/IT department, Government College Women University, Sialkot, Pakistan
Narmeenijaz25@gmail.com
Nadia Iftikhar, CS/IT department, Government College Women University, Sialkot, Pakistan
Nadiaiftikhar11@gmail.com
Sidra Anwar, CS/IT department, Government College Women University, Sialkot, Pakistan
engrsid.es@gmail.com

Abstract:

Network Security is used to secure the network from unauthorized access. In 21st, Century Network Security is very important because a lot of hackers design mechanism to break the security system and misuse the sensitive information. Network Security in an organization is much important where many chances of hacking the sensitive information take place. Many organizations use different Security Techniques such as "Firewall", "Encryption Technology", "Intrusion Detection" to secure the Network. Other Techniques that are used to secure the Network are Digital Signature, Use of Finger Prints, and Face Scan as Password (Voice Prints, Retina Scan, and Iris Scan). In this Paper, Case Study will be conducted to collect the information about their security system and determine the weakness of their Security System. This research identifies the weakness of their Security System and suggests the new ideas that improve their Security Network.

Keywords

1. *Network Security, Network security in organizations.*

2. Introduction

[16] The work on network security is started before the 1930. "Enigma Machine is developed by Polish Cryptographers in 1918 which changed messages in the form of encrypted messages. After this in 1930, "Alan Turing" a great scientist he break the code for Enigma. Network security becomes very important during the World War II. During 1960 the word "Hackers" was introduced by the scholars of "Massachusetts Institute of Technology (MIT)". Department of Defense introduced the "Arpanet" which become popular to convert data and information.[3] In 1970, Telnet Protocol was introduced which provides the opportunities to people to use the network that was only limited to government and researchers. In 1980, hacking crimes according to network security was go forth. During 1990, internet become familiar among people and its used is increased day by day and the security issue also increased as the growing rate of the internet.

3. Related Work

[16] Biometric identification is used for security. Biometric provide a better method of authentication than password. Than the new technology are introduced as smart card Digital Signature, Use of Finger Prints, Face

Scan as Password (Voice Prints, Retina Scan, Iris Scan) that are used for security purpose.

Than new software technologies were introduced for security such as "firewall", "Anti viruses", "VPN", "Intrusion Detection" and "Encryption Technology".

4. Aim and Objectives

Aims and objectives are as follows:

To determine the flaws of the security system that is used in the organization.

To provide the new security those improve/enhance the security system

5. Motivation behind the Study

Motivation behind the study is to give new ideas that improve the security system in the organization. So they can protect their sensitive information.

6. Literature Review

"Von Solms" (1996) identify that network security has been developed in three stages: In 1960's, the first stage was started when network security refer to assure and check physical security of resources. In the mid of 1970's, the second stage was started, network security was used to measure the specific. Security needs of organizations instead of the fact that the scope of information security had covered quickly. In this competitive world, if organization wants to survive and to work in connected and distributed networks of machines, its third step will be to link its IT services altogether and to move its system into complex environment accordingly. Things which make information security very important in the organization depend on the environment in which people work. Organization relies on computers and computing control has been put down to the individual desktop. Employees of the organizations use these computing techniques to complete their routine task and employees found dangerous threats because they have direct approach to organization's resources. "Lampson" (2002) work on security then after thirty years indicate that organization system still remain dangerous for attacks. The reason is that security establishment is very expensive and complex to maintain. There was percept between employees of the organization and security provides in such a way that the employees have the ability to achieve their work "(Sandhu, 2003)". "Straub and Welke identify that the information security has been ignored by top manager, middle manager and employees alike". The reason of this ignorance is that the security system of the organization become less secure and the security consult become more dominant and destructive than is necessary "(Straub & Welke, 1998)".

To provide higher security on the sensitive information of the organization is to recognize the main threat that organization information desperately needed "(Whitman, 2003)". There are "circumstances that the threat have the ability to cause harm" to sensitive information/data and classified as external and internal threats. Many publications and surveys such as "(Whitman, 2003; Ernst & Young, 2004; Doherty & Fulford, 2005; and DTI, 2006) quantify the sources and consequences of threats to information faced by organizations". (Whitman, et al. 2005) criticize the statement "Information security has been considered as a technical problem with a technical solution" because he said "that is simply untrue because information security is about managing risk" (Lampson, 2002; and Garbars, 2002) said that managing risk is about discovering and measuring threats to sensitive information assets in the organization and taking actions to resolves the threats. When organization fail to manage their security system then organization have to face the problem of loss of money. "The UK's biggest building society Nationwide was given almost one million pounds fine after a lost laptop with customer details was stolen from an employee's home (BBC,2007)".

The conclusion is that the information security is managerial problem not a technical problem. There is need to highlight effective plan, software, strategies and other important security mechanism that help the organization to secure their system. (A. Garg, S. Pramanik, 2004) describe the digital document in an organization that is classified into secret, top-secret and confidential and unclassified. In this paper, they propose an automatic framework called CREDIT (Changing Relative Importance of Documents for Insider abuse Prevention) that indicates document reclassification as a way to deal circumstances misuse from unintentional access permission. This framework takes less time and effort. The employees use user name and password for authentication to access the resources of the organization. (Louis J. Bottino, IEEE 2006) This paper describes the security techniques that are “Firewall”, “Intrusion Detection Technique”. Intrusion Detection uses the digital signature for security. Virtual Private Network are also an example of security appliance. This paper also describes the Cryptography technique which uses the encryption and decryption techniques to secure the network from unauthorized access. This paper describes the attacks that penetrate our computer system and network. When we send large email and upload large files then different types of attacks occur such as Data Flooding Daniel of Services Adware Spyware. Adware is a type of attack that cause by the Advertiser who want to search about their customer buying habits. Spyware is a type of attackthat is caused when we visit any website or download any application which copy, remove or destroy our data easily. Spyware is more harmful to the network. This paper also describes that many organization use firewall for their Security System. According to one company firewall that is use for security system are not able to deal the network and “Application Layer” attack as “Daniel of Service” attack, “Worms”, ”Intrusion and “Trojan”. They will not able discover the threat/attacks and let the organization completely expose.

6.1. Internal Threat

Installation of unnecessary software, miss-use of software and hardware components, personnel errors, illegal use of resources in your activities, miss-use of authority, misplacing the software and hardware parts.

6.2. External Threat

This threat occurs because of computer viruses, natural disasters, hacking and spam emails.

7. Research Methodology

7.1. Research Process

Figure 1 elaborates the research process of the research.

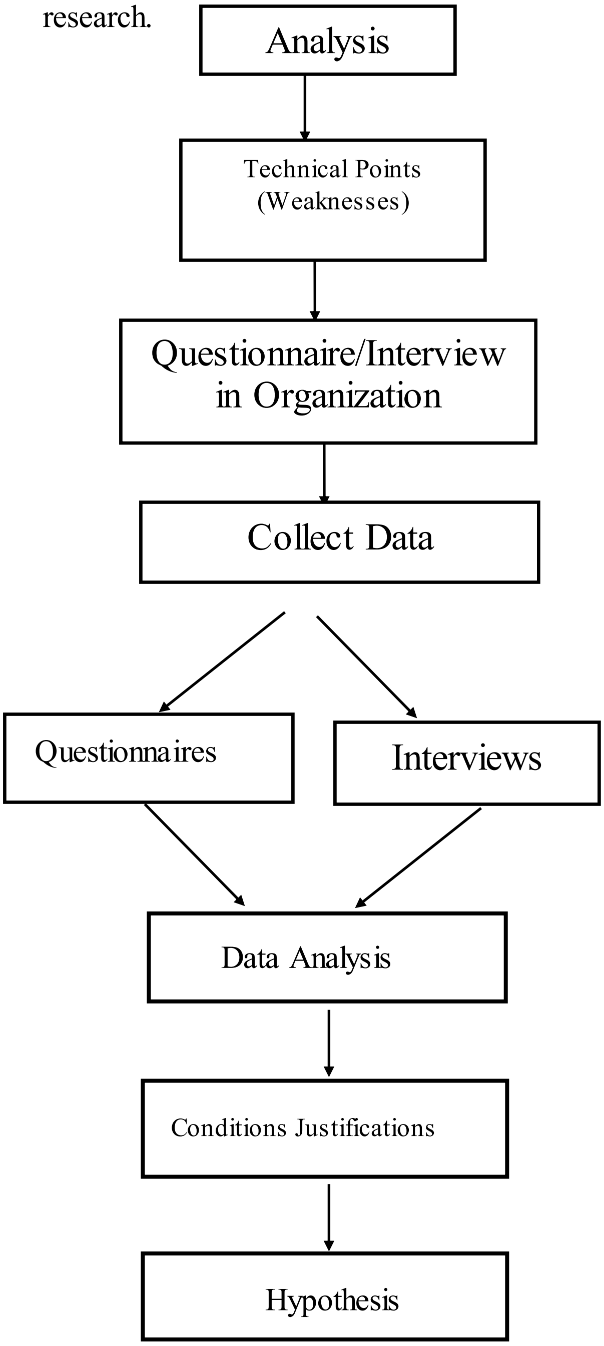
Analysis
Technical Points (Weaknesses)
Questionnaire/Interview in Organization
Collect Data
Questionnaires
Interviews
Data Analysis
Conditions Justifications
Hypothesis

Figure 2: Research

7.2. Research Process

Provide weakness of the security system in the organization through Case study. This case study will be exploratory in nature to gather data to describe conditions and to generate a hypothesis for future investigation.

7.3. Sample Design

7.3.1. Sample selection

QSA Surgical

7.3.2. Population frame

IT Industries

7.3.3. Population frame

The sample size for the proposed research shall be around 2 or more Organizations.

7.3.4. Population frame

The sampling technique will be used for organizations in which metropolitan area have applied.

7.4. Data Collection Procedure

Interviews or Self-Completion Questionnaires will be used to collect information from the organization.

7.4.1. Unit of Analysis

Unit of analysis would be IT Managers working in those organizations.

7.4.2. Time Horizon

The data for the research will be collected for one time in the year 2016; it makes the research a cross- sectional research.

7.4.3. Measurement Scale

The result of this questionnaire is measured by the scale of 5-points. Like, the scale has 1 to 5 points where we move from strongly disagree to strongly agree. Here 1= strongly disagree and 5= strongly agree.

8. Case Study

We selected QSA Surgical industry to conduct Case Study. In QSA Surgical Industry first HR manager conduct our interview to know about our knowledge. Then we go into IT department to conduct questions for our case study. We meet to the IT Department manager and asked about their security network in the organization that is which security approaches they use for their security system. Which antivirus they installed on their system to protect from viruses? Asked about their future approaches which better technology they will be used in future?

They give information about their security system. They use more than one server in their network where the main server locate/exist nobody know about the main server. They build multiple virtual machines in their network and authenticate it with user name and password. And assign different passwords and user names to different machines. If the hacker wants to hack the virtual machine they must know the user name and password. They save limited data on every virtual machine if the hacker hack the one machine they can access only that limited data on that machine and cannot access data on other machines because user name and password are different on every machine. They use live IP Address in their network. Every time they will open their system live IP Address will be same. They are confident about their network system that nobody can hack their network. They installed registered antivirus in their network. They use Systematic Norton Anti-virus in their network. If the virus enters in their system through damage or virus file then this anti-virus will be protected from all these viruses. They were fully satisfying their whole security system.

9. Recommendations

In our exploration of their security framework, we discover a few shortcomings in their framework. That if programmer hack their virtual machine than information will be lost and it can be hurtful for industry. So they will utilize computerized mark to secure their virtual machine. In the event that Digital mark/signature is use in virtual machine then touchy information/data may be perused by utilizing that particular mark. Diverse marks will be applied on various virtual machines to secure the system. Thusly, their security will be high so event of hacking will be less and no one can access to their database.

10. Conclusion

Arrange security is most imperative component to secure the delicate data from unapproved clients inside the association Programmers configuration/create component to break the security framework and abuse the touchy data of the system. Distinctive security methods, for example, "Firewall",“ Interruption Detection", “Encryption Technology" is utilized to shield data from unapproved get to. This Case Study is led to gather the security data from particular association to decide the quality and shortcoming of their security framework. They utilize virtual machines and live IP deliver to secure their framework. At that point we recommend them to pick advanced mark to secure their virtual machine. Along these lines they secure their entire framework and ensure their delicate data through programmers.

11. Acknowledgement

We would like to thanks the top management of QSA Surgical Industry for allowing us to share their data with us. Also a special thanks to our teacher who guide us at every step in this research.

12. References

[i] Louis J. Bottino, Federal Aviation Administration William J. Hughes Technical.” SECURITY MEASURES IN A SECURECOMPUTERCOMMUNICATIONS ARCHITECTURE.” *IEEE*, 2006.

[ii] Yali Liu, Cherita Corbett and Ken Chiang.” SIDD:A Framework for Detecting Sensitive Data Exfiltration by an Insider Attack.” Proceedings of the 42nd Hawaii International Conference on System Sciences – 2009.

[iii] Yudistira Asnar, Tong Li, FabioMassacci. “Computer Aided Threat Identification”, Conference on Commerce and Enterprise Computing 1EEE 2011.

[iv] Vijender Kumar Solanki, IEEE Student Member, Kumar Pal Singh, Faculty, Dr. M Venkatesan.” Firewalls Policies Enhancement Strategies towards Securing Network” IEEE Conference on Information and Communication Technologies (ICT 2013).

[v] A. Garg, S. Pramanik, V. Sankaranarayanan, and S. Upadhyaya. ”Dynamic Document Reclassification for Preventing Insider Abuse” Proceedings of the 2004 IEEE Workshop on Infonnation Assurance United States Military Academy, West Point, NY 10-11 June.

[vi] Ankit Dhamija.” A Novel Cryptographic and Steganography Approach for Secure Cloud Data Migration” International Conference on Green Computing and Internet of Things (ICGCIoT) 2015.

[vii] Zulaiha Ali Othman, Entisar E. Eljadi.” Network Anomaly Detection Tools Based on Association Rules” International Conference on Electrical Engineering and Informatics, Bandung, Indonesia 17-19 July 2011.

[viii] Greg Miiller.” Issues in inter-organisational encryption systems” International Conference for Internet Technology and Secured Transactions (ICITST-2012).

[ix] Florian Skopik, Markus Wurzenberger, Giuseppe Settanni, Roman Fiedler.” Establishing National Cyber Situational Awareness through Incident Information Clustering” 2015.

[x] Abdelmajid Lakbabi, Ghizlane Orhanou, Said EI Hajji. “VPN IPSEC & SSL Technology” 2-4 December 2012 Portugal.

[xi] Jie Shan “Analysis and research of computer network security”. Journal of Chemical and Pharmaceutical Research, 2014, 6(7):874-877

[xii] Anass RGHIOUI, Mohammed BOUHORMA, Abderrahim BENSLIMANE "Analytical study of security aspects in 6LoWPAN networks". International Conference on Information and Communication Technology for the Muslim World. 2013 IEEE.

[xiii] Candace Suh-Lee, Juyeon Jo "Quantifying Security Risk by Measuring Network Risk Conditions". IEEE 2015.

[xiv] Aniwat Hemanidhi, Sanon Chimmanee, Parinya Sanguansat "Network Risk Evaluation from Security Metric of Vulnerability Detection Tools". 2014 IEEE

[xv] Udaya Tupakula, Vijay Varadharajan "Trust Enhanced Security Architecture for Detecting Insider Threats." IEEE International Conference on Trust, Security and Privacy in Computing and Communications. 2013.

[xvi] Bhavya Daya. "Network Security: History, Importance, and Future"

[xvii] University of Florida Department of Electric al and Computer Engineering.