Network security challenges and solutions

Ebrahimi Omid, Ebrahimi Hava
Department Of computer Islamic Azad University, Ayatollah Amoli branch Amol, Iran

***Abstract*- Today, social networking aspects of community life had been affected. Enabling communication between people in cyberspace, share information, familiarity with each other, rapid notification, the benefits of social networks. In addition to these features, security and privacy of social networking comes in either case. Especially, when a social network, in order to conduct research, to be published in full or made accessible to researchers. In this paper, we investigate the attacks and the published data privacy that social networks have studied the presents. Finally, there are different models for preserving the privacy of individuals, as well as new attacks are raised that require study and research in this area reveals.**

key words: Social networking, dissemination of data, privacy, neighboring attacks, unnamed model k-

I. Introduction

Network dysfunction, use of unauthorized software, software failures, hardware failures, natural disasters, terrorist attacks, and employee mistakes can prevent proper operating information systems. Computers Systems play critical role in business, government and daily life so that organizations need to secure and control their top priority. Security refers to policy, methods that prevents the unauthorized access, alteration, theft or physical damage to information systems.

II. Abuse and vulnerabilities of the system

Before computerized automation, data about the odds or organizations are retained on paper. Information systems of data are centralized in a computer files that potentially are achieved by a large number of people and by groups outside the organization. When large amounts of data have been stored in electronic form, they are more vulnerable when in manual form.

Architecture is included a web-based request, usually a web client, and a servant, and also the company's information systems were connected to the database. Floods, power outages, fire and other electrical problem can be caused disturbances at the point in the network. If a system crash or hardware break, errors in programming, installation, misplaced, or cause unauthorized modification of computer software fails. Without strong safeguards, valuable data was lost, destroyed or would be wrong hands, revealing a trade secret or important personal information be broken.[1]

III. Challenges of the internet network

Public networks such as the Internet-based networks are more vulnerable because they are open to everyone. Computers are constantly connected to the Internet by intermediary's cable or DSL (Digital Subscriber Line) (Azter to penetration by foreigners). URLs because of they are proven to work where (where) they are easily identified. [5]

(With dial - up service for anyone who is allocated a temporary IP address and a fixed target to hackers create. Internet technology-based telephone service (see chapter 8) has been switched voice networks could be vulnerable if it is a private network to make voice is not high on most over IP) VoIP (not encrypted traffic over the public Internet) therefore everyone will be connected to a network (on) the talks listen. Pointers can exert influence credit card and personal information confidential dialogue with the other businesses are still using VoIP voice service transitions floods came up with the pseudo close. Vulnerability widespread use of e-mail and instant messaging (IM) has increased. Employees may use e-mail messages that play valuable trade secrets and confidential financial data or customer information to unauthorized recipients.[2]

https://sites.google.com/site/IJCSWN/

ISSN 2519-0814

Technologies and tools for security and control

1. Achieving to control
2. Firewall
3. Intrusion Detection Systems
4. Software ANTIVIRUS
5. Coding

IV. Network Vulnerability Assessment

New exploits are released daily, and the task of mitigating risk to the devices on your network can be daunting and resource-intensive for IT. We can help. We combine traditional scanning with expert analysis and recommended remediation to identify and eliminate problematic entry points to give you peace of mind. Our experts can perform internal or external vulnerability assessments, epending on your specific needs. Our Vulnerability Assessments help satisfy compliance and audit requirements while opening your eyes to existing security weaknesses. Our analysts organize your vulnerabilities by class and assign a prioritized risk rating so that after the assessment is complete, you have a clear direction which security vulnerabilities should be addressed first to achieve an optimal security posture.[3]

V. Network Vulnerability Scanning

Being proactive with network security is always the best approach. We help you take precautionary security measures to identify and address your security weaknesses. Our Network Vulnerability Scanning Services can reduce the burden on IT, evaluate risk, and satisfy recurring scanning requirements for audit and security testing needs. It can be done as often as you'd like. Just tell us when and we'll take care of the rest. We will routinely scan the active IPs on your network to identify vulnerabilities such as unpatched systems and vulnerable configurations and web applications. Our experts take the time to clearly interpret and explain your results and advise you to take the necessary steps for constant protection, getting you on track to managing security risk and meeting security program objectives.[4]

VI. Security threats

Theoretically, NFV is an ideal solution for deploying new network equipment and services because network functions can be dynamically updated via software downloads and updates instead of replacing physical hardware. However, some security and robustness issues still need to be addressed to fully attain the benefits of using NFV. We will particularly face two significant security challenges: (1) Network function-specific security issues and (2) Generic virtualization-related security issues [6], as shown in Since NFV is working on a network infrastructure, it is important to achieve the desired performance levels for enabling NFV.

Unfortunately, most existing IP based networks are vulnerable to network traffic attacks such as distributed denial of service (DDoS). In theory, NFV controllers are otentially seen as a risk of single point of failure. The chance of such attacks is heavily dependent on the network topology and selection of NFV controllers [6].

VII. Conclusion

Security and control should be one of the first areas to be addressed in the design of an information system. Security and control should be the responsibility of every person in the organization. Management is responsible for developing the structure and quality standards for the organization.

https://sites.google.com/site/IJCSWN/

ISSN 2519-0814

References

[١]Sweeney L., Achieving k-anonymity privacy protection using generalization and suppression. International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, 10 (5), 2002.

[2]Machanavajjhala, A. and Kifer, D. and Gehrke, J. and Venkitasubramaniam, M., l-diversity: Privacy beyond k- anonymity, ACM Transactions on Knowledge Discovery from Data (TKDD), vol. 1, no. 1, p. 3-es, ACM, 2007.

[3]Zhou, B. and Pei, J., The k-anonymity and l-diversity approaches for privacy preservation in social networks against neighborhood attacks, Knowledge and Information Systems, p. 1-31, Springer, 2010.

[4]https://truedigitalsecurity.com/services/network-security

[5]Andrej Gisbrecht, Barbara Hammer: Data visualization by nonlinear dimensionality reduction. Wiley Interdisc. Rew.: Data Mining and Knowledge Discovery 5(2):51–73 (2015).

[6] Alcatel-Lucent, Providing Security n NFV- Challenges and Opportunities, Alcatel-Lucent White Paper. Technical Report, Alcatel-Lucent, 2014.

ISSN 2519-0814