A Brief Study on Measures to Improve Cyber Network Security

J.Durga Prasad Rao
Additional Director & HOD
Computer Science
Shri Shankaracharya
Mahavidayalaya, Junwani,
Bhilai

Satyendra Kurariya
HOD Computer Science
Mata Gujari College
Jabalpur

Ram Krishna Akuli
Research Scholar
Computer Science
Dr. C.V. Raman University,
Bilaspur

ABSTRACT
Security measures are of prime concern to guarantee wellbeing and unwavering quality of associations. Hacking of data and information should be seriously addressed provided they can hamper any major loss to society, nation or at the expense of universe. The researchers feel to encompass limits to have adeep understanding of probable security measures. For example – network integration, cyber issues, firewall, information filtering, error detection and preventionsystem, and security updates.

Keywords
System, Security, Cyber-attacks, cyber network

1. INTRODUCTION
In today's information age, an association's reliance on cyberspace is turning into an inexorably vital part of hierarchical security. As diverse associations framework are interconnected in cyberspace, the level of danger to national security has expanded significantly. The danger to digital security is developing. Computer frameworks at universities and colleges have ended up favored focuses as they store same record as bank. In scholastic establishment, malicious programming (malware), phishing, framework assaults, informal community focusing on, and peer-to-peer (P2P) data spillage are every day issues. Most college's money related, managerial, work related records, library records, certain examination and other protected innovation related records are open through a grounds system and consequently they are vulnerable to security ruptures that may open the establishment to misfortunes and different dangers.

Cyber-attack alludes to the utilization of planned activities maybe over an amplified time of time—to adjust, disturb, deceive, degrade, or annihilate foe computer frameworks or cyber networks or the data and/or programs occupant in or traveling these frameworks or cyber networks. Such consequences for foe frameworks might likewise have circuitous impacts on entities coupled to or dependent on them. A cyber-attack looks to cause foe computer frameworks and cyber networks to be inaccessible or conniving and subsequently less helpful to the foe.Chart below shows daily trends of Attack in month of January 2015.

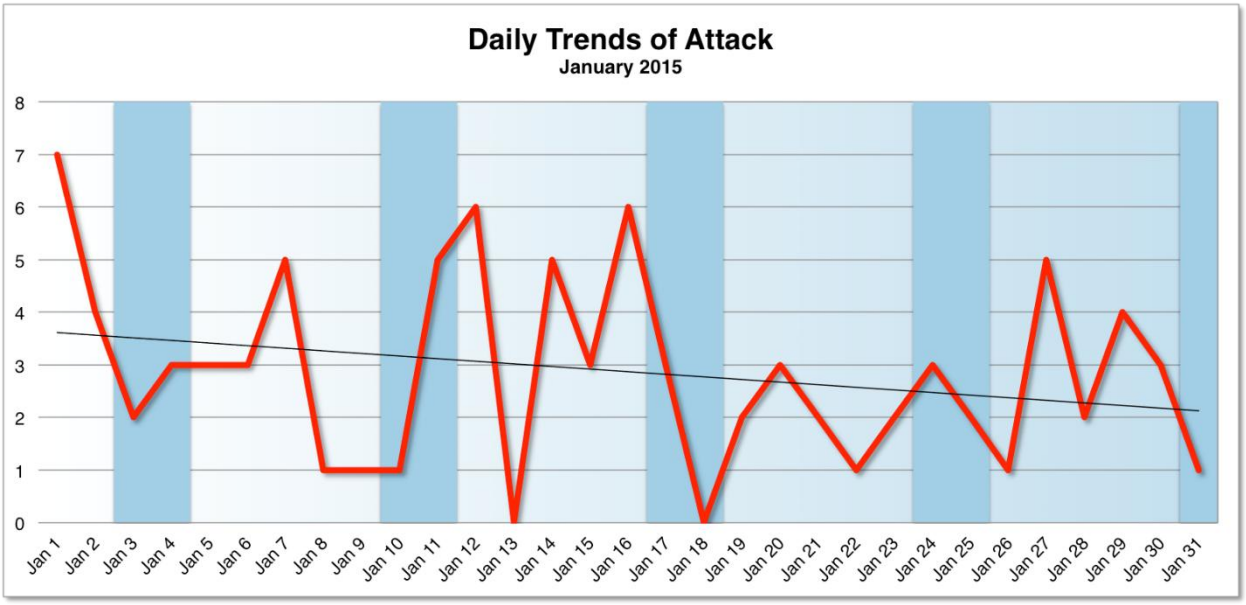
In his study Chichao Lu finds increase in number of cybercrimes cases also he highlights psychological aspects of criminals. Activity Information Management in United Kingdom found Cyber-attack is on frequent rise. It is also revealed that government sectors are more vulnerable to cyber-attack as compared to MNCs. According to NASSCOM 2014 report only 56% of Indian corporate sectors have deployed firewalls, antivirus and prevention systems.

Jeffrey R DiBiasi views that there should be proper updates of advance security features. Dr. Rose Shumba lays more stress on evaluation of security practices and training of staff. Akaninyene Walter Udoeyop proposes a model to detect abnormal behavior of reporting users. Prime need of the hour is to regularupdationof security measures to detect, prevent and counter attack cybercrime.

2. MEASURES TO IMPROVE CYBER NETWORK SECURITY.

2.1. Implementing auditing and mapping
Cyber network's infrastructure should be well defined. This includes clear model specification, location, firewall configuration, routers, switches, Ethernet cabling, ports, and wireless access points. Also connectivity path should be precisely specified. Focus on peripherals such as servers, computer, printers or any other device should be properly addressed.

Vulnerabilities and weakness found during mapping and auditing should be alleviated. Wrongly configured firewall or physical security threats can also encountered during auditing. This will increase performance, security and reliability.



Source (www.http://hackmageddon.com/category/security/cyber-attacks-statistics/)

Auditing and mapping can be manually performed for small cyber network. However for larger cyber network auditing and mapping programs are more beneficial.

2.2. Cyber network Updating

Firmware and software updates should be checked regularly. Default password should be replaced with strong passwords. It should be reviewed by entering into different login sessions, including unused functionality. Basics including OS and driver updates, personal firewall activation, and active updated antivirus should be addressed.

2.3. Physically securing the cyber network

Hackers can take advantage of open Ethernet port receiving wireless access to cyber network. Hence it is better to disconnect unused Ethernet port or make it invisible.

Secure use of door and cabinet locks should be realized. Prevention of outsiders from entering into cyber network should be blocked by ensuring good building security plan.

2.4. Preferring MAC address filtering

Both wired cyber network and wireless cyber network suffer from security issues. Former provides quick and easy authentication and/or encryption method, while the latter provides easy to deploy mechanism.

MAC address filtering provides first layer of security though it can be surpassed by focused hacker. However it can prevent a guest to plug into the cyber network. With regular updates it gives more control over devices on the cyber network.

2.5. Implementing VLANs to separate traffic

VLANs find there use in configuring with dynamic assignment. Ethernet ports, wireless access points, and dynamic users in multiple virtual cyber networks can be grouped by utilizing VLANs.

For example tablet in cyber network (wired or Wi-Fi) can be configured in assigned VLAN. In this case 802.1X authentication will be preferred option.

To utilize VLAN, router and switches must be properly addressed.

2.6. Encrypt, Encrypt and Encrypt

Encryption always makes sense to stop or minimize eavesdrop on the cyber network. Encryption in different phases can be also be better choice. However, decryption process should also be equally reciprocal way.

It must be very much ensured that effective throughput rates drops during improper encryption process placing overhead burden on the cyber network. IPsec can be option with regular updates.

3. CONCLUSION

Cyber security has turned out to be essential topic of concern because of globalization of interconnection of networks. The existence of atmosphere of machines is ever changing because of security demands. Cyber security triggers from the moment system is connected to pool of networks. The basic cause of security flaws, fall prey to vulnerable data and networks. Best cyber security network helps to bring in safety and reliable environment for service providers and users. Cyber security systems should regularly update and check its limitations and flaws. They should also have measure to quarantine unwanted data.

In this study it is found that many organizations are vulnerable to cyber-attacks as they fall below cyber security standards. On adopting above mentioned measures cyber-attacks can be minimized and information can be better utilized for target domain.

4. REFERENCES

[1] Akaninyene Walter Udoeyop, ―Cyber Profiling for Insider Threat Detection‖, 8-2010

[2] ChiChao et al., ―Cybercrime & Cybercriminals: An Overview of the Taiwan Experience‖, Journal of computers, Vol. 1, No. 6, September 2006.

[3] Deng, J., R. Han and S. Mishra, 2013. Smart environments: technologies, protocols and Defending against path-based DoS attacks in applications, pp: 11-46.

[4] Haboub, R. and M. Ouzzif, 2014. Secure Routing IN ACM workshop on Security of ad hoc and sensor WSN. International Journal, pp: 2. networks. ACM.

[5] Huang, Yan and Yang (2009).Research of Security Metric Architecture for Next Generation Network. Proceedings of IC-NIDC2009.

[6] Implementing a Network Security Metrics Program By Paul W LowansGIAC available on 23 Sep 13

[7] Jain, M.K., 2013. Wireless sensor networks:

[8] Jeffrey R. DiBiasi, ―Cyberterrorism: Cyber Prevention Vs Cyber Recovery‖, 12-2007.

[9] Kalita, H.K. and A. Kar, 2014. Wireless sensor networks. Wireless communications and mobile network security analysis. International Journal of computing, 8(1): 1-24. Next-Generation Networks (IJNGN), 1(1): 1-10

[10] Ning, P., A. Liu and W. Du, 2014. Mitigating DoS Security issues and challenges. International Journal attacks against broadcast authentication in wireless of Computer and Information Technology, sensor networks. ACM Transactions on Sensor 2(1): 62-67. Networks (TOSN), 4(1): 1.

[11] Seddigh, N., Pieda, P., Matrawy, A., Nandy, B., Lambadaris, I., & Hatfield, A. (2004). Current trends and advances in information assurance metrics. Proceedings of PST2004: The Second Annual Conference on Privacy, Security, and Trust. Fredericton, NB

[12] Shumba Rose, ―Home Computer Security Awareness‖, Computer Science Department, Indiana University of Pennsylvania.

[13] (www. http://hackmageddon.com/category/security/cyber-attacks-statistics/)

[14] www.nasscom.com

[15] www.cyberlaws.com