Computer and Network Security

Cha Zhi Ye
Universiti Teknologi Malaysia (UTM), 81310 Skudai, Johor Bahru, Johor, Malaysia.
Lim Zeng Kai
Universiti Teknologi Malaysia (UTM), 81310 Skudai, Johor Bahru, Johor, Malaysia.
Mohamad Hadif Nazhan
Universiti Teknologi Malaysia (UTM), 81310 Skudai, Johor Bahru, Johor, Malaysia.
Shafira Ika Maharani
Universiti Teknologi Malaysia (UTM), 81310 Skudai, Johor Bahru, Johor, Malaysia.

Jonathan Ting Moi Yao
Universiti Teknologi Malaysia (UTM), 81310 Skudai, Johor Bahru, Johor, Malaysia.
Wong Pei San
Universiti Teknologi Malaysia (UTM), 81310 Skudai, Johor Bahru, Johor, Malaysia.
Lee Wan Fu
Universiti Teknologi Malaysia (UTM), 81310 Skudai, Johor Bahru, Johor, Malaysia.
MUHAMMAD ANGWIN SAYRESTIAN
Universiti Teknologi Malaysia (UTM), 81310 Skudai, Johor Bahru, Johor, Malaysia.

Abstract⸻ **This paper is about computer security threats, ways to overcome them, and current issues that occur. In the era of globalization, the advancement of internet technologies has led to user safety and privacy issues increase. There are lots of threats we faced such as malware programs, DoS, and phishing. The ways to overcome these problems are improving our computer. We can do it usually by using a VPN, enable the firewall, and clear our browser history weekly. For important files and documents, data encryption is essential to improve security. However, contrary to the hackers, the cybersecurity talent is not enough to overcome the attacks that come every day. The attack methods are now improving with various vulnerabilities until causing cybersecurity workers to need spending more time and suffer a lot. For small companies and enterprises without technical talents, they unable to resist cyber-attacks and only can be alert to the tricks of cybercriminals.**

Keywords — Threats, ways, current issues, technology

I. INTRODUCTION

Rules and configurations are designed for computer and network security to monitor any unauthorized access, misuse, and modification of a network and its resources. Only assigned network administrators are allowed to gain access to the database. Just like a guard that keeps our housing estates safe, computer security is needed to monitor and prevent unauthorized access from outside attackers. Their job is to protect our privacy and message integrity. So, we can save and transfer the data on the network without worries. Every organization regardless of size requires a degree of network security solutions to protect it from the cyber threats in the wild now.

II. COMPUTER SECURITY THREATS

A. Malware programs

Viruses, worms, trojan horses, ransomware, spyware, adware, rogue, wiper, phishing, and scareware are an example of malware software. The computer virus is the most common malware which is designed to spread from computer to computer using some tricks. Usually, they are sent by email or downloaded from websites. They will disable, destroy, or steal private personal information. Eventually, causing the user to lose their computer data. Worms are programs that replicate quickly and affect our computers' processing speed. Adware and spyware are designed to track the data of the computer. Adware is to track the browsing habits to show the related advertisement, while spyware is to steal personal information like passwords, addresses, and even credit card numbers.

B. DoS and DDoS

DoS, or denial-of-service, is an attack carried out by one computer and its internet connection by pouring packets through the website so that other users can ultimately not access the website. An attack by DDos, or distributed denial-of-service, is more serious. It is launched from many machines and, as it can have thousands of IP addresses, it is difficult to counter. Besides, not all of those machines belong to the attacker. Other computers are usually affected by Trojan horses which are one of the aforementioned malware that attacks the host computer without being aware of its owner.

C.Phishing

Phishing is a strategy designed to access personal data such as user identity, location, password, credit card number, and CVV number. It is usually carried out by instant messaging and email spoofing by directing the users to a fake website that looks legitimate. The website contains messages that try to trick the user to reveal their private information and data, usually with a cover of a banking website.

III. WAYS TO IMPROVE COMPUTER SECURITY

A. VPN

Virtual private network (VPN) is a new way to solve the problem of information security, one of the most successful technology subjects, a VPN technology is to establish a dedicated network, generate the info through the safety of encryption "pipe" within the public network. There are two sorts of the mainstream mechanism of VPN, these two mechanisms are the routing filtration technology and tunnel technology to build the general public communication network.

B. Firewall

Firewalls are obligated to ensure network security, network management applications through technology, packet filtering technology, and agent technology, effectively control network access permissions, comprehensive data to external restrictions and discrimination. Meanwhile, the firewall can conceal the internal network structure and restrict the access of the external network to the internal network to ensure the security of the internal network.

C. Data Encryption

Information technology is a key encryption technology to achieve information security and help strengthen security. It translates important plaintext ciphertexts through specific encryption algorithms. Therefore, even if data files are lost or stolen, unauthorized users cannot directly read them as long as the key is difficult to crack. So, it will not cause the leakage of confidential information, thereby greatly ensuring information security.

IV. CURRENT ISSUES

A. Talent Shortage

The shortage of computer security talents is a serious problem that is occurring in the world. Companies are looking for cybersecurity talents, because no matter how large or small, all companies need at least one cybersecurity talent as an IT backbone to support their systems.

B. New and Intensive Attacks

Cybercriminals are improving from time to time to find better idea to commit crimes. It is almost impossible to keep up with the attacks in many countries. For instance, PowerShell is a technique that uses malicious scripts to evade antivirus software are majorly used in Saudi Arabian cyberattack.

C. New Vulnerabilities

More and more technologies are being developed without having seconds of rest. On the contrary, this has brought it with the potential of vulnerabilities that hackers and cybercriminals are finding. Keeping up with the vulnerabilities of new technologies is too much difficult for cybersecurity workers.

D. Small Business Limitation

Most of the larger companies are the target of cybercriminals. However, big corporations usually have powerful backups of cybersecurity workers and measures to overcome the attacks. But for a small business are lacking financial resources to manage the cybersecurity problem, which leaves them vulnerable to attack.

V. CONCLUSION

Computer network security is becoming a crucial problem with network development at this stage. We ought to comprehensively a variety of safety authentication, always beware of cybercriminals, and learn cybersecurity knowledge to ensure company sensitive information security. Not just employing a certain protective measure as it's no guarantee that the network information security. The key to building a secure network is to determine what safety means to you and what security you need. Once it is carefully defined, it usually refers to the defined strategy to evaluate everything related to the network. With the increase in the use of the Internet, there are various attacks on security strategies. Therefore, we must depart from security threats through the utilization of advanced security technology and software technology to effectively monitor potential threats and timely warning to stop malicious behavior. To secure the conventional use of the network, network security staff remain needed in everyday work to largely minimize the unknown danger of network security.

REFERENCES

[1] A beginner's guide to network security, CISCO Systems [Online] available: http://www.cisco.com/warp/public/cc/so/neso/sqso/beggu_pl.pdf

[2] Importance of Network Security [Online] available: http://www.content4reprint.com/computers/security/importance-of-network-security-system.html

[3] Predictions and Trends for Information, Computer and Network Security [Online] available: http://www.sans.edu/research/security-laboratory/article/2140

[4] Network Security Types of attacks [Online] available: http://computernetworkingnotes.com/network-security-access-lists-standards-and-extended/types-of-attack.html

[5] Securing the Intelligent Network [Online] available: http://www.trendmicro.co.in/cloud-content/us/pdfs/security-intelligence/white-papers/wp_idc_network-overwatch-layer_threat-mngmt.pdf

[6] Network security needs big data [Online] available: http://www.computerworld.com/article/2851517/network-security-needs-big-data.html

[7] Most Common Network Security Risks (and What They Do) [Online] available: https://www.theamegroup.com/5-common-network-security-risks/

[8] University Science What is Network Security? [Online] available: https://www.forcepoint.com/cyber-edu/network-secu