The Computer Network Security and Preventive Measures in the Background of Big Data Era

Jing Wang, Xing Wang, Yi Xiao
School of Intelligence Science and Information Engineering
Xi'an Peihua University, Xi'an, China
369607673@qq.com, 514591150@qq.com, 237342838@qq.com

Keywords: Big data era; Computer network security; Preventive measures

Abstract. With the progress of the times, the continuous development of science and technology, and the widespread application of computer networks, the Internet, the Internet of Things, big data, cloud computing, and artificial intelligence have gradually entered people's field of vision. In the era of big data era, computer network security has become the focus of attention. Computer network security measures have become key issues in the computer network in the big data era.

1 Analysis of Computer Network Security in the Big Data Era

1.1 Computer Network Security Overview

In the big data era, all aspects of people's lives cannot be separated from computers, and the prevention of computer network security becomes more important. Broadly speaking, all relevant technologies and theories related to the confidentiality, integrity, availability, authenticity, and non-repudiation of information on computer networks are the research areas of computer network security. Computer network security includes physical security and logical security. Physical security means that system equipment and related facilities are physically protected from damage and loss. Logical security includes the integrity, confidentiality, and availability of information.

1.2 Computer Network Security Status

In the big data era, with the continuous development and upgrading of technologies such as the Internet, the Internet of Things, and cloud computing, people's lives, work, and studies are inseparable from computers. The capacity of computer data and information storage is increasing, but it is given to people. Convenience is also obvious. The security problems of various massive data and information generated by computer network applications are also gradually on the rise. For example, computer network problems such as property loss caused by leakage of personal information, computer network defects, and personal password accounts are stolen. Therefore, it is particularly important to strengthen computer network security. It not only threatens personal privacy and security, but also threatens social economic development and social harmony.

2 Factors Affecting Computer Network Security in the Big Data Era

With the popularity of computer network technology, computer networks have become an indispensable part of daily life work. However, while computers bring convenience to people, they also face various threats. The factors affecting computer network security mainly include the following aspects:

(1) System Vulnerabilities

There are certain bugs in the current system of the computer itself. During the process of using or downloading the program for the hardware and software of the computer, due to some negligence, the user creates a loophole in the computer network system. If the system vulnerabilities or software vulnerabilities are not repaired in time, the security and confidentiality of computer data information will be greatly threatened, and the security problems of user information disclosure may be caused.

(2) Human Error

In the process of computer operations, there are also people who operate to cause computer network security problems, which can be divided into two aspects: man-intentional operation and man-made malicious operation. Although computer networks have been popularized and applied, there has been a great deal of confusion in the level of proficiency in computer operations. Some people have accidentally deleted important files of computer systems because they are unfamiliar with computers. This makes computers vulnerable to security risks and leads to leakage of user data information. This leaves a stumbling block for lawless elements (or hackers). Once important information is stolen or used by lawless elements, it will cause irreparable damage.

(3) Computer Virus

Computer viruses are the most common factor affecting computer network security. With the continuous development of computer network technology, various types of computer viruses are also increasing and changing, and they also affect the security of computer networks at any time. Once the computer is infected with the virus, then every step of the system operation will be damaged by the computer virus, not only the system will be affected, the application program may also be affected, steal important data information of the user, if serious, cause the computer to crash.

(4) Hacker Attacks

In the big data era, cyber hackers are subtle, and they are very destructive to computers. In the era of huge data, the overall value density of computer information has decreased, and we use the basic analysis tools of computer network security. It is impossible to identify the covert attacks of hackers. Once the computer becomes the object of hacking, the network security damage caused by us is incalculable.

(5) Weak Security Awareness

With the popularization of computer networks nowadays, users are pursuing the Internet speed of computer networks and leaving them in a bare state. In addition to the system and general application software, no antivirus tools have been installed. The security of user data faces severe challenges. The user's own weak security awareness is another factor that affects the security of computer networks.

(6) Insufficient Computer Network Security Management

The effective security management of computer network is the key link of computer network against external damage and computer maintenance. In the big data era, users have caused various damages to computer systems due to lack of management and daily maintenance during the process of using computers. Furthermore, computer administrators are not strict about computer network management and lack of network security awareness, causing computer information to appear. Leaks, even more serious series of security risks; especially in government, enterprises, schools and other units, if a computer network system with a large amount of important personal information is not strengthened, it will cause incalculable serious losses to the above units.

3 Computer Network Security Measures in the Big Data Era

The huge amount of data, diverse data types, and low processing speed and value density are the basic characteristics of the big data era. Based on these characteristics, we will discuss computer network security precautions from the following aspects:

(1) Establish a Complete Computer Network Security System

According to the current situation of computer network security, a complete network security system should be established to prevent all aspects of networks, systems, applications, and data. Network security should be viewed as a dynamic process, as shown in Fig.1.

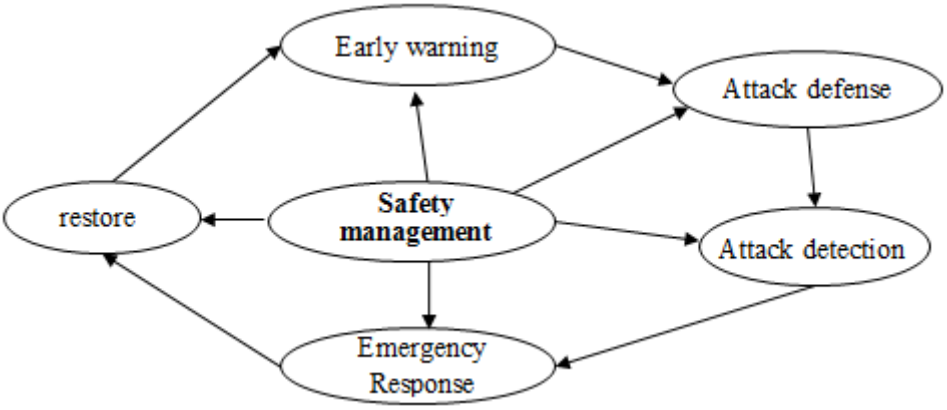

Figure 1. Computer Network Security System

As shown in Fig.1, the computer network security protection system consists of six parts: early warning, attack defense, attack detection, emergency response, recovery and security management. Security management is carried through the entire prevention system. It is the most important part of the whole system of prevention.

(2) Formulate a Complete Computer Network Management System and Strengthen the Management of Network Security

Formulate a computer network security management system, strengthen the management of network software, improve the professional quality of network management personnel, and enhance managers' responsibility to protect user information. Prevent all unrelated personnel from accessing computers and management platforms related to computer network security, reduce the risk of leaking user information, and severely crack down on intentional disclosure and sale of user information, and formulate relevant regulations to regulate computer network management behavior. To strengthen the construction of network security infrastructure and increase the importance of network security can ensure the smooth development of all aspects of network security.

(3) Remind Users to Improve Computer Network Security Awareness

Always remind users to improve the awareness of computer network security prevention. When setting user names, especially user passwords, use long and complex mixed passwords as much as possible to increase the complexity of passwords, and set them by combinations of characters, numbers, and punctuation marks. To improve the difficulty of password cracking, different websites must use different passwords, do not use the same password, and change passwords from time to time to improve the security of computer networks. At the same time, set your own wireless router access permissions, you can set the IP and MAC address binding. Try not to use public WIFI to log in and open some websites and software related to personal privacy in public places.

(4) Using Virus Anti-virus Technology to Update System Patches

Computer viruses have the characteristics of reproductive, infectious, latent, concealed, destructive, and triggerable, as shown in Fig.2. In the context of today's big data era, due to these characteristics of computers, the difficulty in preventing computer viruses has increased, but it is also the most important.

When anti-virus software is installed and used in a computer system, the system security can be monitored in real-time. At the same time, the virus is frequently checked, anti-virus software and virus database are updated, and system vulnerabilities are promptly repaired to ensure the security of the computer network system.

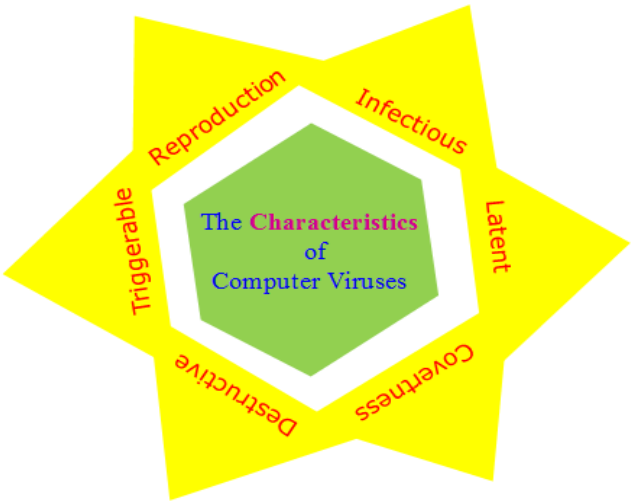

Figure 2. Characteristics of Computer Viruses

(5) Strengthen Cyber Hacking Prevention and Rational Use of Firewall Technology

Another major threat to computer network security is hacking. Combining the characteristics of the era of big data, integrating big data resources, building a defense against attack model, and registering and recording hacked attack objects as a powerful data reference for preventing attacks can effectively prevent Harm caused by hacking. In addition to using effective anti-hacking tools, it is also necessary to strengthen the isolation between the computer's internal network and external network, make rational use of firewalls and other technologies, accurately identify network attacks, effectively protect network systems, and reduce the possibility of hacking.

Firewall system implementation diagram, as shown in Fig.3.

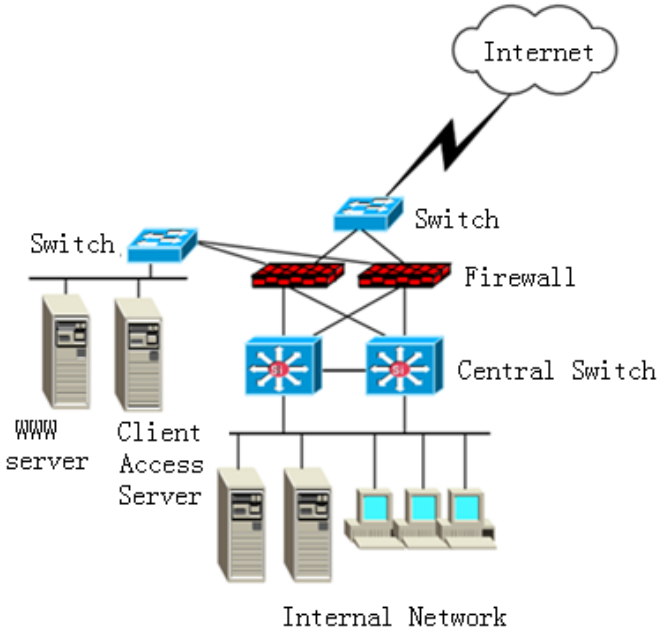

Figure 3. Firewall System Implementation Diagram

(6) Improve the Technical Level of Network Security Managers

Computer network security managers must not only strictly manage computer networks and deal with problems encountered in computer networks in a timely manner, but also take appropriate measures to prevent computer viruses and network hackers from intruding, so that the entire computer network can operate normally and the network needs to be improved. The level of security management personnel technology.

(7) Make a Backup of Data

A complete computer network security system, in addition to the above preventive measures, also needs to strengthen data backup and data recovery capabilities. Data backup looks simple and boring,

but it is very necessary. We only need to restore the data backups that we have made before, and we can avoid the serious consequences of the data being hacked by a network hacker or a virus.

4 Conclusion

In the big data era, the application scale of computer network security is becoming wider and wider. It is necessary to strengthen the protection of computer network environment security in order to ensure the normal operation of computer networks. By establishing a complete set of computer network security precautions; formulating a comprehensive computer network management system to strengthen network security management; reminding users to improve computer network security awareness; using virus anti-virus technology to update system vulnerability patches; Intrusion prevention, the rational use of firewall technology; improve the technical level of network security management personnel; do a good job of data backup and other measures can effectively prevent the computer network security is destroyed to ensure network security.

References

[1] Wei Zhang, Ming Tang, Huayong Yang. 2017.Computer Network Technology [M]. Beijing: Tsinghua University Press:171.

[2] Xizhong Wang, Tie Guo, Junqiang Huang, Chaochen Song. 2014. Analysis of Computer Network Security Vulnerabilities and Preventive Measures [J]. Computer Security: 48-50.

[3] Rui Han. 2014. Analysis of main hidden dangers and management measures of computer network security [J]. Information and Communications:152-153.

[4] Houcai Kang. 2016. Computer Network Security Prevention in the Big Data Era[J].China Computer and Communication:24-25,34.