Research on Computer Information Technology and Network Security Application

Chen Meng

Shandong Medical College, Linyi, Shandong, China

Keywords: Computer, Information technology, Network security, Applied research.

Abstract: With the development of the Internet, information technology is gradually connected with the daily life of society. In this context, the importance of cybersecurity has become more apparent. Computer information technology involves multi-directional technologies such as computer technology, network communication technology, network cryptography and network security technology. The essence of network security is that information is not forcibly accessed by unauthorized users without permission when it is transmitted and stored on the network. This paper analyzes the different nature of computer information technology and analyzes the different preventive measures in the case of rapid development of network technology.

1. Research background

1.1 Literature review

With the popularity of computers, computer information technology has also been widely used in social life. Information technology has gradually become the core of promoting social progress, and it is the main technology for the advancement of human society. Information technology has now covered people's lives and work, and it is widely used in transportation, business, statistics, teaching, etc. (Wang, 2017).People have become accustomed to relying on the Internet, so focusing on the development of information technology and cybersecurity is of great significance to the progress of human society. Under the mainstream trend of the Internet, many network security issues have also become prominent, and network security has received more and more attention. Nowadays, computer viruses and hacker technologies cross intrusion, and the scope of proliferation on the network is getting larger and larger. The protection of large-scale infected machines and cracked files has become a serious threat to information security (Xu, 2012). Because people pay more attention to network security, the current information management technology needs to be strengthened. The hidden dangers of the network not only threaten the entire network system, but also cause unnecessary losses to users (Yang, 2017).

1.2 Research purpose

A computer is an intelligent electronic device that can automatically run according to a program and automatically process massive resources. Since its invention in the twentieth century, it has had a great impact on human production technology and social activities, and has grown rapidly with vigorous vitality. Especially the emergence of the Internet, its application field has expanded from the initial simple calculation to the current military, scientific research and all aspects of life (Li et al, 2015). How to protect the network security of users is the main direction of this paper when how to ensure the convenience of computer information technology. When computer information technology promotes the development and progress of related fields, how can we ensure that the legitimate rights and interests of users are not infringed. It is necessary to understand the nature of the Internet and know how the Internet works. Therefore, it is clear what methods the criminals use to infringe on the interests of users, and what effective methods are in place to prevent these violations.

  DOI: 10.25236/aisct.2019.017

2. Characteristics of computer information technology

Information technology refers to the general term for methods and equipment for acquiring, processing, storing, transforming, displaying and transmitting text, numerical, image and audio information, including providing equipment and providing information services, with the support of computers and communication technologies. It contains the following features.

2.1 Transitive

Because information activities are essentially for the production, delivery and use of resources. Information technology has changed the way information is transmitted in the past, transforming the linear transmission of information into a non-linear transmission method (Li and Zeng, 2016). The use of information dissemination in a variety of media formats has made resource transmission faster and more comprehensive, and thus has greatly improved the communication with the past.

2.2 Share

Sharing is the ability of multiple users to obtain data resources contained in a database through a computer network. Users are not limited by the channel and can integrate the resources in the database. The biggest benefit of sharing is that multiple users can get the same information at the same time, so as to achieve efficient use of resources and improve people's work efficiency.

2.3 Dependency

Information is not a substance, it is an Abstract existence, it needs to be attached to a carrier to be passed or stored. The same information can be attached to different carriers, which means that this information can be obtained in different ways. Therefore, the dependence of information technology also makes the information have the advantages of being able to store, spread and convert. Moreover, information technology should be attached to “people”, talents are the terminals that control computers, and all information technology can be displayed through human operations.

2.4 Processing

The reception of information includes resource awareness, resource identification, resource acquisition, and information input. Storage means that the received information is converted, transferred, and buffered, saved, backed up, etc. by the storage device. The information conversion, transmission, and release prove that the computer information technology has processability.

2.5 Timeliness

In people's daily life, timeliness refers to the difference in the nature of the same thing at different times. The same is true for information technology. The existence of computer information technology shortens the time of collecting, transmitting and using information, making the information immediacy, thus increasing the value of information.

2.6 Authenticity

Computer information technology covers a wide range of areas, such as e-commerce, resource information, and scientific research. A lot of information is published by authoritative publishers and is highly credible. But sometimes there are false information, so that the user's interests are damaged. Therefore, when obtaining resources, it is necessary to distinguish the authenticity and avoid unnecessary losses.

3. The main types of network security risks

3.1 Computer virus intrusion

A computer virus intrusion is a set of computer instructions or program code that a compiler inserts into a computer program, causing various performance degradations or operational impediments to the computer. It is very powerful, destructive, reproducible and contagious.

Viruses are generally transmitted in the following four ways. The first is to spread by using an externally infected floppy disk or a hard disk carrying a virus to move to another place. The second way is the spread of large-capacity read-only pirated discs. The third is the Internet's file download and e-mail dissemination. The last is to spread through point-to-point communication systems and wireless channels.

3.2 Hacking

The so-called hacking refers to a person who is proficient in computer technology illegally trying to crack or destroy a program, system and network security, which is a relatively common cyber security threat. Hackers illegally invade users' computers, steal user-stored resources, delete user data, steal user accounts, passwords, and even property. The general means of hacking is also the implantation of a Trojan virus. When a virus is implanted into a computer, it can cause the computer to crash, slow down, automatically download, and smash, causing network paralysis.

Hackers generally invade in the following four ways. The first is to easily capture many valuable things by recording the activity of the keyboard to record the user's password and conversation content. The second is the browser vulnerability, mainly IE cache and cookie issues, the user login site and its account and even password. The third type is web browsing, which is easy to record the user name and password when logging in to the personal web page. The last one is to steal your hard drive data through the LAN.

3.3 Internet fraud

The interoperability, virtuality and openness of computer network technology give many lawless elements a chance. The lawless elements use fictional facts or methods of concealing the truth to make the awareness of prevention low through shopping platforms, chat tools, download links, etc. Users are deceived and cause property damage.

Criminals generally deceive users by the following three means. One is online shopping fraud, which sells goods far below the market price, and users often have both goods and goods. The second is virtual game equipment fraud, peddling game equipment, playing the game's lies to deceive users. The third is phishing. Criminals use the “hacking Trojan”, “network monitoring” and fake websites or web pages to steal the user's bank account number, securities account number, password information and other personal information, and then steal the user's money or Online Shopping.

3.4 Network vulnerability

Some scholars believe that when the various operations of the system conflict with the security policy of the system, a security hole is created. Vulnerabilities are mainly caused by errors in design and implementation, resulting in damage to information integrity, availability and confidentiality. Once a network vulnerability is discovered by a hacker, it will be attacked quickly, causing irreparable damage. However, vulnerabilities generally exist in individual users, campus users, and enterprise computer users who lack protection systems, mainly because managers' awareness of network prevention is weak, lack of regular inspections and system repairs, resulting in information leakage or economic losses. The scope of the vulnerability is relatively broad, mainly including the following five. First, there are bugs in software writing, second, system configuration errors, third, plaintext communication information is being monitored, fourth, secret information disclosure, and fifth, internal and external attacks.

4. Application path of network security in computer information technology

4.1 Establish a firewall security system

Users can establish firewalls to block the entry of external insecure factors to prevent unauthorized access by unauthorized external users. Let the combination of hardware and software form a firewall inspection system to monitor and check all incoming and outgoing information. More importantly, users can use a firewall to separate one network segment from another network

segment to prevent the impact on the entire network due to problems with one network segment. As the only point of access, the firewall can record between the protected network and the external network, and information that is not allowed to enter will be intercepted by the firewall as dangerous information. As the main measure of computer network security technology, firewall can protect users' network security to a large extent.

4.2 Regularly upgrade anti-virus and anti-virus software

Regularly upgrading anti-virus and anti-virus software is a very effective preventive measure. On the one hand, anti-virus software can monitor and disk data in real time, while performing memory scanning to ensure the security of the operating system. Individual anti-virus software also has a firewall function for double protection. Moreover, the anti-virus software can use the anti-virus engine to judge whether the program is a virus program, and the detection and killing process will be automatically performed after the identification is completed. On the other hand, you can use anti-virus software to check and eliminate the virus. Anti-virus software scans and checks the internal resources of the system, automatically analyzes the logical relationship between program actions, and comprehensively applies the knowledge of virus identification rules to automatically determine new viruses to achieve active defense. Because the virus is constantly updated, it is necessary to upgrade the two software regularly to ensure the immediacy of the virus database. Anti-virus and anti-virus software can effectively clean up viruses that already exist on your computer.

4.3 Introducing new network monitoring technology

The rapid development of the Internet has made traditional maintenance and protection technologies unable to meet user requirements, and technological innovation must be introduced to introduce new types of network monitoring technologies. For example, encryption technology can be used to encrypt important data. Key management techniques can also be used to ensure that the Internet delivers public data securely. Finally, identity authentication technology can be used to allow users to ensure the security of computer information through identity information and passwords.

4.4 New IDS and IPS dual system protection

On the one hand, IDS new network intrusion detection system after the firewall can be used to identify common attack types such as system scanning, denial of service and system penetration. The advantage of the IDS new network intrusion detection system is to monitor network traffic without affecting network performance and improve the basic integrity of information security. On the other hand, you can use the IPS Intrusion Prevention System, which not only detects intrusions, but also terminates intrusions through intelligent response, providing deeper protection than IDS. Dual system protection is more suiTable for a wide range of attacks that are not very targeted, and the ability to respond to professional hackers is slightly insufficient.

5. Conclusion

The current level and characteristics of computer information technology bring many conveniences to people's lives and cause many problems. Network information technology is the development and management of information, and the use of this information to promote development. However, network information technology itself has some defects. For example, the management of massive resource processing is not used in conjunction with information management, and there is a lack of information security processing in application. The relevant managers have low professional standards, lack of strong supervision and so on. In addition, criminals outside the computer invade the network through various means, infringing on the legitimate rights and interests of users. This paper summarizes the relevant aspects of computer information technology, and hopes that users can use the computer information technology to bring convenience, while security can be strongly protected and no longer suffer losses.

References

[1] Wang Z.P.,(2017) The Development Direction of Computer Information Technology and its Application Research. Information and Computers, 22(20):41-42+46.

[2] Li H.S., Zhan X.Y., Wu. Z., et al,(2015) Research on the Trend of Computer Technology Development. Wireless Connected Technology,12(1):71-72.

[3] Xu R.S.,(2012) The Development and Research Status of Network Security. Information Security and Communication Confidentiality,34(11):25-25.

[4] Yang H.,(2017) Computer Information Technology Application and Network Security Strategy. Section Teaching Journal - Electronic Edition(Late),9(1):261-261.

[5] Li Q., Zeng W.,(2016),International Collaboration in Cyber Security Governance. China Science and Technology Forum,32(11):26-31.