Main Problems and Countermeasures of Enterprise Computer Network Security

Yi Liu

School of Accounting, Harbin University of Commerce, Harbin, China

jyn7777@sina.com

Keywords: Computer; Network Information Security; Problems; Measures

Abstract: In the context of the information age, computer networks have changed various fields of social production and life. Due to the vulnerability of the computer network and the various network attacks it has suffered, events that have damaged individuals and public interests have emerged in an endless stream. The methods of preventing information security problems have also aroused widespread concern. This article analyzes the common problems of computer network information security on the basis of elaborating the connotation of computer network information security, and further proposes scientific and effective preventive measures.

Computer network security

The computer's network security means that the computer is in a relatively safe network environment. Without permission, user data has not been changed, web pages can be opened and browsed in normal mode, and related information is in a safe state. In recent years, many personal information has been leaked, and because the banking system was maliciously attacked, personal information was leaked, and people were subject to various harassment. Therefore, it is necessary to strengthen network security work and strengthen network technology protection. Maintain information data in a relatively safe environment to reduce the possibility of leakage When the computer is attacked or damaged, it will cause data leakage and seriously hinder the normal operation of the network.

The continuous development of computer technology and network technology has had a profound impact on various fields of society. In the office field, network technology can achieve network office information system office, effectively improving the efficiency of enterprises in enterprises. Although the development of office information systems It brings convenience to users, but there are also many security threats. Criminals will use computer technology to attack the existing office information system, causing the office information system to paralyze or steal user information, causing losses to the enterprise. Therefore, in the development and construction at the same time as the office information system, in order to ensure the security of the computer network, it is of great theoretical and practical significance to implement an effective security strategy.

Problem analysis of computer network information security

In the second quarter of 2019, Cross-SiteScripting (Cross-SiteScripting) is the most common type of attack, accounting for nearly 40% of the total threat. SQL Injection (SQLInjection), used to access sensitive information or run operating system commands to further Penetrating the system, accounting for about a quarter of the total number of attacks, the same as the first quarter. Relevant experts expect cross-site scripting attacks and SQL injection will continue to account for more than half of the total web application attacks. In addition, frequent attacks in the second quarter the list also includes Information Leak and XML Injection, both of which require disclosure.

In this era, people are on the Internet almost at all times, and many important communication activities are carried out through the computer network. The user's demand for computer functions and the frequency of use make them put forward higher requirements for the information security of

the computer network. In fact, When the data on the computer is destroyed, this will not only cause property damage, but also seriously endanger the safety of life. Therefore, maintaining the information security of the computer network is very important. In order to better protect the information security of the computer network, we must determine What are the factors that may cause the insecurity of computer network information, so that we can take preventive measures against these factors.

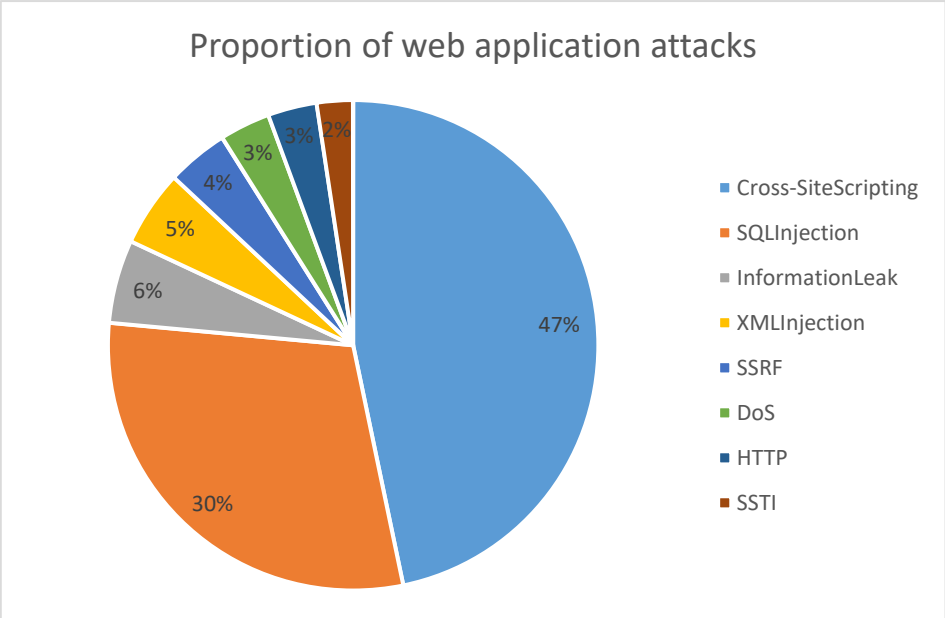

Figure 1. The proportion of virus attacks

The attacks on manufacturing company websites are relatively targeted, and are basically carried out by experienced hackers, so although the number of attacks in this field is very small, these attacks are actually the most dangerous.

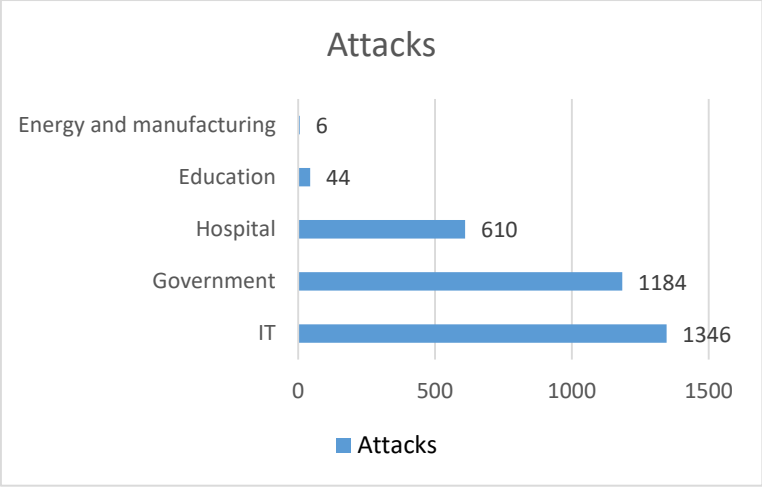

Figure 2. Average number of attacks per day in different industries

Virus threat

Viruses have a huge impact on the security of computer networks. In computers that are off-network, they are generally not affected by viruses, but the speed of viruses spreading in the network environment will be very high, and there are many types of viruses. It is difficult to detect and process viruses in a timely manner. Not only that, viruses also have a lot of threats to the computer, for example, they may have an impact on the working speed of the computer, make the computer run slower, and also cause damage to the computer files and damage the computer. Software and hardware. Generally speaking, computer viruses spread from the network to the

computer, or through mobile hardware such as U disk, some viruses can also pass through the computer's security defense system, making the computer infected with viruses. When working with information systems, viruses can easily enter the computer system, thereby destroying the hardware and software in the system, and causing the entire information system to crash and fail to operate normally, which is very detrimental to the company's daily office transaction processing, even facing corporate information. The risk of theft. Under the threat of viruses, a lot of information about the enterprise or unit can beStolen criminals, the leaked trade secrets or confidential units, enterprises or units would cause huge losses. Therefore, to ensure network security, strengthening computer virus prevention is very important.

Hacking

The behavior of hackers attacking the computer network seriously threatens the security of the computer network. With the continuous popularization and improvement of the level of computers in our country, various kinds of hacker attacks on the computer network have emerged to achieve illegal gains and invade companies or government networks. The purpose of stealing confidential documents, causing adverse social effects, and even stealing other people's bank passwords through hacking to steal. Hackers may use various means to invade other people's computers and engage in illegal criminal activities. These hackers use some loopholes in the computer network to exploit them Edited programs or software to invade other people's networks, making the society in the threat of being hacked. The information system is based on Ethernet technology and uses broadcast communication methods. Information transmission between two nodes may also be affected by other data. Node interception. If a hacker hacks into the internal network node of the enterprise, it will also cause the enterprise's information to be completely monitored by the hacker, which poses a huge threat to the enterprise's work. For example, in August 2019, an Australian hacker teenager hacked into the Apple server. Access to a large number of user account lettersMany users worry about leakage of personal information on the Apple server. The incident has been reported to Apple, it caused a serious negative impact.

System vulnerabilities in the computer network itself

In the history of the development of computer networks, every operating system has a variety of vulnerabilities and problems, which cannot be avoided. Commonly used windows systems and Apple systems, no matter which version will exist or more There are fewer vulnerabilities, and when a new operating system is launched in the market, once the new system comes online, the manufacturer will continue to update and replace it to eliminate the defects of these systems and continuously eliminate the vulnerabilities in the system. Computer systems are vulnerable, Mainly manifested in the vulnerability of hardware equipment, the vulnerability of software, and the agreement between producers and users. The vulnerabilities of the system need to be continuously retrieved, searched and repaired by the system operation and maintenance personnel, otherwise the system will appear very A large security risk may be attacked by others by illegal means at any time, causing losses and threatening the network security of the computer. Therefore, the system vulnerabilities of the computer network itself are also a hidden danger affecting the security of the computer network, and need to be further strengthened and perfect.

Preventive measures for computer network information security problems

Strengthen computer network virus processing

The harm of computer viruses is huge. Viruses may cause computers in the network area to lose their normal working capacity and destroy all data. The needs of enterprise information systems to prevent and control viruses are obviously different from the virus prevention on traditional computers, and network viruses need to be prevented. And control. Only by combining the prevention of network viruses and network control systems can the goal of preventing and controlling network viruses be achieved. Network management is the basis for preventing network

viruses. Most enterprise information systems are likely to be infected with viruses, mainly because of network management Vulnerabilities, and lack of effective methods to prevent and control network viruses. Therefore, it is necessary to improve the traditional office system management methods, improve the pertinence of network security management, and comprehensively use the following technologies to prevent and control network viruses.

Therefore, in the process of managing computer network security, we must concentrate on strengthening the detection and resolution of network viruses. In order to prevent computer network viruses, the most important thing is to install computer virus protection programs for computer systems. (1) Use antivirus software correctly Products, install network anti-virus software products, and pay attention to software updates and replacements. Currently widely used anti-virus software such as Kingsoft Internet Security, Kaspersky, Little Red Umbrella and 360 anti-virus software can effectively detect and destroy network viruses. Anti-virus software supply The vendor will update the software and release the latest version from time to time. The office information system administrator must download the antivirus software upgrade package through a secure channel and install it in time so that the antivirus software can kill the latest network viruses and improve the response of the computer network system to virus attacks. Ability. Among the viruses that may exist in the computer network system, network administrators and security users can also use computer anti-virus software for comprehensive detection to ensure the relative security of the computer network. Finally, for computer viruses and hackers, network security experts You can also add fire protection to the network systemWall to prevent hackers in the external network from attacking the network in the area to prevent information theft and leakage. (2) Strengthen network management and security management in office areas, increase capital investment, and ensure that hardware technology meets the needs and protection requirements of the office, and Ensure that the enterprise information system conforms to and the virus server configuration can be matched with each other to avoid that some virus prevention functions cannot be achieved. Through comprehensive prevention and control of viruses and management on LANs and WANs, the security of the system is improved.

Set up a network firewall

When a corporate network is maliciously attacked, it poses a serious threat to the security of the company's website. This is a very common situation. Network security issues have a major impact on the overall development of the company and are directly related to the company's information security. Therefore, network viruses must be prevented to eliminate security vulnerabilities In addition, we must pay full attention to the prevention of hackers, you can use the network firewall to avoid malicious intrusion into the external network. Setting up security software in the firewall can be used to monitor the activity of the computer network in real time. Once the request for illegal access or misconduct is found These requests are processed immediately to facilitate people surfing the Internet. In recent years, people's awareness of network security has increased day by day. In order to improve the security of the company's internal network, the possibility of network security accidents is decreasing through the setting of firewalls. In addition, it needs to be established The firewall monitors the network to ensure the rationality of reading and transmission. Through the audit of the network, the detailed record of the access record is realized, and the network access log is automatically created to ensure the security of the network. When there is a problem with the network security, the firewall will automatically Issue alerts to help improve network security effectiveness.

Reasonable use of data encryption technology

When using computer network technology to transmit information, it is easy to have security problems, such as loss and leakage of information. The use of effective data encryption technology can effectively reduce the security risk of information transmission and provide users with good information transmission in their daily work and life Environment. After encrypting important personal information and confidential information with data encryption technology, even if the data file is obtained by other people, you must enter the decryption key before viewing the information.

At the same time, when using data encryption technology for encryption, you can also Combined with some passive protection mechanisms to ensure information protection. For example, when entering the information key, if the input error is repeated multiple times, the passive mechanism will start and execute the automatic destruction of the information in the data file, which largely solves the information Leaked security issues.

Conclusion

Therefore, under the guidance of computer networks, the development of enterprise information systems has gained more ways and methods, which in turn provides more technical support for the economic development of enterprises. In general, enterprise information systems rely on the Internet and are easy Affected by network security issues. In order to make computer office information systems play a greater value, people need to strengthen the application of network security technology, thereby improving the efficiency of enterprise operations. Computer network security issues must be regarded as an important task of computer security management Content, understand the root cause of computer security problems, develop reasonable network security measures, and provide users with a safe network environment.

References

[1]. Feng Mengyao. Computer network security issues and preventive measures [j]. Digital Communication World, 2019 (2): 82-83.

[2]. Sun Yangli. Discussion on the Existing Problems and Preventive Measures of Computer Network Security [j]. Computer Products and Circulation, 2018 (12): 19.

[3]. Yang Jianwei. Problems in computer network security and prevention measures [j]. Information and Computer (Theoretical Edition), 2018 (18): 203-204.

[4]. Lei Ming. The current situation and countermeasures of computer network security [j]. Science Times, 2013 (23).

[5]. Wang Zhiqiang. Research on Hidden Troubles and Countermeasures of Computer Network Security Based on the Internet Economic Era [j]. Information System Engineering, 2018 (06): 72.

[6]. Wang Xiaonan. Research on the countermeasures against computer network security vulnerabilities [j]. Network Security Technology and Application, 2014 (03): 125-126.

[7]. Li Shaobiao. Main characteristics of network viruses and countermeasures of hidden dangers of computer network security [j]. Silicon Valley, 2014 (09): 153-153,147.

[8]. Liu Zhijie. On the status and countermeasures of computer network information security in the era of big data [J]. Computer Knowledge and Technology, 2017.21 (17).

[9]. Huang Jian. Discussion on computer network security problems and countermeasures in the era of big data [j]. Talent, 2018: 233

[10]. Si Lijuan. Main hidden dangers and management methods of computer network security [j]. Automation and Instrumentation, 2017.