2018 International Conference on Computer Science and Biomedical Engineering (CSBIOE 2018)

Discussion on computer network security risks and emergency response technology

Zhang Jing, Du Zhibo, Gao Chaoying

Zaozhuang Vocational College of Science&Technology，Tengzhou，Shandong，277500，China

Keywords: Computer; Network security risks; Emergency response

Abstract. In the ever-changing process of modern information technology, the use of computer network has been effectively developed and popularized, and the computer network security has also received much attention. Computer network security is not a technical security issue, but a security management issue. From the category analysis, computer network security is a function of a computer information system. Therefore, when considering the security of computer network system comprehensively, we should not only analyze the technical security of network system, but also use targeted measures to ensure the security of network information, so as to effectively create a good network environment computer communication system.

Computer network technology is the soul of Internet development. The development of computer network technology is closely linked with Internet technology. Each year, tens of billions of dollars are lost due to network security. so we can see that network security is particularly important. In particular, the modern Internet is widely used in various industries, the Internet users are increasing and we are more and more dependent on the Internet technology. However, because of the poor stability of the Internet technology, network security problems often appear. Therefore, we must further study Internet technology and find a perfect and effective security technology. Based on this, this paper analyzes the network security risks in the process of modern computer network communication comprehensively, and puts forward the corresponding emergency response technology, so as to effectively ensure the security of the computer network in the communication process.

1 Computer network security technology and its security risks

1.1 The role of computer network security technology

In simple terms, computer network security is information security, that is, whether computer information has good confidentiality, and whether it can effectively prevent the outsiders from malicious computer information theft and malicious vandalism. Computer network security technology has a wide range, including security, confidentiality and other technologies. Computer network security plays an important role. In the context of the increasing popularity of modern computers, both individual user and corporate users are particularly dependent on computers. If the security of the computer network is not guaranteed, the information of the enterprise or individual will be leaked. However, at present, the computer security technology in our country can not effectively guarantee the security of the data in the transmission process, and has some loopholes in the process of data transmission, so that some malicious people enter the system and bring serious losses to the users.

1.2 Computer network security risks

1.2.1 Virus risk

Relevant practice shows that the computer network virus has been written and disseminated from the program, and the virus industry chain has been moving towards Internet development. Relevant part of the research process shows that the general computer virus will have a more active situation, the most important mode of transmission is the Trojan virus in computer networks. At present, computer viruses and related Trojan programs are generally not detected by the safe anti-virus system, nor can they be found, and the virus's ability to damage the security system is constantly increasing. It can be seen that modern computer networks are threatened by potential conditions.

1.2.2 Lack of cognition

In the process of computer use, some enterprises and individuals lack full knowledge and understanding of the security risks in computer networks at present. And they also can not realize the good security measure of the computer network, thus the probability of occurrence of the internal network security accident is raised and even has a certain upward trend. It can be seen that the internal network threats also belong to the more serious security threats. When computer security policy is unknown or unenforceable, if the users use unsafe site, or click on an unlawful link in an e-mail without taking measures of data encryption, then this part of the loopholes will increase the occurrence probability of security threats. Personnel are also changing in the process of movement, then the use of no encryption devices will lead to greater risk in the development of the network. Moreover, in the whole process, because of the problem of dual use of one machine or the situation of multiple use of one machine, the frequency of switching between internal network and external network is increased, and the probability of information leakage and virus spreading is also effectively improved.

1.2.3 Hacker threat

In the modern computer network security threats, one of the most important is the hacker.At present, cyber security in computer network information systems is more likely to be threatened by hackers. To some extent, computer networks are platforms in which hackers can attack the contents of the network through their own technical features and economic conditions. They can make full use of network security vulnerabilities to attack computer network systems so as to effectively obtain corresponding information, thus obtain the corresponding benefit. Then the information and data in the attacked computer network will be damaged or lost. And that will lead to the breakdown of the network system, seriously endanger the network security and affect the normal life of the people. To some extent, hackers belong to the greatest potential hazard in the computer network security risks.

1.2.4 Operating system

At present, most computers use the Windows operating system. However, because the system has loopholes, they are also favored by hackers and viruses. They are relatively easy to attack the loopholes in the operating system and cause the computer operating system to not work properly. If the user information, passwords can be easily cracked, then the hacker will be able to operate the operating system interface for any operation, as a result, it will cause greater losses to users. This requires regular updates and testing for the operating system. Some large enterprises and related government departments use large network operating systems in order to reduce the vulnerability of the system. To a certain extent, it can effectively guarantee network security, but it still requires professionals to operate the system and improve the promotion cost, so the operation system cannot be popularized.

2 Security emergency response technology of computer network

2.1 Emergency response of computer network security

The object of the emergency response of the computer network is the information, storage and processing of information security events in the network or computer. The main body of the incident includes the system itself, the outside world and the inside of the organization, the computer virus and so on. According to the security objectives of the computer information system, the security incidents can be defined as the information processing system CIA and the information destruction behavior.

Corresponding computer network security emergency activities mainly include two aspects: First, remedial measures. This is also the measure used after a security incident. Its main purpose is to effectively reduce the loss caused by the event, which includes the system itself or the person. It mainly refers to the operation of virus detection, system backup, system recovery, isolation, intruder forensics and virus elimination after discovering security incidents. Second, take precautions. It mainly refers to preparing for safety incidents, such as making safety plans, assessing risks, issuing safety notices and training awareness of safety. It also includes a variety of precautionary measures.

The above two aspects of work can complement each other. It provides a framework for preparing and planning response actions after the appears of security events, otherwise the response will be confused. This kind of action without rules will increase the loss of safety events. In addition, the event response refers to the understanding of the problems and shortcomings in the event plan, so that the lessons can be learned to achieve the effective improvement of the security plan. Therefore, these two aspects can create a positive feedback mechanism and effectively create an organizational security system.

2.2 Emergency response technology of computer network security

2.2.1 Firewall

The purpose of the firewall is to use computer software and hardware to cooperate with each other to create a network security control valve in the computer LAN and the Internet, in order to effectively prevent the internal LAN from being intruded illegally. A firewall refers to the creation of a separation barrier in the Internet and intranets. Firewall technology is now widely used in computer networks. Because of its high degree of transparency, simple and practical, and the original calculation and network usage system security it maintains, it is currently the most economical and effective measures to improve network security. The main purpose of setting up a firewall in an independent used router is to filter information data that is dangerous and unreachable . The firewall can also be set up in the computer host, which can effectively guarantee the security of the computing network.

2.2.2 Computer network tracking technology

Computer network tracking technology refers to using the corresponding computer information collection to achieve a comprehensive analysis of the problem, and finally finding the IP address of cyber attackers effectively, so as to find a targeted solution. The main content of this technology is to confirm whether the computer network host is in a safe state. Based on this premise, we can effectively process and analyze the collected data, so that the network providers can achieve corresponding activities in the network association. The computer network tracking technology mainly includes active and standby. Active tracking technology and information implicit technology are closely linked. For example, adding special tags and undetectable content to the returned HTTP file, allowing the computer network to trace the origin of the cyber attacks using the appropriate special tags. Passive tracking technology refers to tracking events by using corresponding product equipment, for example, the existing products are mainly based on the comprehensive analysis of network print content to achieve tracking. In theory, computer networks mainly connected to different states effectively. The network feature data is also changing constantly. Then, we use the record of different locations of network attack markers to analyze the differences of trajectories of network nodes through all the networks in the same time, so that we can get the trajectory of the future network attacks.

2.2.3 Information evidence acquisition technology

Computer information acquisition technology refers to the collection, identification, maintenance, and inspection of the information stored within the computer or network equipment. Computer information forensics technology mainly includes technologies of physical evidence and information discovery. In the emergency response technology, it is particularly important to obtain the evidence of the invasion of the computer by the attacker. This technology can not only effectively combat cybercrime, but also provide some judicial evidence to the judicial supervisory authority. The acquisition of physical evidence refers to techniques that we find and search the relevant original records at the crime scene. This is also the basic work for the collection of evidence. After obtaining the physical evidence, we must ensure that the data obtained will not be damaged by other networks. The key technology also enables lossless backups, as well as repairing deleted files. The information discovery technology can analyze the original evidence in an all-round way and find evidence that can prove the crime.

Conclusion

In the continuous development of network technology and information technology, the range of

Internet has been effectively expanded. The diversified information in the network has facilitated the use of the Internet. But because the scope of computer network is more and more extensive, and its geographic distribution is wide, the network is also open and free, and it can also cross borders such as national boundaries, which brings the greatest potential safety hazard to users. Therefore, it is important to improve the network security problem effectively. Network security problems in the process of use is simply the information security of the network, that is, the hardware, data and software in network system can be effectively protected, and will not be damaged, changed or leaked maliciously. As long as the system can run smoothly and reliably, then the network service will not be interrupted. Based on this, this paper analyzes the potential safety hazard of the computer in the process of operation, and then resolves it through the targeted emergency response technology.

Reference

[1] Lu Canju. Analysis of Computer Network Security Risks and Emergency Response Technology[J]. Journal of Modern Industrial Economics and Information Technology, 2016,(12):86-87,89.

[2] Lin Yamei. Analysis of Computer Network Security Risks and Emergency Response Technology[J]. COMMUNICATIONS WORLD,2015,(19):66-67.

[3] Chen Lingling. Discussion on Computer Network Security Potential and Emergency Response Technology[J]. Digital technology and Application,2016,(4):200.

[4] Cui Nannan. Analysis of Computer Network Security and Emergency Response Technology[J]. Computer CD Software and Applications,2013,(4):148-149.

[5] Zhao Yangjie, Liu Junshan. Research on Computer Network Invasion Emergency Response[J]. Consumer Electronics Magazine,2013,(6):64-64.

[6] Xu Meiling, Li Qian. Discussion on the Emergency Response Technology of Computer Network Security[J]. Wireless Internet Technology,2013,(4):20-20.

[7] Zhang Shengtao, Zhang Wenqian. Research on Computer Network Security and Emergency Response Technology[J]. Journal of Dossier,2016,(3):733.