World Scientific Research Journal (WSRJ) ISSN: 2472-3703
www.wsr-j.org

Research on the Development and Trend of Network Information Security Technology and Management

Fang Wei

Network and Education Technology Center, Binzhou University, Binzhou 256600, China

fw528@126.com

Abstract: With the continuous development of network information technology, great changes have taken place in people's work and life style. To a certain extent, network information technology has brought convenience to people and promoted the development and progress of all walks of life in society. However, the security problem of network information technology has also brought great trouble to the people. More and more attention has been paid to network information security technology and management. This paper will analyze the current situation of network information security, influence factors, technical means, management measures and countermeasures, and elaborate the development trend and analyze the key problems in depth so as to lay the foundation for the follow-up research.
Keywords: Network information security; Network security technology; Network information security management.

---

1. INTRODUCTION

With the continuous development of network technology, the status of the Internet in the work and life is constantly improving. Human beings are almost always in the exchange of data information through the network and the outside world. Information has become an important production resource, and the network has become the carrier of mass information. Network information is closely related to work and life, and its safety is very important for the normal operation of work and life. For the state, network information security is an important part of national security; for individuals, the disclosure of network information may cause personal privacy and property loss [1]. In February 2014, the Central Committee of the network security and information management was set up by the Central Committee, and general secretary Xi Jinping was the leader of the group. This is another important measure to implement the party's strategic deployment in the third Plenary Session of the 18th CPC Central Committee [2]. This top level design helps to ensure the national network and information security. It is the necessity of the modernization of the national governance system and the governance capacity. Requirement. General Secretary Xi pointed out that "without network security, there will be no

national security; without information, there will be no modernization." It can be seen that the research on network information security technology and management is very meaningful.

2. CURRENT SITUATION OF NETWORK INFORMATION SECURITY MANAGEMENT

While the development of network information technology provides convenience for people, it also brings new problems, such as network virus attack, private data leakage, sensitive information being stolen, and so on. The solution of these problems is imminent.

In recent years, the threat of the global network information security has been increasing, and the network information security has emerged as a new form. Many government websites have been attacked by network and the key facilities are frequently attacked by hackers. For example, in May 2015, the German Parliament was attacked by the network, and some information systems of the house of commons were shut down. In June, the Canadian government network servers, federal e-mail and department websites were hacked; many Russian media websites were attacked by large scale refusal services and network servers were paralyzed several times. The 750 thousand user information of Japan Airlines system was stolen; and so on, [3]. Based on this, all countries attach great importance to it and take various measures to deal with it actively. For example, the United States Department of Defense issued the cyberspace strategy, launching a network defense exercise for cyberspace, focusing on strengthening and cyber deterrence. Russia compiled the 2016 edition of the Russian Federal network information security theory, which proposed the continuous expansion of the scale of cyber crime, Russian information and communication technology and products. The five threat factors that affect the security of Russian state in the field of human information are made. The EU issued a security plan from 2015 to 2020 to deal with terrorist attacks and network crimes as the main goal; Japan introduced a new network security strategy, and began to implement the "unique code system", emphasizing the importance of the government organs of Japan. The information system is isolated from the Internet.

3. INFLUENCING FACTORS

The main objects of network information security management include network operation system, database and key hardware facilities. The network information security management technology is mainly aimed at the management of the network information security system, using various network security technologies to manage the security of the network information, in order to improve the security of the network information system. At the same time, a secure network can be constructed by controlling the hardware in the network system. The information environment of the collaterals. Generally speaking, the influencing factors of network information security can be divided into the following two categories.

3.1 External object factors

In network information security, hacker intrusion and attack are the main factors threatening network information security. The hacker has a complete understanding of the network

information system, mastery of the operation and logical relationship of all parts of the software system, and can use various technical means to invade the network information system, so as to obtain some important information data and even destroy the whole network information system [4]. The hacker's commonly used intrusion methods have illegal stealing and eavesdropping important information in the network information system, or modifying the database, causing the paralysis of the system to work normally.

Network virus is also a threat to the security of network information security, once the virus intrusion into the network information system, there will be data loss, slow system operation and other problems. Moreover, the spread and self replication ability of the network virus is very strong. Although it generally does not contain system files, it will also cause some harm to the network information system.

Network crime will also bring a great threat to the network information security. Network crime is a criminal act, such as computer technology, programming, decryption and other software instructions, and the implementation of network attacks. In general, cyber crimes include Internet fraud, information peeping, Internet slander and other phenomena. These crimes will bring great threat to people's work and life.

3.2 Self main factors

With the continuous development of network technology, operating systems and software systems are constantly upgrading, and there will be new vulnerabilities in the process of upgrading. Hackers use these vulnerabilities to attack and destroy the network information system, and steal some important information and file information, which brings great harm to the computer network system. In view of the various security risks existing in the network information system, it needs to be monitored through the corresponding security detection tools. In view of the vulnerabilities existing in various software, the general need to use antivirus software to repair it. However, there are loopholes in these security tools and anti-virus software, which will be exploited by hackers who are familiar with network technology.

In addition, due to the improper operation of the network information manager or the inaccurate encryption measures, errors occurred in the actual operation process. The illegal elements just use this opportunity to attack the computer network information system, steal the network information or destroy the network data. Moreover, some security software and security mechanisms used in network system information system also have some shortcomings. For example, firewall is a security protection software to prevent external intrusion, but attacks on Intranet can not be prevented.

4. NETWORK INFORMATION SECURITY TECHNOLOGY

4.1 Firewall technology

Generally, the firewall is a combination of software and hardware devices, a barrier between the intranet and the external network, between the private network and the public network. It is an image of security. It is a combination of computer hardware and software, and a security

gateway (Security G) is established between Internet and Intranet. Ateway), which protects the intranet from the intrusion of illegal users, and the firewall consists mainly of 4 parts of the service access rules, validation tools, packet filtering, and application gateways, which are composed of [5]. Firewall can effectively improve the security of network information system and the ability of virus protection, and play an important role in building a healthy and civilized network environment. Its main technical principle is to form a protective barrier in the TCP/IP network transmission layer and access control of past data information. It can not only analyze, filter, prevent illegal network access requests, but also transmit normal communication data[6]. At the same time, firewall technology plays a role of monitoring and tracking in network information security, and can record all kinds of communication logs between different networks.

Network information security is closely related to firewalls. They complement each other and make progress together. The function of the firewall is mainly embodied in three aspects. First, analyze the running state of network data, monitor the unsafe factors, and filter and prevent dangerous access requests. The firewall monitoring technology can study the computer network communication system as a whole, and analyze the external network information repeatedly, so as to achieve the purpose of preventing the risk and controlling the threat. Second, the multi-stage filtering technology of the firewall provides packet filtering services based on the set access control rules. Through the analysis of the communication protocol of the corresponding network layer, the protocol security is guaranteed and the protection is realized. When a packet is passed through a firewall system, the firewall will be filtered according to the access rules set by the network administrator. If the network address site that is to be accessed is set to prevent the access object, all the data from the site of this address will be blocked. Third, the firewall's network address conversion technology makes the firewall play the role of the proxy server in the network. Through mapping, the internal network address is converted to the external network address to be accessed. The real IP identity of each host is hidden and the hackers of the external network can not be attacked from the next hand, thus protecting the network information security.

4.2 Access control technology

Access control is an important part of the user's entry into the network system. First, the user name and password are identified and verified. Through the identification of user accounts and the verification of the password, the illegal operations of some illegal users can be prevented. With regard to the setting of accounts and passwords, users need to have some awareness of network security and set up passwords that are not easy to see through. Nowadays, there are also mature non password security access technologies, such as UsbKey in the online banking information system. When users log in, the digital certificate and password will not be recorded on the local computer, which greatly reduces the information leakage in the process of network communication. After the transaction is completed, the user can pull out the U shield and achieve the control of the user's information.

4.3 Data encryption technology

Data encryption technology is to encrypt network information, in order to prevent information data from being stolen by malicious means. There are two main methods of data encryption: key encryption and function encryption; the main components of the data encryption technology include the storage and encryption technology of data information, the transmission and encryption technology and the key management technology. The application of data encryption technology in all walks of life has important practical significance in guaranteeing the security of network information data. In the process of user interaction, data encryption technology can effectively prevent important information from being stolen, thus improving the security of network information. However, in the actual operation process, it is difficult to realize the effective application of data encryption. The main reason is that the data encryption technology involves more types of program, higher requirements for network technicians and difficult to master, and the process of data encryption technology is more complicated and complicated. To improve the level of network information management personnel.

5. MAIN COUNTERMEASURES OF NETWORK INFORMATION SECURITY MANAGEMENT

5.1 Build a perfect management mechanism

At present, the network information work has been responsible for independent agencies, the Ministry of industry and information is the most important department, but under the current regulatory mechanism, the Ministry of industry and information can not be intersectoral supervision. The relevant laws and regulations related to network information security appear in the form of single line law. There is no unified legislation and no system. However, with the continuous development of network information technology, it is a general trend to introduce special laws and regulations as soon as possible. The network is the product of the continuous development and progress of human society. The user relationship is very complex, the form of network is numerous and diverse, the Internet is used by any class of people, and many users are not aware of the risk of network information security. Although the technical means mentioned above can guarantee the security of network information, the security and management of network information involve many aspects, and it is difficult to master all aspects of the needs by a single organization. In the future, the future will face more complex network information security and its management problems. It is necessary to construct a relatively perfect management mechanism as soon as possible, take measures from laws, regulations, talents, management and technology, improve management level, increase the ability of independent research and development at the national level, and expand the construction of professional and technical personnel. Wait.

5.2 Cultivate a good sense of management

Network information security management refers to the standard requirements that must be followed in order to achieve information security in the network environment. Generally

speaking, the network information security countermeasures mainly include three aspects: first, the legal system, the timely formulation of the network information data transmission security closely related laws and regulations. At the same time, we should carry out safety education and related technical training for network information security managers to improve their safety management consciousness and comprehensive business level. Second, advanced management technology is an important prerequisite to ensure the safe operation of network information. Network users need to understand the potential threats and risks of the network environment, and evaluate them, determine the corresponding types of security services, and formulate corresponding security mechanisms, thus forming a relatively perfect network information security management. Technology. Third, the leadership of enterprises and institutions should attach great importance to the importance of network information security and strengthen the education and training of network information security managers.

5.3 Introduction of network information security audit system

Network security management technology is a very complex system engineering, firewall technology and intrusion detection technology are mainly for the external network environment security measures, but they cannot completely protect the network information from attack. If we want to truly create a more perfect network information security environment, we need to introduce security management technology into the intranet. Combined with the development of network information security technology in China, we must work hard on the research and development of the network information industry, develop a network information security audit system that can make up for the loopholes in the firewall technology, create a good ecological environment for the vast network users, and avoid the user's important information stolen by illegal molecules.

The network information security audit system can accurately record every operation log and content of the network user, monitor the operation process of the database server and the whole network behavior. For example, internal personnel send important documents to leaders or colleagues through QQ, WeChat, or mailboxes. These documents involve important data in the industry. If they are leaked out, the country or unit will suffer serious losses. If the network security audit system is introduced, all network operation behavior will pass through the system, and any operation can quickly locate, quickly identify the parties concerned, provide evidence and convenience for the follow-up processing. In addition, the network information security audit system can also control the whole network security situation as a whole, on the one hand prevent some of the internal important confidential information to the outside world; on the one hand, it can also carry out intelligent detection and evaluation of the network information, so as to accurately identify potential security risks that may affect the system operation. In order to protect the network information environment more and more healthy and stable, and to achieve sustained and harmonious development.

5.4 Protective measures

In the network information security management, the hacker or the attacker occupies the initiative. When the attack is carried out, what technology to use and where to start, the attacker

has the dominant advantage and has the active right in the confrontation. And the safety management side only completes a very comprehensive defensive measure to resist this kind of opponent, and there are great risks in the process of challenge.

In the management and protection of network information security, technology is the key factor, and the strength of technological force determines the result to a large extent. The network information security protection has a certain complexity. The security protection products of the network information security are also diversified and diversified. The infrastructure and software system itself is composed of different brands, different models and different structures. All the protection scope is not only the network attack and the virus invasion of these objects. Factors, but also on the product itself loopholes, short board risks brought about by the implementation of comprehensive protection measures. Moreover, the key technologies of the hardware and software systems are opaque to the users, so that the network security managers have no foundation for the control of the risk, and the security problems are not available. At the same time, it also reflects the shortage of network information security management personnel, especially those who can combine technology, security and management closely and make full use of the talent is more short, training professional technical personnel is the prerequisite for technology and protection measures. Only with the network information security management professionals, can the network information security protection work well, can resist the various network security threats and risks, thus forming a healthy network operation environment, this is a harmonious and benign cycle process.

In a word, it is also a complex system work to do a good job of network security protection. Equipment protection is the basis of network information security. Security management is the guarantee of network information security. The security strategy is an important link of network information security management. Once the security practice is appeared, the emergency treatment is also a part of the protection measures. Reduce the loss and harm to the minimum.

6. FUTURE TRENDS AND PROSPECTS

6.1 Network security protection technology to intelligent control

At present, the network information security technology has an embarrassment of "high one feet high and one foot high," and the means of security protection are at a disadvantage, which further stimulates the development of network security management technology. Network security protection and management are the whole process of network technology development for a long time. Through monitoring and tracking, data analysis and statistics, parameter collection, testing and other technical means to analyze the network state synthetically, find out the existing problems or loopholes, so as to adjust the software parameters and hardware configuration, so that the whole network can be adjusted. The collaterals run on the best track. With the development of intelligent tools and technical means, it is believed that the network information security protection will be gradually transformed by artificial intelligence.

Through the intelligent decision support system, the network security managers can provide appropriate solutions and suggestions to the network security managers, and can also carry out data analysis and explanation.

6.2 System of network information security management

In the process of network information security management, technology and management are complementary and indispensable, and even management will play a greater role. Technical level is high, management level can not keep up, loopholes and security problems are difficult to combat. We should gradually establish a network information security management system to provide legal guarantee and economic guarantee for network security problems. In the future, the demand for network information security will become more and more high. The demand for network information security of network service will be more and more large, and the integrated defense system will change from single to comprehensive. In addition, the integration of hardware and software functions is also the trend of the times. The convenience of life requires the less components of the hardware in the future, and the functions also want to be integrated into the same set of network systems.

6.3 Coverage of network security technology and management will continue to expand

With the popularization and improvement of large data and cloud computing technology, network security technology also has a new demand, and the security and management of cloud data has become a problem that we pay attention to. A large number of network information security needs determine that the coverage and depth of network information security technology and management will be further expanded.

ACKNOWLEDGEMENTS

The author was supported by Key Research Project of Binzhou Social Science Planning in 2018, China (18-SKGH-27).

REFERENCES

[1] Y. Liu, Y. J. Hao. Summary of foreign information security situation in 2015, Secrecy Science and Technology, Vol. 12 (2015), 16-18. (In Chinese)
[2] T. Y. Pu, Z. C. Rao. Computer information network security status and preventive measures, Electronic technology and software engineering, Vol. 6 (2018), 233-234. (In Chinese)
[3] L. J. Yin. Application Research of firewall technology in computer network security, Journal of Xingtai Polytechnic College, Vol. 2 (2018), 102-104. (In Chinese)
[4] K. Peng. Development and application of computer network security management technology, Electronic technology and software engineering, Vol. 6 (2018), 224. (In Chinese)
[5] X. Z. Liu. Application value of data encryption technology in computer network security[J], Electronic technology and software engineering, Vol. 6 (2018), 197. (In Chinese)
[6] W. Ding. Development status and trend of network security technology, China management informatization, Vol. 6 (2015), 47. (In Chinese)