Research on Information Security and Protection Strategy of Computer Network Based on Information Entropy

Zhijie Li*

Guangdong Mechanical & Electrical Polytechnic, College of Computer and Design Guangzhou, Guangdong, 510550, China

Keywords: Computer; Informatization; Risk Management; Security Measures

Abstract: Now the computer has been popularized to thousands of households, has been widely used. Computer security is also facing severe challenges. In order to make the computer Internet better serve human beings, it is necessary to improve all kinds of computer security standards. With the continuous improvement of social informationization, a globally integrated information society has been formed, which leads to the rapid increase of people's dependence on computer networks. The uncertainties that threaten the security of network information are gradually increasing, and network information security incidents occur frequently. As the basis of risk management, risk assessment is an important way for organizations to determine information security requirements, and belongs to the process of planning information security management system. As global information becomes more widespread, its role is becoming more and more important. The security measures of the network should be able to address a wide range of threats and vulnerabilities. This ensures the confidentiality, integrity and availability of network information.

1. Introduction

Now is the Internet information age, computer information science and technology has been popularized to most people. Information technology is developing rapidly, network has penetrated into all walks of life, and air traffic control related units are no exception [1]. With the rapid development of computer technology, the development of today's society has been inseparable from the information network. With the wide application and rapid development of computer network technology, computer information network has become the infrastructure of modern information society [2]. The degree of social informatization continues to increase, forming a globally integrated information society, which has led to a rapid increase in people's dependence on computer networks [3]. Risk management refers to identifying, controlling, and reducing or eliminating security risks that may affect an information system within an accepTable cost range. Now is the age of knowledge, Internet knowledge has long been transparent [4]. In the process of using the Internet, we will encounter various security issues. The uncertainties that threaten the security of network information are gradually increasing, and network information security incidents occur frequently.

Because the information transmitted by computer networks involves various fields such as finance, science education, and military, it contains huge economic or national interests [5]. Computer security issues have also become increasingly prominent, with the vulnerabilities and potential threats of nature and man-made factors. Computer networks have become an important tool in people's daily work, life and learning. As the basis of risk management, risk assessment is an important way for organizations to determine information security requirements, and belongs to the process of organization information security management system planning [6]. Although the operating system and anti-virus software are doing perfectly, many strategies are given. However, other serious problems are neglected and the real protection safety cannot be guaranteed. Network information security is related to national security and national development. With the global informatization becoming more and more extensive, its role is becoming more and more important [7]. Network security measures should be able to address all kinds of threats and vulnerabilities in an all-round way. Only in this way can the confidentiality, integrity and availability of network information be ensured.

2. Threats to Network Security

Computer information security is to protect personal data stored in the computer information will not be leaked or stolen by others. It also protects computer hardware, applications and operating systems that have been maliciously destroyed. Vigorously safeguarding network information security is to protect the hardware and software of network system. Only by physically isolating the Intranet from the Public Network can the Intranet be truly protected from hacker attacks from the Internet. In view of the openness, sharing and convenience of computer network, computer information network has brought great convenience to people's work, life and learning. With the understanding of the importance of information security risk assessment, risk assessment tools are widely used, and new requirements for the development of risk assessment tools are also proposed [8]. Intelligent decision support provides expert-level solutions for the average user in the face of various security situations. According to the expert experience, the reasoning analysis gives the best and innovative control method.

Most of the current people who use computers have had a process of poisoning. For users, the definition of network information security will be different because of different angles. There are many ways to scan, either by manual scanning or by port scanning software. Computer network information security risk assessment can effectively analyze the current and future risk development trends and locations of network information systems. To assess the threat and impact of these risks on computer network information security, so as to better formulate security defense strategies. Intelligent risk assessment tools have learning ability, which can generate new knowledge in continuous use and face new problems. Computer network is a shared resource and one of the main media for people to communicate, but it is also the living environment of unsTable factors.

As a user, they want their private information not to be stolen on the network. Many useful information can be obtained by scanning the port of the target computer. Data cleaning is carried out from the analysis of abnormal node training data and extracted parameters, and then data generalization is carried out to determine the possibility of the data being sampled and detected appearing in the model. Figure 1 shows how big data reshapes the structure of Internet information security supervision.

Fig. 1 Big data reshapes the structure of Internet information security supervision

In the management of employees, it is necessary to increase management efforts and assign operators the authority to operate. When entering a commercial website, you must protect your username and password and protect your personal information. A good network configuration requires formal and unambiguous description of all network components and their architecture, functions, and interrelationships, including the process of discovering and configuring critical devices on the network [9]. Through port scanning, you can get a lot of useful information to discover system security vulnerabilities. The security requirement of computer network information system is determined, and the network security control is included in the implementation plan of computer network information system. Current risk analysis tools mainly rank risks to remind users that major risks need to be addressed first. It did not calculate how much economic losses the organization would suffer from major risks. Software reinforcement is to try to make up for system software vulnerabilities, install anti-virus protection software, avoid installing software from unknown sources, and some bundled software.

3. Network Security Protection of Computer

Human destruction of computers is also a major hidden danger faced by security issues. For example, hacker attacks can be handled by power off, but man-made malicious attacks can not be prevented. The main purpose of configuration management is to enhance the network manager's control over network configuration, which is achieved by providing fast access to device configuration data. As a mature technology, monitoring plays an irreplaceable role in assisting network administrators to monitor network transmission data and eliminate network failures. The computer network information system needs to be regularly evaluated for security testing to measure the effectiveness of the security control of the computer network information system. Only the network information system security risk assessment is in the initial stage, and the relevant risk assessment practice experience is insufficient. The risk assessment of computer network information systems involves a large number of disciplines, which is both a technical issue and a problem of management and research. Organizational managers are concerned with the issue of economic losses. Because they want to use limited funds for information security management, while weighing the cost-to-value ratio.

Information security risks are security incidents caused by the vulnerability of human or natural threat utilization systems. And the impact on the organization due to the importance of damaged information assets. Some viruses with harmful effects will be camouflaged and hidden, so that anti-virus software cannot kill and kill, which brings great inconvenience to the users. The performance management is based on the network performance standard to detect the utilization of the network, which is mainly composed of the detection of performance alarms and the network reconfiguration after the performance failure. Network monitoring also brings great hidden dangers to network security. When information is transmitted, tools can be used to set the network interface in the mode of monitoring. It is also necessary to promote multi-disciplinary risk identification so that the accuracy of risk assessment of computer network information systems can be audited. Avoid the content of legacy risk caused by incompleteness, leading to the existence of holes in information system security defense measures. Regular risk assessment is needed to understand and master the security status of the system. Risk assessment is an indispensable technical means in the process of information system security level determination and construction.

The purpose of risk assessment is to fully and accurately understand the status quo of network security in organizations, and to find out the security problems and possible hazards of the system. Because the computer network is popular, information security can not be effectively guaranteed. The goal of performance management is to detect and measure all aspects related to network performance and to ensure that network performance can be maintained at an accepTable level. The purpose of information encryption is to protect the data, files, passwords and control information in the network, and to protect the data transmitted on the network. Data transmission encryption technology mainly encrypts the data stream in transmission. Commonly used are link encryption, node encryption and end-to-end encryption [10]. It is necessary to fully transform the traditional security defense concept of the computer network information system management unit, and fully understand the risk identification and assessment of the computer network system. In turn, it supports risk assessment and better realizes the security defense of computer network information systems. Through reasonable steps to develop a security strategy and its management and implementation specifications that suit the specific conditions of the system, it provides a reference for the design of the security system.

4. Conclusion

The arrival of the information age is the age when people enjoy life, so Internet information technology has become an indispensable existence. Users' demand for security will become higher and higher, and the network security requirements for network services and individuals or enterprises will become larger and larger. With the development of computer technology and communication technology, computer networks will increasingly become an important means of information exchange, and have penetrated into various fields of social life. The complexity and uncertainty of the system are getting higher and higher, so relying on traditional quantitative analysis methods can not fully obtain the hidden risk factors in the information system. Through risk assessment, we can clearly understand the important assets, main threats and weaknesses of business information systems. Risk assessment, as a means of checking the rationality of information security guarantee system, plays an important role in ensuring information security. We should improve laws and regulations and strengthen the management of the computer industry. Strengthen supervision on information security to ensure that network information runs in a healthy environment.

Acknowledgement

The 13th Five-Year Plan of Philosophy and Social Sciences Development in Guangzhou for 201 9 (Grant No. 2019GZGJ174).

References

[1] Songchang J, Shuqiang Y, Hong Y, et al. Design and Implementation of Network Information Security Testing Platform[J]. Journal of Chinese Computer Systems, 2013, 34(10):2304-2309.

[2] Dong, Na L. Design of Computer Information Network Security System[J]. Applied Mechanics and Materials, 2014, 539:305-309.

[3] Chen T M. Chapter 8. Guarding Against Network Intrusions[J]. Computer & Information Security Handbook, 2013:149-163.

[4] Pawar M V, Anuradha J. Network Security and Types of Attacks in Network[J]. Procedia Computer Science, 2015, 48:503-506.

[5] Kraemer S, Carayon P. Human errors and violations in computer and information security: the viewpoint of network administrators and security specialists.[J]. Applied Ergonomics, 2007, 38(2):143-154.

[6] Oshri I, Kotlarsky J, Hirsch C. Information security in networkable Windows-based operating system devices: Challenges and solutions[J]. Computers & Security, 2007, 26(2):177-182.

[7] Abler R T, Contis D, Grizzard J B, et al. Georgia tech information security center hands-on network security laboratory[J]. IEEE Transactions on Education, 2006, 49(1):82-87.

[8] Oorschot P C V, Robert J M, Martin M V. A monitoring system for detecting repeated packets with applications to computer worms[J]. International Journal of Information Security, 2006, 5(3):186-199.

[9] Zhang S. A model for evaluating computer network security systems with 2-tuple linguistic information[J]. Computers & Mathematics with Applications, 2011, 62(4):1916-1922.

[10] Kraemer S, Carayon P, Clem J. Human and organizational factors in computer and information security: Pathways to vulnerabilities[J]. Computers & Security, 2009, 28(7):509-520.