Design of Computer Network Security Defense System Based on Big Data

Wei Huang*
Lijiang Teacher’s Colleges, Yunnan, Lijiang, 674199, China

*Corresponding author e-mail: huangwei@lj-edu.cn

Abstract. The era of big data promotes the development of computer network, which plays a very important role. Big data can improve people's life and work enthusiasm with high quality, and further sublimate the standard of the masses. Because of the openness of computer network, it always leads to unnecessary security problems. Therefore, in order to apply the computer network on a large scale and avoid the information leakage caused by the network, this paper proposes the research on the design of computer network security defense system based on the background of big data. First of all, the importance of computer network security is discussed; secondly, the types of network security attacks are discussed, and the computer network security defense system is built by using multi angle and active security defense strategy to maintain the safe operation of the network; then, the risk algorithm is analyzed, and the risk of the whole computer network can be estimated by setting the weight according to the importance of the obtained resources So as to formulate reasonable safety measures. Finally, through the system test, the system has good analysis ability and defense ability, and has outstanding effect in computer network defense.

Keywords: Big Data, Computer Network, Information Leakage, Security Defense

1. Introduction
With the development of science and technology, promoting people's life, making people go further in the information age. Computer technology and network technology are involved in a wide range of fields. The Internet and big data connect people all over the world. If people used to say that "the ends of the earth are very close to each other" only described people's spiritual intimacy, today's computer network has made this sentence a reality. In recent years, human life is inseparable from the Internet, 90% of the world wants to access the Internet, so the network security problem is becoming increasingly prominent.

With the popularity of big data [1-3], the importance of data makes the importance of network security increasingly prominent. The destructive activities of virus attacks [4] and hackers [5] have seriously affected the normal order of network society and national security. Therefore, computer network security defense [6-8] is particularly important in the new era. When we have important network security issues and timely improve the system, improve the security defense ability of the system, improve the computer network security is imperative [9-10]. In the development of computer
technology, there will be a variety of new problems and risk factors. We need to maintain network security on a large scale to avoid the loss of interests caused by the disclosure of information of the masses.

On the basis of big data, this paper creates a computer network security defense system. We start from the network security factors, analyze its importance, types and significance of attack, multi angle, active defense system. The network risk assessment can be carried out by analyzing the network risk algorithm. Finally, through the practice certification, the system carries out regular risk assessment on the regional network and shows the results. It reminds the network security maintainer to carry out system protection. The success rate of intercepting danger is 86%, and the accuracy rate of risk assessment is 74%. From the data, the defense system can effectively intercept various unsafe factors in the network, and timely remind the network maintenance personnel to upgrade the system regularly. Protect the resources and information security of citizens and create a green network environment.

2. Computer Network Security Analysis Algorithm

2.1. The Importance of Computer Network Security under the Background of Big Data
In today's information society, big data contains a lot of social data information, so the security of information system is of great significance to the whole society. From the state to the small to the individual, to the company and enterprise, the security of information system needs to be fully protected.

State and individual: both national defense and individual pay attention to network information security. Only when the information is protected correspondingly, political information and private information are not exposed, which directly harms the national economy. It is important to avoid information leakage and damage to the system caused by system leakage and damage. Through information filtering and other measures, mainly control the information leaked through illegal channels on the network, so as to prevent a large number of circulations.

Companies and enterprises: the importance of business information can be imagined. If the trade secrets are disclosed to the opponents, it will cause an invisible attack, affect the profits of the company or enterprise, and even endanger its reputation and market share.

2.2. Function Analysis of Computer Network Defense System under the Background of Big Data
Cloud computing, Internet plus, distributed network technology integrate server, user client, communication resources and other hardware and software facilities, and form a large scale network interaction system with clear and independent functions, providing technical support for the development of big data. Modern network technology pays more attention to system throughput, fault tolerance and other data, and the concurrency of most application systems has been greatly improved. When using B / S, C / S, P2P and other functional levels, big data applications can be divided into three functional levels, namely application service layer, management middle layer and infrastructure layer. These three functional levels are closely linked and operate independently. Each layer is composed of different hardware facilities to complete different functions and jointly provide technical support for big data application center.

2.3. Hierarchical Analysis of Computer Network Security Defense System Structure
Network security structure can be divided into three categories

Physical security is the protection of information transmission and storage on the network. That is to protect computer network equipment, facilities and other media from natural environmental accidents, as well as personal or various computer crimes caused by damage.

Security control refers to the control and management of the operation and process of the information stored and transmitted in the network information system. The emphasis is on the preliminary security protection of the information in the network information processing layer. Security control is mainly realized by the existing operating system or network management software,
router configuration, etc. Security control only provides preliminary security function and network information protection.

Security service is to protect and identify the confidentiality, integrity and authenticity of application layer network information, meet the security needs of users, and prevent and resist various security threats and attacks. Security services can make up for and improve the existing operating system and network information system security vulnerabilities to a certain extent.

2.4. Risk Algorithm Analysis

At the same time, the importance of information resources is taken as the weight. We will be able to estimate the risk of the entire network system.

Table 1. Overall risk value of the system

|          | Integrity | Confidentiality | Usability |
|----------|-----------|-----------------|-----------|
|          | 50%       | 20%             | 30%       |

Shown as Table 1, the physical damage factors in integrity, confidentiality and availability are uncertain, misoperation, system vulnerabilities, internal vulnerabilities, viruses, etc.

Suppose we use $W_i$ to indicate the importance of resources, and $R_i$ to indicate the danger of resources. We use values from 0 to 1 to indicate the importance of resources. 0 is the smallest and 1 is the largest. The risk value of resources is expressed as 0 - 10, with 0 as the lowest and 10 as the highest. Then $WR_i = W_i * R_i$ represents the hazard value of weighted resources. Only the hardware resources in the simple network system shown in the following figure are taken as an example. We estimate the risk of the entire network system.

![Simple network diagram](image)

**Figure 1.** Simple network diagram

Shown as Figure 1, there are weights and danger values. We can calculate the risk of the whole network system by estimating the network hardware facilities.

$$WR_1 = R_1 * W_1 = 7 * 0.8 = 5.6 \quad (1)$$

$$WR_2 = R_2 * W_2 = 7 * 0.5 = 3.5 \quad (2)$$

$$WR_3 = R_3 * W_3 = 20 * 2 = 40 \quad (3)$$

The network hazard value of the system is as follows:

$$WR = \frac{(WR_1 + WR_2 + WR_3)}{W_1 + W_2 + W_3} = \frac{49.1}{1.5} = 32.7 \quad (4)$$
3. Implementation of Computer Network Security Defense System under the Background of Big Data

3.1. Realization of Network Security Defense System Module
Through risk analysis, the network security defense system is constructed. These technical means mainly include the following types:

Firewall: firewall technology is known as the earliest and most mature network security technology. It combines the hardware and software of the computer, which is equivalent to establishing a protection layer between the internal protection network and the external network. All the data flow through the external network layer must be protected by the external network, so it is necessary to analyze all the data flow through the network.

Intrusion Detection Technology: different from firewall technology, intrusion detection technology focuses on filtering network layer packets based on rules. It is an analysis, record and detection of user application layer information, data and behavior. Through the analysis of security log and behavior data, the behavior is identified and classified to identify intrusion and attack. Intrusion detection technology is based on the information data of computer system to analyze the possibility of being attacked or other abnormal operations in the current computer network. It can realize real-time early warning and monitoring of the system and prevent security threats.

Audit and supervision technology: audit monitoring system is a very important system in network security. It mainly records all the activities in the network, and makes real-time, semi real-time or offline analysis of the records, so as to discover and warn the illegal activities in the network, track the attack activities, so as to reduce the consequences and risks of attacks.

Encryption technology: This is a very traditional but very effective information security measure. The encryption system in the network is mainly composed of storage encryption and transmission encryption. Storage encryption is mainly used in notes of application business system, while transmission encryption is mainly used in remote communication system and multi security VPN.

3.2. Experimental Ideas
In this paper, the functional requirements of the defense system are analyzed. Because the network virus can invade through a variety of ways, its hiding ability is outstanding, and it will cause great harm if it lurks in the computer network for a long time. Therefore, the research of computer network defense system must be carried out. The traditional way of prevention is to rely on firewall and other software for basic prevention. In this prevention system, active defense mode is added to the prevention system to check the system defects in real time. Active preventive measures are used to maintain the security of network system and determine the reliability of network operation. Through field investigation and practice, the system is applied to the evaluation of the regional computer network. The TCP/IP protocol runs through the four network layers. Through the experiment, the feasibility of the network defense system is very high, which provides efficient protection for the following network security problems.

3.3. Experimental Design
(1) The network defense system designed in this paper is applied to a certain area to detect the security of the host. Network attacks are carried out in four different periods, which are divided into attack a, attack B, attack C and attack D. Wait for the system to detect the attack and give a warning, and evaluate its loss and risk, and compare it with the real value (range 0-100).

(2) We simulate the test data of each module of the system in the form of questionnaire, and conduct a survey in the local network security maintenance company, and send the questionnaire to the local famous expert email in the form of file, and wait for the reply to make statistics. We set the score range of each module as 0-10 points, and then make them score according to the evaluation data.

4. Discussion
4.1. Comparison of Loss Value and Risk Value Assessment with Real Value

Figure 2. Comparison of loss value, risk value and real value

Shown as Figure 2, the different types of attacks in the four time periods have different hazard coefficients, and the risk value of the attack types is obtained by the risk analysis algorithm. For different types of attacks, the system needs to provide corresponding defense measures. Therefore, compared with the real value, the loss value and risk value are around the true value. After the test results are sent to the administrator, the results are recorded. The experimental results show that the system has the ability of analysis and defense for various types of attacks. Although there is a gap between the evaluation value and the real value, it provides a great help for the follow-up research.

4.2. Computer Network Maintenance Personnel and Expert Test Item Score
Figure 3. Scoring results of test items

Shown as Figure 3, computer network staff and experts have relatively high scores on the indicators of the system. The staff scored the highest on the intranet module of the system, which was 8.4. They think that the Intranet can prevent unauthorized users from accessing and probably exclude hacker attacks. It can also effectively prevent the leakage of sensitive information, ensure the controllability of the intranet, and prevent the abuse of power by internal personnel. The internal network can also provide external services, and the internal network defense of the system is very effective. Experts also gave high marks to the internal network defense. The second is the demand for server security, with scores over 7. The module can directly prevent unauthorized users from deleting and modifying data and avoid data leakage. The overall score of the network defense system module is high, although there are deficiencies, but it will be improved in the future.

5. Conclusions

The rapid development of computer technology puts forward higher requirements for network security. In the new social production conditions, the defense mechanism of the security system should keep pace with the times. New attack methods and means continue to emerge, improve the awareness of network security, strengthen the construction and improvement of computer network security defense system, is an urgent problem for computer industry practitioners. Although there is a gap between the value of risk and loss of different types of attacks and the real value, it can be concluded that the analysis and defense capabilities of the system meet the needs of network security. Through the detection of module data, the staff and experts can score the module, the security performance of the server and intranet is relatively high, and other modules are relatively low. To sum up, computer professional and technical personnel should actively explore, constantly improve the technology and level, enhance the defense ability of the system itself, realize the effective defense of network security threats, and strive to maintain a safe and healthy computer network environment.

References

[1] Howe, D. , Costanzo, M. , Fey, P. , Gojobori, T. , Hannick, L. , & Hide, W. , et al. (2008). Big data: the future of biocuration. Nature, 455(7209), 47-50.
[2] Armstrong, K. . (2014). Big data: a revolution that will transform how we live, work, and think. Mathematics & Computer Education, 47(10), 181-183.
[3] Naimi, A. I. , & Westreich, D. J. . (2014). Big data : a revolution that will transform how we live, work, and think | clc. American Journal of Epidemiology, 179(9), 1143-1144.
[4] Menge, D. N. L. , & Weitz, J. S. . (2009). Dangerous nutrients: evolution of phytoplankton resource uptake subject to virus attack. Journal of Theoretical Biology, 257(1), 104-115.
[5] Khera, & Mandeep. (2017). Think like a hacker. J Diabetes, Technol, 11(2), 207-212.
[6] Kayssi, A. , Ali El - Hajj, Assir, M. E. , & Sayyid, R. . (2015). Web - based tutoring and testing in a computer networks course. Computer Applications in Engineering Education, 7(1), 1-7.
[7] Jin, X. T. , & Yeh, R. K. . (2017). Graph distance-dependent labeling related to code assignment in computer networks. Naval Research Logs, 52(2), 159-164.
[8] Nezhad, S. M. T. , Nazari, M. , & Gharavol, E. A. . (2016). A novel dos and ddos attacks detection algorithm using arima time series model and chaotic system in computer networks. IEEE Communications Letters, 20(4), 700-703.
[9] Chen, G. , Gong, Y. , Xiao, P. , & Chambers, J. A. . (2015). Physical layer network security in the full-duplex relay system. IEEE Transactions on Information Forensics and Security, 10(3), 574-583.
[10] Kak, A. . (2017). "computer and network security". Friend of ence Amateurs, 31(9), 785-786.