Analysis of Computer Network Security and Countermeasures Based on Big Data

Jiang Baohua, Sun Hui*

College of Humanities & Sciences of Northeast Normal University, Changchun, Jilin, 130117, China

*Corresponding Author

Keywords: Big Data, Information Security, Network Security

Abstract: in This Paper, from the Current Situation of Computer Network Development, the Author Analyzes the Advantages of Big Data Information Technology, and Analyzes the Information Security Problems Faced by Enterprises in the Era of Big Data. Finally, Based on the Analysis of the Current Situation, the Paper Discusses in Detail the Measures That Small and Medium-Sized Enterprises Should Deal with in Information Security Protection, Hoping to Provide a Certain Degree for the Research of Relevant Content Basis of Reference.

1. Introduction

With the Common Development of Internet, Internet of Things and Cloud Computing Technology, We Have Entered the Era of Big Data. Using Efficient Big Data Technology is Conducive to Enterprises to Improve Their Own Advantages and Create Higher Production Capacity. However, Many Potential Crises Also Follow. Data Leakage is Becoming a Serious Disaster Area for Information Security of Global Internet Enterprises. as a Result of Data Leakage, the Credibility of Enterprises Decreases and Major Property Losses Occur Frequently [1]. Therefore, in the Era of Big Data, How to Solve This World Problem, Internet Enterprises in Addition to Apologizing, More Importantly, How to Prevent in Advance.

2. Overview of Big Data Era

In the era of “big data”, McKinsey, the world famous consulting company, was first mentioned. People are investigating and using a lot of data. With the new wave of production efficiency and consumer surplus, with the deepening of cloud technology, big data has attracted more and more attention.

The so-called big data (usually structured, used to describe the large amount of unstructured data of the enterprise), the data capacity of the previous TB to Pb or even ZB instructions. This data is used for analysis, which costs a lot of money and time. Big data analysis often needs to be combined with cloud computing. It requires tens, hundreds or thousands of computers for distributed computing [2].

In the era of big data, data also has the practical characteristics of low density. Big data technology can be used to reflect general information in society. The diversity of data information makes the proportion of each information continuously reduce, and the information of data is not correct and realistic, thus reducing the value of big data information.

In recent years, despite the popularity of the network and the development of computer technology, the general public began to have a new concept of big data. The popularization and application of big data involves enterprises, universities, government departments and other important institutions. Although the extensive development of big data technology has been affirmed, the security problems related to it have gradually become prominent, and information security has begun to appear loopholes in such a wide range of applications, which has a very serious threat to the operation of computer network itself and computer network security [3]. The crime caused by information security is rampant gradually, how to ensure information security has

  DOI: 10.25236/ISMHI.2019.035

become an urgent problem for enterprises and related departments.

3. The Current Situation of Computer Network Information Security in the Era of Big Data

3.1 People's Awareness of Computer Information Security Needs to Be Strengthened

When the Internet technology moves into the era of big data, network services can be closer to people's lives, which brings a lot of convenience. But at the same time, the frequency of related risks caused by the network is higher and higher. At present, on the one hand, due to the weak awareness of computer network security protection of most users and some network communication managers, information leakage, theft, loss and other security problems often occur in the computer network [4]. In addition, in the aspect of information management, because some network security administrators do not maintain the network which they are responsible for, the whole network system is vulnerable to attack; a variety of organizations such as various enterprises and schools have their own local area network [5]. There are a lot of data information stored in these networks. If we don't take reasonable and effective network maintenance measures to manage the related networks in a good and orderly way, it will inevitably lead to the leakage of information and bring unnecessary losses to the organization.

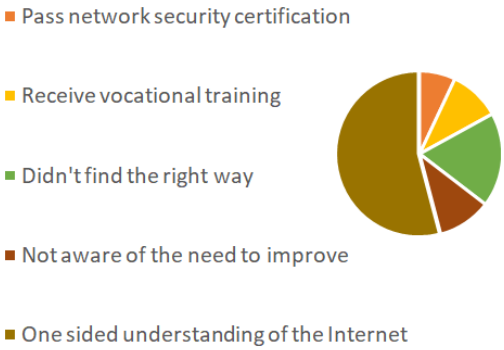

Fig.1 Network Security Survey Chart under Big Data

3.2 There Are Security Holes in the Computer Network

Computer network is composed of tens of thousands of network websites and various network software, which are always used in the specific operation of computer network. In fact, in the process of designing each website or network software, there will be more or less a certain number of vulnerabilities. Among these loopholes, some “loopholes” are the back door programs left behind by designers at the beginning of design in order to facilitate their own manipulation. When these backdoor programs are used by lawbreakers, it is easy to cause network paralysis, information leakage and huge losses [6]. At the same time, some hackers in order to steal the business secret information in the enterprise database will attack and invade the weak protection links of the core components of the enterprise network, such as routers and servers, which will have a very adverse impact.

Despite the rapid development of defect mining technology, however, no matter what kind of testing method is used, all defects in software and network can not be completely eliminated. Different from hardware, software will not suffer from physical damage, but it may fail due to some hidden factors. Because of the complexity and difference of network, the detection and prediction of network defects is always an important task [7].

4. Information Leakage Has a Serious Impact on Social Production and Life in the Era of Big Data

Computers and networks are part of human life for a long time. Generally speaking, most portals need personal information, such as name, age, location, etc. These websites store a large number of personal information. Due to the lag of network security protection management of crime related

enterprises, they can not be limited and managed, and many operations of website managers. Many website managers can easily control people's privacy to illegally make profits and other illegal behaviors.

According to data released by Tencent security joint lab, the number of specific apt type network attacks by enterprises in mainland China and Hong Kong increased by an average of 969%. Of the 440 Chinese companies surveyed, seven were attacked every day, about half of the global average. However, in the past two years, the average number of global cyber attacks has decreased by 3%, after 2015, by 30%, and the number of China is on the rise.

On March 17, 2018, the New York Times and the guardian jointly published an in-depth report, exposing the time when more than 50 million users' information and data on Facebook were stolen. A company called “Cambridge Analytics” illegally obtained the data of a third-party psychological test application that works on Facebook [8]. It uses algorithms to analyze big data, and predicts the political tendency of each user according to their daily hobbies, personality characteristics and behavior characteristics, so as to make profits. As early as 2015, Facebook knew about the data leakage incident and asked Cambridge to analyze and delete the acquired data. However, the company concealed the truth from Facebook and Facebook did not disclose the information in time. The backwardness of each website management system also provides opportunities for a large number of illegal elements. Their behavior will cause the network information to be in an unsafe state, and the personal information and privacy of some people will be leaked, which will bring serious adverse effects to our society.

At present, many enterprises are in the most basic stage of passive defense, that is, by installing some security software, patching vulnerabilities in time to carry out passive defense. For example, when DDoS attacks come, we start to use defense; when hackers invade, we think of using emergency response, which is often a remedial action of “mending the past” after the loss of food. In order to achieve a better degree of security protection, enterprises must strive to reach the third stage through their own efforts, so as to achieve real active discovery [9]. In this way, enterprises can build a better network security system, so as to reduce the security risk of enterprises to a large extent.

In the era of big data, the main problem of computer network security is to do a good job in the maintenance and routine management of computer network hardware, pay attention to the security of computer information dissemination and the comprehensive analysis of management security, so as to promote the improvement of computer network security in the era of big data.

5. Conclusion

In the face of the increasingly severe situation of user information data disclosure, Internet users can no longer continue to have a spectator mentality. As an Internet enterprise, we should set an example to avoid the occurrence of the probability event of “a thousand miles bank, breaking in the ant nest”. If an enterprise wants to develop, the key is to protect the core information of customers. To stand firm in the era of big data, the key is to face up to the problems and solve them.

References

[1] Wang Jia. (2017). Study on Network Information Security Based on Big Data. 2017 9th International Conference on Measuring Technology and Mechatronics Automation (ICMTMA). IEEE.

[2] CHEN Xingshu, ZENG Xuemei, WANG Wenxian. (2017). Big Data Analytics for Network Security and Intelligence. Advanced Engineering Sciences.

[3] Li Y. (2017). Research on Personal Information Security on Social Network in Big Data Era.

[4] S. Vijayakumar Bharathi. (2017). Prioritizing and Ranking the Big Data Information Security Risk Spectrum. Global Journal of Flexible Systems Management, vol. 18, no. 2, pp. 183-201.

[5] Alexander Grusho. (2017). Data Mining and Information Security. International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security. Springer, Cham.

[6] Shi K. (2017). Research on the Network Information Security Evaluation Model and Algorithm Based on Grey Relational Clustering Analysis, vol. 14, no. 1, pp. 69-73.

[7] HU Guo, MEI Dedong. (2017). Research and Application on Network Security of SMV in Smart Substation. Proceedings of the Csee.

[8] Chao Yuan, Yueming Lu, Jiefu Gan. (2017). Evaluating Network Equipment Information Security Based on D-S Evidence Theory and Principal Components Analysis. 2017 IEEE Second International Conference on Data Science in Cyberspace (DSC). IEEE.

[9] Branstetter L, Gandal N, Kuniesky N. (2017). Network-Mediated Knowledge Spillovers: A Cross-Country Comparative Analysis of Information Security Innovations.