Research on Network Information Security Issues and Strategies under the Internet Plus Environment

E Li
School of Intelligent Engineering, Shandong Management University, Jinan, China
1358727189@qq.com

Abstract—In today's world, with the rapid development of science and information technology, the internet has become an indispensable medium in people's daily life. Through the internet, we can carry out various activities very conveniently and save a lot of manpower and material resources. In recent years, internet plus has become a hot word. It aims to deeply integrate the internet with traditional industries and create new development ecology with the help of internet platform and network information technology. With the deepening of network information technology, network information security has become an increasingly prominent problem. This paper analyzes the network information security problems under the internet plus environment, and puts forward corresponding countermeasures to reduce the emergence of various network information security problems in order to maintain people's information security.

1. INTRODUCTION
The concept of internet plus was first proposed by premier li keqiang in the government work report delivered at the third session of the 12th National People's Congress on March 5, 2015. Internet plus is a new form of internet development under the innovation 2.0 era. It is also a new form of economic and social development promoted by the knowledge society innovation 2.0 era.

2. THE CONNOTATION OF INTERNET PLUS
Internet plus is the further practical result of internet thinking, which promotes the continuous evolution of economic forms, drives the vitality of social and economic entities, and provides a broad network platform for reform, innovation and development[1]. Generally speaking, internet plus means internet plus various traditional industries, but this is not a simple addition of the two, but the use of information and communication technology and internet platform, so that the internet and traditional industries can integrate deeply, so as to create a new development ecology. It represents a new social form, that is, make full use of the internet in the allocation of social resources optimization and integration, deeply integrate the innovation achievements of the internet into the economic and social fields, improve the creativity and productivity of the whole society, and form a new form of economic development with internet as infrastructure and tool.

Under the environment of internet plus, the network will naturally become a platform for people to carry out various activities. People can do almost any business through the network platform, most of which involves the input of people's personal information, especially all kinds of consumer activities, all of those relate to the safety of people's various vital interests. So, under the internet plus environment, how to better maintain people's information security has become an increasingly important issue[2].
3. THE CONNOTATION OF NETWORK INFORMATION SECURITY

Network information security is a comprehensive subject, which involves computer science, network technology, communication technology, cryptography, information security technology, applied mathematics, number theory, information theory and other disciplines[3].

It mainly means that the hardware and software of the network system and the data in the system are protected from being damaged, changed or leaked for accidental or malicious reasons. The system runs continuously and reliably with no interruption of network services[4].

Network information security has the following main characteristics:

3.1 Integrity
It refers to that information keeps the characteristics of non modification, non destruction and non loss in the process of transmission, exchange, storage and processing. That is, it is the most basic security feature to keep the information as it is, so that information can be generated, stored and transmitted correctly.

3.2 Confidentiality
Information is not disclosed to unauthorized individuals, entities or processes according to given requirements, or provide features for its utilization. This character means that it can prevent the disclosure of useful information to unauthorized individuals or entities, it also emphasizes that useful information is only used by authorized objects.

3.3 Availability
This character refers to the network information can be accessed correctly by authorized entities, and can be used in normal circumstance, or it can be restored to use under abnormal conditions. That is, it can correctly access the required information when the system is running, and if the system fails, it can be quickly restored. Usability is a measure of user oriented security performance of network information system.

3.4 Nonrepudiation
In the process of information exchange between the two parties, it is determined that it is the participants themselves and the real identity of the information provided by the participants. That is, all the participants cannot deny their real identity, the originality of the information provided, and the completion of the operation and commitment[5].

3.5 Controllability
This character refers to that the information and content of the circulation network system can be controlled. That is, all the information in the network system can be transmitted and stored in a certain range and space. In addition to the general form of communication website and communication content monitoring, the most typical policy is encryption policy, if the encryption algorithm is managed by a third party, it must be carried out in strict accordance with the regulations.

4. ANALYSIS OF FACTORS AFFECTING NETWORK INFORMATION SECURITY

Due to the complexity of current network structure, factors affecting network information security are also diverse. According to relevant investigation and research, the threats to network information security mainly includes the following aspects:

4.1 Virus invasion
Every computer can be faced with the risk of being attacked by a virus at any time anywhere. Computer viruses usually hide in files or program code, waiting for the opportunity to carry out self-replication, and can be spread through the network, disk, disc and many other mediums. Computer viruses spread so quickly that they can bring an immense impact for people.

The "virulence" of the virus is different, some of them can make some warning information playfully on affected machine, others may destroy or endanger personal computer and even the whole enterprise network.
Some hackers intentionally release viruses to destroy data, but most viruses are inadvertently spread. Computers can be attacked when employees open infected email attachments or download files with the virus, which caused the virus to spread. These viruses spread from one computer to another, making it difficult to detect them from a central point[6].

4.2 Hacking
With the development of computer technology, hacker has become a kind of threat. The illegal breaking in by hackers refers to the activities of deleting, duplicating and even destroying data by hackers who use the security vulnerabilities of enterprise network to illegally access the internal network or data resources without permission. Generally speaking, there are usually two kinds of intrusion motives and forms commonly used by hackers.

Hackers enter the network or personal computer by looking for an unprotected path, and when they do this, they can steal data, destroy files and applications, and prevent legitimate users from using the network, all of these will do harm to enterprises. Hackers’ illegal intrusion will have the potential of corporate killers, and enterprises have to be careful to prevent it.

4.3 Data theft and interception
Data eavesdropping and interception, that is the interception of specific packets on the network and analysis to obtain the required information directly or indirectly. Some enterprises need to take effective measures to prevent the interception of important data, such as the user's credit card number, when transmitting with the third-party network. Encryption is the best way to protect transmitted data from external eavesdropping by turning it into a code that can only be restored and read by an authorized receiver.

4.4 Denial of service
Generally speaking, denial of service attacks can paralyze a single computer or the whole network. The purpose of denial of service is to prevent users from using various network services normally, or to disturb some normal services of computer users. For example, they can prevent the users from accessing the service by breaking the connection between two computers. They can block legitimate network communication by sending a large amount of information to the enterprise network, which will eventually damage not only the network architecture itself, but also the operation of the entire enterprise.

4.5 E-commerce attack
E-commerce attack refers to the hacker who attempts to illegally invade the system from the technical level analysis, or through guessing program to decipher the intercepted user account and password, so as to make further operation after entering the system; or the hackers may use the vulnerability of some service processes provided by the server to obtain useful information and enter the system; or the hackers may use the weak links and security vulnerabilities existing in the network and the system itself or caused by setting errors to conduct electronic seduction, in order to obtain further useful information; or the hackers can obtain user’s password and hack the system through the system application vulnerability.

Of course, in addition to the factors affecting network information security mentioned above, there are also other factors, for example, malicious scanning, password cracking, data tampering, address spoofing, spam, infrastructure damage, and so on. All these factors as mentioned above can make a certain threat to network information security, so, we must take much more attention to these factors[7].

In order to understand the influence of the factors mentioned above on the network information security of the enterprise in detail, so as to strengthen the prevention of the network information security of the enterprise, in this paper, an internet company called A was investigated in our city, and the information on the number of times of various network information security attacks on all the enterprise websites in 2019 was obtained. Then the data obtained were statistically analyzed. The details are as follows: The times of all kinds of internal websites of the enterprise were attacked by various types of network information security threats are 14468 in total in 2019. The times of virus invasion are 2438, the times of hacking are 3896, the times of data theft and interception are 1284, the times of the denial of service are 2686, the times of E-commerce attack are 3168, and the times of others are 996. The times of different types of network information security are different, we can see the differences between them in the following table and figure.
### TABLE I: TABLE OF THE STATISTICS OF THE TIMES THAT COMPANY A WAS ATTACKED BY DIFFERENT TYPES OF NETWORK INFORMATION SECURITY IN 2019

| Types                  | Virus invasion | Hacking          | Data theft and interception | Denial of service | E-commerce attack | Others |
|------------------------|----------------|------------------|-----------------------------|-------------------|-------------------|--------|
| Times                  | 2438           | 3896             | 1284                        | 2686              | 3168              | 996    |

![Figure I: Histogram of the statistics of the times that Company A was attacked by different types of network information security in 2019](image)

### 5. Strategies for Maintaining Network Information Security

5.1 *Combination of technology and management:*

Technology and management are not isolated. Network information security is not only a technical problem, but also a management problem for an information-based enterprise. Antivirus programs or software patches usually appear online soon after many viruses or security holes appear, but why the viruses can still spread all over the world? Why the patches on the microsoft home page and various anti-virus tools can not stop the virus from spreading? The most fundamental reason is that many users (including enterprise users) may not form the habit of actively maintaining system security and lack a good management mechanism for security.

The key to ensure the safety of the system, first of all, pay attention to safety management, but not just sitting by. We can say that the information security of the enterprises, is an important problem which involves the whole enterprise. We must draw up the overall management strategies of keeping pace with the times from the height of the combination of management and technology, and implement these strategies conscientiously, only by this can we achieve the goal of improving enterprise information system security.

5.2 *Conduct risk assessment:*

It requires companies to find out which systems are networked, what their vulnerabilities are, what specific risks they pose to their operations, and how those risks impact the entire company.

5.3 *Make various safety implementation plans:*

It includes establishing the company's safety policy, mastering the basic technology needed to ensure safety, and planning the solutions that the company should take in case of a specific safety accident. The prevention strategy of enterprise network security is to decide how an organization can protect itself[4].
Generally speaking, security policy consists of two parts: an overall security policy and specific rules it contains. The overall security strategy establishes an organization's strategic security guidelines and allocates the manpower and resources necessary to achieve them.

Plan implementation: all security policies must be supported by a sound management control architecture, the most important element of which is to establish a complete security solution.

5.4 Physical protection:
That is, when the network is constructed, two sets of mutually independent networks will be established separately, one sets for office automation within the department, and the other sets for connecting to the internet. At the same time, only one hard disk is always working, in this way, the real physical security isolation is achieved.

5.5 Remote access control:
The main intent of this strategy is to facilitate some remote dial-up users in the enterprise, when they configure the user authentication server in the internal network. This strategy is mainly used to verify the identity and password of the access user technically, register all MAC addresses of the user's machine at the same time, and isolate illegal users by dynamically binding the IP address and MAC address[5].

5.6 Virus protection:
All network users should enhance the awareness of network drug control, and make unified arrangements for all networks to ensure timely and effective protection against viruses.

5.7 Actively use a firewall for protection:
At present, the most sophisticated firewall with the highest level of security is the covert intelligence gateway, which hides the gateway behind the public system to protect it from direct attacks. A covert intelligence gateway provides almost transparent access to internet services while preventing unauthorized access to private networks from outside. Generally speaking, the security performance of this kind of firewall is very high, it's the least vulnerable to damage and invasion[6].

6. CONCLUSION
Under the internet plus environment, the development of science and technology will be much more rapid, and the application of internet platforms will be more extensive and deeper. People can almost conduct a variety of business activities through internet platforms. Therefore, network information security has been attached more and more importance. This paper briefly analyzes the concept and characteristics of network security, analyzes several common factors affecting network information security, and finally introduces several commonly used strategies to suppress network security threats.

Generally speaking, the problem of network information security is not a simple technical problem, it involves security management and people's security awareness and other aspects. Therefore, we must consider all the problems when people use the comprehensive network platform. We should make different security strategies according to different network security problem, so that, we can avoid or reduce the generation and spread of network security problems effectively. At the same time, this strategy can also provide a safe network environment for people's daily life, work and study. We hope that the internet plus action plan will benefit the vast number of internet users.

REFERENCES
[1] Wang shiwei. On information security, network security, network space security [J]. Journal of Chinese library, 2015,03:72~84.
[2] Yu yue. Computer network information security and protection [J]. Electronic technology and software engineering, 2017,12:229.
[3] Yu jingping. On network information security and countermeasures [J]. China strategic emerging industry, 2012,12.

[4] Yu xiaoqiu. Information security and network security analysis [J]. China information security. 2014(08).

[5] Zhou lian-bo. Research on information security, network security and network space security [J]. Network security technology and application. 2015(12).

[6] Zhang baosheng, zou benna. Emphasis on network security to prevent digital risks [J]. Computer programming skills and maintenance. 2014(10).

[7] Wang xingwei, li jie, tan zhenhua, ma lianbo, li fuliang, huang min. Current situation and future trend of network technology for "Internet +" [J].2016.04:729~741.

[8] Jiang qiping. "Internet +" and the future shape of China's economy [J].2015,05:52~63.