The Establishment and Implementation of Information Network Security Plan

Wang Yuanyuan
Ideological and Political Department
Xi'an Peihua University
Xi'an, 710125, China
e-mail: 64789178@qq.com

***Abstract*—This paper explains the idea of information security and discusses the establishment of the security system of information network. By using the information system security engineering method, we will establish and improve the network security plan and disaster recovery plan through strict organization and management, adequate financial support, strong talent support and deep technical guarantee. This paper puts forward the overall strategic goal of the "people-oriented, to prevent the main" network security and the overall plan to solve the network security problems.**

Keywords-Information Security; Network Security; Network Security Plan

Information is the main trend of development in contemporary society. The rapid development of information has a great impact on all aspects of the state and society. The information network is the nervous system of the information society. As the main infrastructure of information communication, the security problem has become a new security research hotspot. At present, the threat control of network security has been extended from the technical level to the management level to a great extent.

I. AN OVERVIEW OF INFORMATION NETWORK SECURITY

A. The Concept of Information Network Security and The Idea of Information Security

Information network security is a security protection to prevent accidents and malicious attacks from the confidentiality, integrity, availability, controllability and non-repudiation of information itself and information system (network structure, application services, etc.). Information network security is based on the physical layer and operation level of information network system, as well as the protection of information itself (data layer) and the level of attack (content level).

The definition of the definition of network security at the technical level has been relatively complete. But the security of information network is a multi-dimensional, multi factor and multi-objective system. The establishment of a security system cannot rely solely on a single security mechanism and a variety of security services. Access to the security of the entire information network system depends on the combination of multiple security mechanisms and a variety of security services. The concept of information security, which was produced in 1990s, is the result of this idea.

The security system of information security is to ensure the security of information system through the combination of level and depth protection, active and passive defense. The basic components are shown in Figure 1.

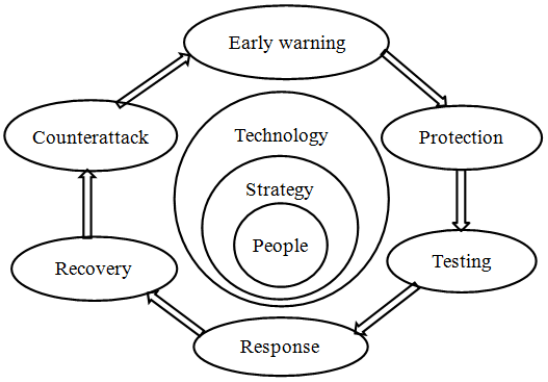

Figure 1. Information security system components

In the system of "human centered", the information security system not only attaches importance to the adoption

of safety protection technology to protect information, but also emphasizes "preventive measures". Active defense strategy is adopted to improve the ability of intrusion detection, vulnerability scanning, virus prevention, evaluation and audit, and the ability of rapid response and recovery after attack.

B. *The Necessity of the Research on the Security of Information Network and the Establishment of the Security System*

The development of information network technology has accelerated the process of social information. The development of information has opened up a broad space for the application of the information network system. However, because of the irrational decision making for the development of technology for many years, the dependence of the state and the society and the public on the information network has gradually increased. Information network is realizing information exchange and sharing. While greatly facilitating and enriching social life, network security has become an important factor affecting national security and social stability due to the vulnerability of network itself and human attacks and destruction.

Therefore, the current government of the world has taken information security as the focus of government work. Many laws and regulations related to information security have been issued. The international organization for standardization has also developed a large number of safety standards. The information security system in China is also under construction.

According to the goal of information security system in China, the design and implementation of information network security is comprehensively considered from the perspective of personnel, technology, management, legislation and operation. We have put forward the international safety standards and national security law as a guide, the use of information system security engineering method, through rigorous management, adequate funding, strong talent support, strong technical guarantee, establish and improve the network security plan and disaster recovery plan. Based on the principle of "people first", we should achieve the goal of achieving all levels of safety assurance from border security to host safety, and strive to reduce the security threat to an acceptable level and effectively control risks. In the event of an invasion and other disasters, a full range of security strategic objectives with powerful recovery and counterattack capabilities are achieved.

II. NETWORK SECURITY PLAN

A. *Objectives of the Security Plan*

According to the relevant national laws and regulations, as well as the strategic objectives of the information network security system, the network security plan is formulated. The aim is to strengthen the security of network security and establish a relatively safe information network environment. Through the effective implementation of the plan, the following four major goals are achieved:

1) Establish a solid technical basis. We should educate and train technical groups with strong network security capabilities, establish relevant organizations, identify and improve the responsibilities of security personnel, and defend, detect, respond and recover against possible infringed networks.

2) Detection and response. Detection and monitoring of network status should be timely. When an attack is found, it can react quickly and control the attack, and quickly restore or rebuild the normal running state of the network.

3) Defense and recovery. Establish an efficient network defense system. The protection of key infrastructure is free from network invasion and virus invasion. Reduce network vulnerability. It has strong defense and recovery capabilities for network attacks that have occurred and may occur.

4) The necessary ability to counterattack. The existing security defense capability may not be enough to achieve the desired security target for the aggressive attack. It is necessary to have the ability to fight back, to prevent or even destroy the invaders' attempt.

B. *The Main Contents of the Network Security Plan*

The security of information network issystem engineering. It not only needs solid technical support, but also is restricted by many factors, such as staffing, organization construction, management level, national legislation and so on. Therefore, it is necessary to formulate

a feasible and efficient network security plan according to the objective of the all-round network security strategy. We should reasonably allocate all kinds of resources and coordinate the relations in all aspects.

The plan mainly includes eight points:

1) To establish an active defense system. Identify key infrastructure and interdependence. The software and hardware of the network system, which is the carrier of information dissemination, storage and processing in the vulnerability information network system, is an important infrastructure in the whole system. The interdependence between these facilities, especially the key infrastructure, is given full attention. It also conducts continuous vulnerability assessment and audit of the software and hardware systems used in the network. The ability of the invaders to destroy the critical infrastructure is estimated. Develop a practical scheme to repair the vulnerability of the system and constantly modify and update the scheme.

The evaluation and audit work will effectively destroy the invaders' attempt, which is bound to be the target of the invaders to carry out the attack. Therefore, enough attention should be given to the safety of the assessment and audit work itself.

2) Detection of attacks and illegal intrusion, and pay attention to the collection of network security information.

Acknowledgement and correction of vulnerability can delay but not completely prevent malicious intrusion to the information network system. Therefore, we need to carry out active defense at all levels of information network system, install and configure intrusion detection system, vulnerability scanning system, emergency response system and so on. The network management department should always pay attention to the collection of network security information, help the end users to resist attacks and prevent virus invasion. Establish security management organization according to the network operation situation.

a) Safety management group. The Group monitors and manages the entire network system and coordinates the work of the group and other groups. When attacked, the system is resumed with the other groups.

b) Emergency response team. Responsible for security technology research and development, providing expert help to other groups to help them isolate, control, and resolve intrusion and attacks. In the case of attack, it is able to respond quickly and provide solutions.

c) Intrusion detection team. It is responsible for uninterrupted network security detection, and to collect security information legally, and provide security information for other groups at any time. The system backup work is done in collaboration with the operation Department to support the recovery work after the attack.

3) Improve fast response and resilience

Response and recovery plans are formulated in each key infrastructure and key information of each category in the system. In the case of attack, it can be controlled in time, at least to ensure the minimum operation of the network, so that the work of other departments is less affected.

When an attack occurs, the response is as follows:

a) The rapid control of the intruders and blocking the access to the system.

b) Other more stringent defense measures are quickly launched.

c) Close the non-critical operating system.

d) To enable the redundant takeover system in an emergency, and so on.

After blocking the invasion, it is necessary to quickly restore or rebuild the system that is attacked or infected, and should have the corresponding recovery capability for different attacks.

a) Physical recovery, set up spare equipment, and dredge the network as soon as possible.

b) The soft and hardware loopholes in the repair system.

c) Repair or replace damaged soft and hardware resources.

d) Recover the damaged data from the backup database as soon as possible.

e) When the time and technical conditions are allowed, the intrusion information is analyzed and the source of invasion is traced. If necessary, information is provided to the public security organs.

4) Prioritization of key facilities and information, and level management.

Prioritize key facilities and information. The more sensitive information and the facilities that have a great impact on the operation, the more valuable it is. At the same time, they are more likely to encounter risks. Therefore, we need to take more secure measures for facilities and information with high priority, so that intruders can't encroach on critical facilities and obtain confidential information in a general way. Even if you get it, you can't parse the actual meaning of the information.

5) Pay attention to the collection and exchange of information, consistent with national law

In order to ensure the security of the network, it is necessary to establish a reliable, unimpeded and special communication channel. Establish a unified safety standard. The network management department should work closely with other departments to share security information and strengthen the research and development of security related technologies.

6) Pay attention to the training and employment of talents and strengthen the construction of institutions

Invite some information security experts to carry out continuous safety training for the existing network managers, actively hire and educate other personnel to make up for the lack of safety talents.

In addition, we have to establish a team of part-time security administrators.

7) Strengthen the construction of the system and improve the management level

Under the guidance of national law, the current regulations and regulations are constantly revised and perfected. It provides a legal framework for the security of information network, and constantly improves the management level.

8) Strengthen the safety education for all kinds of personnel so as to make the public understand the necessity of improving the network security.

Improve the public awareness of network security, enhance the threat to the information system and their understanding and understanding of their characteristics. Improve the ability of our defended invaders to attack before the disastrous events come

III. CONCLUSION

At present, the problem of network security has become a serious form that affects the national security and social stability. The implementation of network security plan has shown profound practical significance. In the long process of security assurance, the network security plan is just the first step, but we can be sure that the problem of network security will also receive more and more attention.

REFERENCE

[1] Gu Huaxiang. The legal measures and Enlightenment for the security of information security abroad [J]. Reform of administrative managemen.2010(12):70-74.

[2] Ma Minhu. Internet security law[M]. Xi'an Jiao Tong University press.2003.

[3] Zhang Lei. Development of computer information network technology [J]. computer knowledge and technology. 2014 (03):482-484.

[4] Wei Suming. Discussion on the computer information network security technology and security measures [J]. Electronics World. 2017 (03):20-21.