Research on Computer Network Security Emergency Response Systematization

Xue Yang and Ai’nan Zhu

People's Public Security University of China, Beijing, 100038, China

Abstract. with the acceleration of information process, computer information system and network has become an important social infrastructure. Based on the study of the basic theory, technology and application of computer network security emergency response, this paper focuses on the relevant strategies to guide the establishment of effective computer network security emergency response mechanism, analyzes the strategy composition, function object and action process of the system framework, and designs the framework of computer network security emergency response strategy system.

Key words. Computer network security; Network events; Emergency response

1. Introduction

1.1. Emergency Response concept
The beginning of emergency response is due to the occurrence of "incidents". The so-called "incidents" or security incidents refer to those improper behaviors that affect the security of computer systems and networks. The loss caused by network security incidents is often huge, and often in a very short period of time. Therefore, the key to deal with network events is speed and efficiency. The content of emergency response technology in "event" includes event classification, event description and event report.[1]

1.2. Objects of emergency response
In this paper, the object of emergency response to network security incidents refers to all security events of information processed by computer and network. The subject of the event may come from nature, human, fault or virus and worm. In addition to the traditional classification of confidentiality, integrity and availability, the objects of emergency response also include scanning and other security violations, which are also called emergency response objects. Generally, there are at least three roles in the process of emergency response: the initiator, the victim and the personnel. We call them "intruders," "victims," and "responders."[2]

2. Computer network security incident emergency response strategy system

2.1. Design principles of emergency response strategy system
The process of strategy formulation is a gradual and continuous improvement process, because it is impossible to formulate a strategy that can fully meet and adapt to the environment and needs of the network system, and can only constantly approach the goal. The design of emergency response strategy system should follow the following principles:
(1) Guiding principle: the strategy in the emergency response strategy system is not a technical solution. It should be a guiding document describing the methods of dealing with network security...
incidents, providing overall guidance for the emergency response work of the whole organization.

(2) According to the principle of integrity, the strategy of emergency response must be comprehensive prevention within the whole network. The overall transportation, any negligence of any link may lead to the vulnerability of the whole emergency response system. The design of the whole emergency response strategy system must take into account both management and technology. At the same time, when formulating the management strategy, we must take into account the response ability that the technology can achieve, and invest enough energy in the management.

(3) Dynamic principle, the complexity of security incidents makes it impossible to achieve perfection in the formulation of specific emergency response strategies. The strategies formulated always focus on the current situation, while information security is dynamic, and information security strategies need to be continuously developed. Therefore, we must constantly improve the strategies, that is, we must implement the idea of security life cycle.

2.2. Framework of emergency response strategy system

According to the design principles of emergency response strategy and the actual characteristics of the current computer network, the framework of the emergency response strategy system for computer network security incidents designed in this paper is shown in Figure 1.

![Figure 1. Framework of emergency response strategy for computer network security incidents.](image)

(1) Integrated emergency response management strategy. The strategy is mainly used to provide guidance for the establishment of response organizations at all levels in the integrated construction of network security emergency response system. It mainly includes: according to the current administrative system structure of each department of the unit, the establishment method of network security emergency response organization is provided; the geographical distribution characteristics and security requirements of the unit are studied; and the information sharing strategy is formulated to facilitate the implementation of integrated emergency response.

(2) Prepare strategy in advance. The strategy is used to guide the emergency response staff to make necessary preparations for various network security incidents that may occur in the future. It mainly includes: making correct risk assessment on the network information system of the Department, determining the important information resources in the network, and regularly organizing relevant
personnel to carry out the simulation exercise of emergency response. 

(3) Response strategy. This strategy is the key of emergency response, which is mainly used to provide guidance for how to solve the problems in the process of emergency response: how to detect whether there is a security event; how to limit the scope of attack; how to restore all the broken systems and network devices to normal task state as far as possible.

(4) Summarize the adjustment strategy. The strategy is mainly used to guide the work after the security incident processing, including reviewing and sorting out the various relevant information of the network security incident and summarizing the steps of the report, as well as the management scheme of event documents and evidence.

(5) Emergency response service support strategy. The strategy is mainly used to guide how to provide the necessary service guarantee for the implementation of the above strategies, including system maintenance, personnel training, technical consultation, technical research and development, safety announcement and legal support.

2.3. **Objects of emergency response strategy**

In this paper, in the strategy system designed according to the characteristics of various information networks, each component element plays a different role in the process of network security emergency response, and has different action objects, as shown in Figure 2.

![Figure 2. Strategy objects.](image)

First of all, the emergency response preparation strategy, response strategy and summary strategy are implemented in sequence according to the time sequence. The implementation of the preparation strategy before the security incident is the premise and foundation of the response strategy. The adequacy of the implementation of the preparation strategy will directly affect the effectiveness of the implementation of the response strategy; The in event response strategy plays an important role in dealing with network security incidents. It is the core of the whole emergency response strategy system. [3] It is not only the continuation of the preparation strategy, but also the description object of the summary strategy. After the event summary strategy acts on the security incident, it is the information transmission link between the preparation strategy and the response strategy. After the event summary strategy can feed back the defects of the emergency response strategy to the preparation strategy, which makes the three form a closed cycle.

Secondly, the emergency response support strategy plays an important role in the whole process of the implementation of the above strategies, providing service guarantee for the implementation of the strategy. Formulating a comprehensive support strategy can effectively guarantee the emergency
response work. It is a key factor for the smooth implementation of the above strategies and an important auxiliary strategy for the above strategies. Finally, the integrated management strategy acts on different emergency response centers, which is a horizontal information channel widely shared by the same type of strategies formulated by different emergency centers. On the one hand, it restricts the formulation of the above strategies to meet the needs of integrated management; on the other hand, it can promote the continuous improvement of the above strategies.

3. Analysis on the function process of system framework

Each component element of the emergency response strategy system has relatively independent functions and clear scope or object of action. The policies form a relationship of mutual dependence and promotion, and jointly serve the emergency response processing of network security. The process of network security emergency treatment is shown in Figure 3.

![Strategy process diagram](image)

**Figure 3. Strategy process**

Before the occurrence of network security incidents, emergency response personnel actively implement the preparation work of emergency response processing. This stage belongs to the preparation stage, and the preparation work is guided by the pre-preparation strategy. The network that has implemented the preparation strategy should have the ability of intrusion detection of network security events, and monitor the network security situation at any time. When the security incident occurs, the abnormal situation of the system is usually first detected by the network security management personnel and network terminal users.

The emergency treatment enters the detection and analysis stage, and the handling process of this stage is guided by the incident response strategy. When network operators find suspicious situations, they should first make an assessment to determine whether it is a security event. If it is determined that it is a security event or the cause of an uncertain event, it shall report the situation to the network security emergency response center of the Department in a timely manner. The internal emergency response center conducts a second assessment according to the actual situation. When it is determined as a network security incident, it will take necessary measures to deal with it immediately through authentication analysis and communication, according to the emergency response plan in the pre-preparation stage.

After the security incident is handled, the necessary summary of the emergency treatment work is made. At this time, the emergency response processing enters the post event summary adjustment stage. The work in this stage should be carried out according to the post event summary adjustment strategy. Through careful summary, we can find the defects in the emergency treatment work, and timely adjust the preparation and in-process response strategy.
emergency response, necessary service support work is needed, which is completed under the
guidance of emergency response service support strategy.

4. Conclusion
Due to natural, technical and human factors, network vulnerabilities are inevitable, and network
information security incidents are inevitable. Emergency response is the last line of defense in the
system of active defense and defense in depth, and is the necessary means and measures to ensure the
survivability of network information. The construction of emergency response system is a complex
system engineering. The life of emergency response system lies in the linkage of various safety
measures. Therefore, it is necessary to fully understand its hierarchical structure, and then to clarify
the main problems to be solved. The emergency response system is very complex and huge. In this
paper, the framework of computer network security emergency response strategy system is designed,
but the deep structure of the main body and functional entity is insufficient, which needs to be
improved.

References
[1] Xiang W. Research on hierarchical structure and linkage of network and information security
emergency response system[J]. Network security technology and application, 2015 (05): 177 +
179.
[2] Hailong L. Discussion on network security emergency response mechanism in Colleges and
universities[J]. Industry and Technology Forum,2020,19(15):277-278.
[3] Daoli H, Hao Y. Legal protection of network security emergency response of China's key
information infrastructure[J]. China information security, 2020 (03): 42-43.
[4] Yuanyuan D. Research on network security incident emergency response linkage system[J].
Wireless Internet technology, 2017 (09): 47-48.
[5] Feng L. Network security situation awareness and emergency response platform solution[J].
Information technology and standardization, 2018 (09): 16-18.
[6] Jinsheng C, Xia D, Liu Ming, Youli L. Research on emergency response strategy system of
network security incidents[J]. Computer application and software, 2009,26 (07): 274-277.