Discussion and Planning Design on the Defense Implementation System of Information Security

Haitao Lv
(Harbin University of Finance, Harbin, Heilongjiang 150030)
hrbjrxy@163.com

Keywords: Security defense; Emergency plans; Linkage technology

Abstract. The importance of information security in the construction of the network information system has become increasingly prominent. The defense implementation system based on the information security is a set of comprehensive, Multi-level integrated information security detection and control equipment, The design can meet the safety management needs of different users, Can help internet users monitor customer network security during the entire life cycle in threat, And effectively control safety risk in the form of emergency plans.

Introduction

With the increasingly severe cyberspace security situation, cyberspace security is not only a hacker attack alone, but gradually transformed into a clear hacker industry chain with a clear division of labor. It has risen to the APT attack mode of national behavior. The victims of cyber attacks emerge in an endless stream. Power outages in Ukraine, damage to Iran's nuclear facilities and extortion of the virus are all examples of cyber security issues. Cyberspace Security is related to the national economy and the people's livelihood, and is related to every aspect of life. The problem of network security has become a major problem related to the security and development of the country and the vital interests of people. President Xi made it clear that "there is no national security without cyber security", which elevates China's cyber security to national security and national strategy".

Status of the Defense System of Information Security

In the field of information security, information security and defense system in various industries are constrained by the technical bottlenecks in the field and and not really implemented. The emergency plan of original information security only stays on the "process design" level, and the emergency plan emphasizes the command and process procedure, and it is not touched at the core technology operation level. When there is a sudden security threat in the network, the discovery of the problem, the analysis of the failure, and the final configuration adjustment can only depend on the manual processing, and the efficiency is difficult to guarantee. (The progress of the problem depends on the technical level, responsiveness and timeliness of the operational staff). How to deal with a sudden security attack? What is the problem and how to deal with the emergency plan at the technical level? This is the most important problem to be solved at present.

Risks and Challenges of Information Security

At present, the risks and challenges of enterprises in the construction of information security are mainly reflected in the following aspects.

The Disadvantages of the Static Security Defense System. No matter how high the standard of network construction is, there will still be a variety of security problems. The source of the problem is mainly due to the following contradictions. On one hand, the risk of information security is "dynamic", and every day there are new virus variants, holes, or new attacks. On the other hand, the defense system of information system is static. For example, the policy rules of the firewall are static, and even if the host is turned into an attack host after the policy has been released, the policy will still be valid and the attack will be released.

The Disadvantages Based On the Concept of Security Domain Boundary Protection. The boundary protection based on "security domain" is the most classic and effective design concept of security defense, which plays an indispensable role in the construction of enterprise's overall security system. But there are unavoidable drawbacks in the protection design of security domain isolation. Security domain protection is only partial defense. Enterprises invested a lot of resources to centrally deploy information security products in the front end of data center, so as to protect the safety of data center. Such a deployment can only guarantee local security in this area of the data center. The most extensive user area in the enterprise network is completely out of control because the user area is connected by the basic network elements such as switches, routers, etc. these devices do not have the security protection function. From a global perspective of "business availability", even if the data center is safe, business is still inaccessible if the user area is not available.

Lack of Accurate Perception And Verification of Threats. The traditional of the defense system framework of network security includes access control, security isolation, border detection / defense, terminal defense, network audit, access control, and so on. The security products involved include: firewall, ids/ips, anti-virus software, desktop management software, network audit and so on. These products are all over the 2nd to seventh layer of the network, and have the data analysis ability from the network layer to the application layer, but still cannot effectively guarantee the network security of the information system.

Demand Analysis of The Defense Implementation System of Information Security

The defense implementation system of information security should be a set of comprehensive, multi-level integrated information security detection and control equipment. The design can meet the needs of different users' safety management, help internet users to monitor the safety status of customers' network during the entire life cycle in threat and effectively control the security risk in the form of emergency plans. Through the deployment of the emergency plan implementation system of information security, the discovery of "the question, the analysis of the problems, and the final problem" link will no longer rely on manual operation. All contingency responses will be automatically disposed according to preset planned tasks.

The Three Phases The Defense Implementation System of Information Security Concerns. At present, all industries have set up an emergency plan that meets its own business characteristics and can be technically implemented. The emergency plan to be short is what kind of problem, what kind of planned task we follow, and we have a targeted solution. To summarize the emergency plan of various industries, the basic concerns include three stages: situational awareness -- emergency plan -- emergency disposal. The emergency plan for information security also requires that real technology be achieved at these three stages

The Perception Technology of Network Defense System. The accurate discovery of the threat information is the prerequisite for the correct implementation of the emergency plan. Therefore, the design of network threat monitoring system (goodlan-tmc) should be a network security situational awareness device that integrates virus scanning, intrusion detection and network monitoring. It can capture all the data transmitted between the networks in real time, and use the built-in threat repository and threat detection engine to detect the virus invasion on the network effectively, and the the behavior and anomaly that violate the security policy by using pattern matching and statistical analysis. The main technical features of the network threat monitoring system at the situational awareness level of the threat are as follows:

There should be a million-level threat feature library to effectively identify known threats. Network threat monitoring system should be an independent hardware deployed by bypass. It has a million level threat feature library. It can accurately identify the known threats through feature comparison. The network threat monitoring system can form isomerism with the host antivirus system that has been deployed in the user network environment, effectively expand the coverage of the virus characteristic library and reduce the occurrence of missing report.

Providing a virtual machine shelling engine to efficiently identify unknown threats. Network threat monitoring system should have advanced virtual machine shelling engine, and virtual machine shelling engine can release its attack behavior through constructing a virtual simulation environmental decoy virus for a virus file(For example, a pure virtual environment is built by simulating the CPU instruction system, the memory management system, the operating system, the API calling system, and so on. Network threat monitoring systems run viruses in a virtual environment and monitor the behavior of the virus(For example, what harmful API is invoked by a virus, what registry key values are modified, what files are created, and so on). Thus, the unknown virus can be effectively determined.

A third party log is used to conduct association analysis to implement the consultation mechanism. Listen to both sides and you will be enlightened, heed only one side and you will be benighted. It is impossible for any security product design to solve all security problems. Due to the limitations of the technology of a single product it is unavoidable to have a certain missing report and misreport.

The network threat monitoring system is equipped with two core technologies: virtual machine shelling engine and intelligent threat analysis engine. The intelligent threat analysis engine can not only use the built-in threat information library and threat detection engine to determine the threat information, but also receive the security logs of the third party devices at the same time. Through the big data mining and AI analysis technology, we analyze the collected threat data and achieve the joint consultation of threat intelligence, so as to effectively solve the problem of missing report and misreport of a single product.

Design of Emergency Plan of Network Defense System

The design of emergency plan task is a core function of information security defense system. The business of each enterprise is different, different network topology, equipment brand and function deployment is different, so the task of emergency plan set must be combined with their own situation for completion.

Under a large number of uncertain factors, how to plan the information security emergency plan of the enterprise so that it can be truly implemented on the ground. By summarizing the emergency plan in various industries, combining with the characteristics of information system, the feasible technical route is designed. Its core practice pays attention to the classification of 3 aspects and the application of emergency linkage technology:

Classification of Threat. The plan and task of emergency plan should first classify the destruction mode and danger level of threat information, and take different emergency handling methods according to different attack categories and danger level. According to the knowledge base of threat information, the classification of the species and the classification of danger levels were carried out on the samples of the nearly one million threats. For example, threat categories include worms, Trojan horses, back doors, viruses, spam, malware, hacker tools, etc. Network managers can design targeted contingency plans by simply considering the category of "threat attacks" and "the level of danger". How to deal with the high-risk Trojan? What about intermediate spam?

Operational Classification. Because of the different importance of business systems in the enterprise, tolerance based on threats is also different.（For example, the security of the financial system is higher than the business stability, and the business stability of the OA system is higher than the security.）As a result, the emergency measures taken when the systems are attacked are different. Therefore, when network managers consider such issues as "how to deal with high-risk Trojan horses," a premise should be set up to take account of the business concerns on the ones which are attacked.

Functional Classification. After classifying threats and business situations, the next thing to do is to respond to the threat substantially, i.e. emergency disposal. The emergency disposal should combine the original network environment of the enterprise, classify the original product functions in advance, and fully call the functions of the products deployed in the network.

For blocking functions, when considering all data sources that cut off attacks against high-risk threats, the firewall's blocking policy function and the ACL control list of switchboards can be invoked.

In terms of the control function: for operational stability is highly demanded or When judging an inaccurate and suspected threat to the host for emergency response, strong filtering and blocking can lead to misoperation, not even the result we expect. A more reasonable way is to limit the suspected dangerous host to a certain "pipe". At this time, the traffic management device in the invocable network can carry out traffic control, and invoke devices with conversational control capabilities to carry out session control.

Emergency Linkage Technique. The emergency disposal function is mainly realized by the emergency linkage platform which reflects the unique technical value in the overall solution. The platform of emergency response connects and integrates functional attributes among different products, and each device is no longer isolated. Functions can be called between different products according to results oriented design ideas(For example, the problem found by A is solved by B). The emergency linkage platform, with multi brand linkage as its core, can widely support the mainstream products in the industry.

Conclusion

The rapid development of network attack technology has brought great pressure to network information security. Single protective measures have been powerless,and a thorough and in-depth protection of the network is required to effectively ensure network security. The deep protection system can not only detect malicious code, but also prevent malicious code from attacking. In the current age of mixed threats, deploying the defense implementation system ofinformation security can effectively meet the security management needs of different enterprises, help enterprises monitor the overall network security situation during the entire life cycle in threat, and effectively control security risk in the form of emergency plans.

References

[1] Yi,X. 2016. The exploration and practice of the stereoscopic defense system of digital campus information security. Network security technology and Application (04):145-146

[2] Weihu,T, et al 2016. Research on anti virus technology of computer active defense based on Information Security. Security of Cyberspace. 7(07):40-42.

[3] Xuedong,W. 2016.Research and design of information security active defense system of "Internet +" age. Security of Cyberspace. 7(06):5-6+13.

[4] Dan,L ,2016. Research on the architecture and application of information security technology based on depth defense. Journal of chongqing electronic engineering vocational college 25(03):147-150.

[5] Yanli,C,2010. New technology in the field of network information security protection: intrusion prevention system. Radio and Television. (05):63-65.

[6] Liang,D and Lei,Z, 2010. Research on the construction planning of the depth defense system of information security. Electric power information. 8(01):41-43.

[7] Yonghong,W, et al 2006. Discussion on defense system of network information security. Journal of the Hebei Academy of Sciences. (01):25-28.

[8] Xuejing,Y and Cui,W,2005. Design of enterprise security defense system based on information security technology. Modern Information. (01):209-210.

[9]Qianlin,Z, et al 2007. Design and application Based on a policy-driven linkage platform. Computer Engineering (02):283-285.

[10]Yibo,Z et al 2017. Demand analysis and planning design of information security active defense warning platform. Security of Cyberspace. 8(Z4):94-97.