Research on the active defense security system based on cloud computing of wisdom campus network

Yuanyuan Chen [1], Wang Yao[2]， Jianghua Luo[3]

1. Information Center of Chongqing University of Technology, Chongqing 400054, China

E-mail: cyy@cqut.edu.cn

2. State power grid maintenance branch of Chongqing electric power company, Chongqing 400039, China

E-mail: wangyao@cq.sgcc.com.cn

3. Information Center of Chongqing University of Posts and Telecommunications, Chongqing 400065, china

E-mail: luojh@cqupt.edu.cn

Abstract: With the popularization of office automation in campus network, the campus network has been threatened more and more. The traditional passive defense system has been difficult to adapt to the current large-scale, complex and covert attack behavior, active defense came into being. Based on WPDRRC model, this paper proposes a new active defense model based on cloud computing. Combining with the existing security technology, in view of wisdom campus network security problems the topology of the active defense system is designed and implemented. Through the assessment, the model has the active defense function, can effectively reduce the system vulnerabilities and hacker attacks.

Key Words: Wisdom Campus, Network Security Model, Active Defense, cloud computing, Firewall, Intrusion Detection System (IDS)

1 INTRODUCTION

With triple play and the continuous development of physical networking technology, cyberspace security has become the fifth national sovereignty after land, sea, air and space. However, as the campus network increasingly depends on information technology, security issues have become increasingly prominent. The means of attack by hacker are also more advanced, hidden. The traditional security technology, such as firewall, intrusion detection, anti-virus and other single point defense equipment, can only deal with the network invasion alone, lack of cooperation between each other, in response to large-scale, changeable, multi-dimensional collaborative attack. The protection is powerless. This requires computer network security protection from passive defense to active defense. Active defense mechanism is in the process of dynamic operation, to monitor the network information, to take the initiative to intercept of intrusion and attack traffic, can contain and transfer the hacker attacks, intelligently analyze the hacker intrusion technology to trace the intruder forensics, and even before the attacks happened to defend. Therefore, in the campus network, how to design the active defense system model, how to deploy a large number of various types of security equipment, how the joint work to form a dynamic, multi-level three-dimensional defense system, which is the key problem to ensure the wisdom Campus[1] network security. The design of the model is very important.

2 DEVELOPMENT OF SECURITY MODEL

2.1 Comparison of Existing Models

Security model is built to protect data and network resource, the simplest security model is the PDR model. It consists of three parts: Protection, Detection and Response. Set up a provable security model based on time, and define as: protection time Pt, detection time Dt

and response time Rt, when the Pt > Dt + Rt that system safety.

PPDR model (also called P2DR) increase policy in the middle of the ring of PDR components, namely the PPDR cycle is under the control of the policy works, forming a complete and closed loop dynamic adaptive security system. PPDR model is the representative of dynamic network security model. The success of this model depends on the correct setting of the system and perfect defense method, and to a great extent, only for a specific threats and environment, it ignores the initiative of cyber security.

Based on PPDR, a dynamic network security model P2DR2C is proposed, which is based on closed-loop control and active defense, Added Restore function, after the system is invaded, can take the corresponding measures to restore the system to normal state. P2DR2C can effectively enhance the system's initiative, adaptability and survivability, ensure network comprehensive security.

MPDRR model is developed on the basis of PDRR model, which absorbs the advantages of PDRR model, and joined the management factor so as to integrate technology and management. The establishment of the entire security system must be unified coordination and implementation of security management.

WPDRRC [2] in the PDRR model before and after strengthen the function of warning and counterattack. The WPDRRC model has 6 links and 3 key elements. 6 links including early warning, protection, detection, response, restore and counterattack, they have strong scheduling and dynamic, and enhance the security mechanism of network system. 3 key elements include personnel, policy and technology. People is the core, policy is the bridge, technology is safeguard. The comparison of the security protection function between WPDRRC information security model and other models is shown in Table 1.

Table1. Comparison of security protection function

	Warning	Protection	Detection	Response	Restore	Counterattack	Management
PDR	×	√	√	√	×	×	×
PPDR	×	√	√	√	×	×	×
PDRR	×	√	√	√	√	×	×
MPDRR	×	√	√	√	√	×	√
WPDRRC	√	√	√	√	√	√	√

2.2 Improved Active Defense Model

Due to dynamic feedback, circulation and continuity, WPDRRC model has more advantages than others. So it gives a good idea and bedding in the research of network security protection.

Aiming at the existing problem of the above model, this paper makes a deep research on computer network security model. Optimized from two aspects of security management policy and big data analysis, on the basis of WPDRRC model put forward a new active defense model PPDFRR based on cloud computing. PPDFRR as shown in Figure 1:

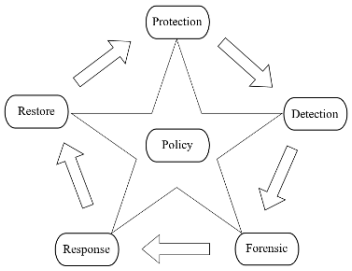

Fig 1. PPDFRR model

Model described in words as follows: network security = security policy + active defense + real-time detection + tracking forensics+ linkage response + prompt restore.

3 ACTIVE DEFENSE SECURITY SYSTEM BASED ON CLOUD COMPUTING

3.1 Cloud Active Defense Security System Architecture

A better security measure is usually the result of a variety of methods, namely the security of computer network should follow the principle of overall security. The Cloud active defense security system architecture[3] can well support the PPDFRR security model, is adapt the

development of wisdom campus network security architecture.

The other parts of the PPDFRR model form a circle around the policy, and are encrypted communication with cloud security center. Cloud security center through the detection and analysis, the first time to update the security policy, all the security protective equipment will form a linkage, defense in depth network security system. According to PPDFRR model, the building of cloud active defense security system architecture should have the following functions:

1. Before the attack, undertake security assessment to each part, timely find vulnerabilities and repair. Security policy is issued to the security protective equipment for security reinforcement, to make a regular backup of important data.

2. In attack, each part can detect the aggressive behavior. Once detect the intrusion behavior, through the router Lure into the Honeynet[4], trace evidence or through a firewall block in time, improve the system's immunity. To Unrecognized suspicious behavior, they can actively collect behavior characteristics, upload the relevant information to the cloud security center for large data analysis. According to the different methods of attack adjust security policy to achieve intelligent protective effect of real-time processing.

3. After the attack, to check the relevant log or security audit equipment, analyze vulnerabilities and attacker source, through the backup to timely restore the resources. Through honeynet technology record and restore intrusion behavior, reproduce the attack path, ensure the authenticity of electronic evidence.

According to the above analysis, the design of cloud active defense security system architecture is shown in Figure 2:

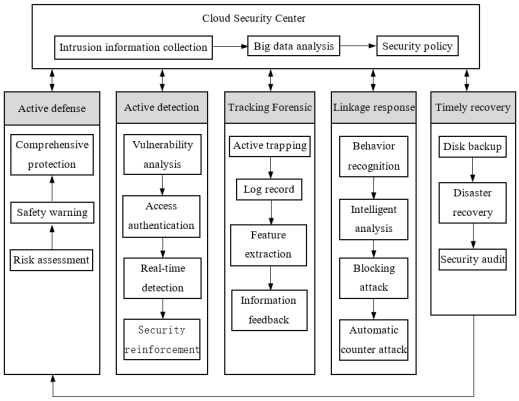

Fig2. Cloud active defense security system architecture

3.2 Policy Subsystem Flow Chart

PPDFRR model contains six parts, under the guidance of policy constitute a dynamic and complete security loop. The policy subsystem[5] is the core position in the entire PPDFRR model, is the center of the other five subsystems. To ensure network security the security measures includ firewall, intrusion detection, authentication, encryption, vulnerability evaluation. So the design of the policy subsystem is very important. The design of active defense system policy subsystem is shown in Figure 3：

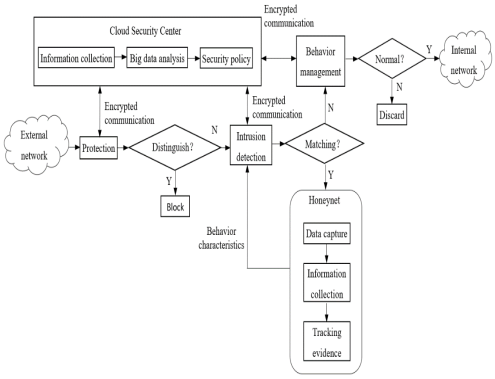

Fig 3. Policy subsystem of the cloud active defense system

Firewall is the basic facilities of campus network intrusion protection, filter attack information, when discovering attack block access. The firewall and the cloud security center real-time encryption communication, according to the security policy to deal with the intrusion behavior.

Intrusion detection system[6] can real-time detect attack behavior, and pattern matching

by feature library. If the match succeeds, intruder is lured into honeynet to capture his behavior, including: firewall logs, IDS logs and Honeynet host system log. Analysis of the behavior, understand the invader attack tools, attack tactics and intrusion motives, etc.. By recording intruder behavior, Honeynet extract behavior characteristics and feedback them to IDS. Then IDS report the information including the corresponding characteristics, traffic, protocols to the cloud security center, carry on large data analysis, optimizing security policy. Security policy issued to the firewall, intrusion detection system and the knowledge base of internet behavior management, enhance the security protection capabilities of the defense tools and detection tools. Honeynet tracks behavior to response intrusion and provide evidence of subsequent legal sanctions against the invaders.

Internet behavior management audit behavior according to the security policy generated after intrustion detecting. The audit results normal access real network otherwise discarded.

other aspects set the overall goal of wisdom campus network security:

1. To achieve the isolation and access control between different security areas or distrust domains.
2. Audit and monitor the contents of the information in and out of the campus network.
3. Equipped with network security analysis, audit monitoring and intrusion detection system.
4. Each node in the campus network uses network anti-virus system, and combined with the single antivirus software, to build a complete set of anti-virus system.
5. Strengthen security management organization and security management system, improve staff's network security awareness and prevention technology.

To achieve security goals above, build wisdom campus network cloud active defense system topology as shown in Figure 4:

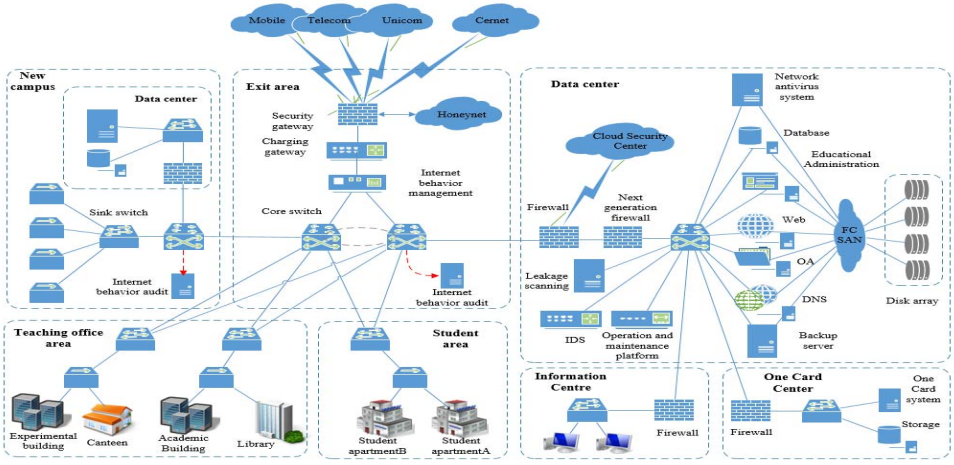

Fig 4. wisdom campus network cloud active defense system topology structure

4 CLOUD ACTIVE DEFENSE SYSTEM DEPLOYMENT

4.1 Cloud Active Defense System Topology

Considering the characteristics and technology of cloud computing, according to the actual situation of the wisdom campus, establish a new network security mechanism. From the physical environment, network, data, applications and

4.2 The Rrealization of Cloud Active Defense system

In order to realize the cloud active defense system based on PPDFRR model, need to all kinds of security products organically to form a dynamic and multi-level security defense system.

In this paper, According to the function structure of wisdom campus network can be divided into seven major areas, namely export area, teaching office area, student area, data center, new campus area, information center area and the card center.

1. In the entrance or exit of network set a security gateway, strict access control. Use VPN data encryption and authentication technology to prevent illegal users access to the network, while ensuring the information in the communication process from being tapped or tampered with. Set up a simulation of the real network environment named Honeynet, capture and study intrusion behavior. Set up network firewall at the entrance of several key areas. Deploy internet behavior management system, provide content audit, traffic monitoring, behavior filtering, alarm and other functions.

2. In the data center area deployment IDS, vulnerability scanning, anti-virus system and the next generation firewall (with WAF, IPS), which can realize centralized monitoring and alarm for malware scan, DDoS attacks, Web application attack, virus file, obtain permission class attack, network sniffer behavior etc.. Build cloud security center, in addition to judge malicious behaviors, also carry out big data analysis of the abnormal logs uploaded by all terminals or boundary equipment, formulate and optimize security policy, real-time distribute to security equipment. Security operation and maintenance personnel can complete the monitoring, analysis, diagnosis work of threat through the operation and maintenance platform.

3. To control the behavior of students, deploy Internet behavior audit in core switch of student area, strengthen the management of internal violations.

4. For the realization of disaster recovery[7], establish Storage Area Network(FC SAN) in the data center to realize virtual server backup.

5. Access remote security assessment system to achieve centrally monitor, manage system vulnerabilities and weak password configuration including Windows host, Unix/Linux server, DNS server.

5 CLOUD ACTIVE DEFENSE SYSTEM EVALUATION

Using remote security evaluation system to real-time monitor the operation status of the wisdom campus network information system, obtain the vulnerability assessment[8] of the various network server and application information system. According to the severity of the consequences of the vulnerability, divide the vulnerability into three categories. Before and after the implementation of the cloud active defense system, conduct vulnerability assessment of services and applications provided by the wisdom campus network, the results are shown in Table 2 and Table 3.

Table 2. Vulnerability assessment results before the implementation

Service	High risk	Medium risk	Low risk	Total
www	25	76	10	111
FTP	1	2	1	4
SNMP	1	0	5	6
Apache	0	15	3	18
PHP	23	48	3	74
Database	8	23	8	39

Table 3. Vulnerability assessment results after the implementation

Service	High risk	Medium risk	Low risk	Total
www	10	36	2	48
FTP	0	0	1	1
SNMP	0	0	2	2
Apache	0	6	2	8
PHP	9	22	1	32
Database	3	8	3	14

Compare the two results of vulnerability assessmention before and after the cloud active defense system to be implemented in a histogram as shown in figure 5.

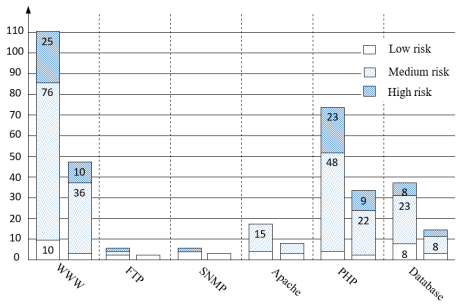

Fig 5. Vulnerability assessment situation comparison

Can be seen before the deployment of cloud active defense system, the campus network's various information systems have different degree of vulnerability, which constitute a great threat to network security, is vulnerable to cyber attacks. After implementing cloud active defense system, the vulnerabilities of software and hardware, operating system and application system are repaired, through cloud security center's security policy to reinforce protection, information system security level was improved obviously.

6 CONCLUSION

Aiming at the existence security problem of wisdom campus network, this paper propose an active defense security model PPDFRR based on cloud computing, combine firewall technology, intrusion detection technology and honeynet technology, study the overall network security. Evaluation result shows that the model can reduce network vulnerability, actively respond to cyber attacks, But the cloud active defense system used in the campus network is still not popular, intrusion detection technology is not mature enough, vulnerability assessment has a large number of false negatives and false positives , the ability of automatic response to security threats is lack, the linkage of the various security devices is not good enough. Therefore, wisdom campus network cloud active defense technology also need continue in-depth study, ensure the equipment, technology, management and so on various aspects factor mutually coordinate, make the real form an organic system.

REFERENCES

[1] Wang Yan, Overall architecture model and typical application analysis of the construction of the wisdom Campus, China Audio Visual Education, No.332, Sep. 2014

[2] Chunhui Yang,Chenghua Yan, Research on the security model of network space, Information Technology, 1009-2552(2015) 04-0075-05

[3] WangBo，Research on cloud computing security system architecture of wisdom campus network, Journal of xinyu university, Vol.17,No.5,Oct.2010

[4] Hongjing Zhao, Chuangming Zhou, Pingli Zhai, Intrusion Deception System Based on network active defense security model, Journal of Air Force Engineering University (NATURAL SCIENCE EDITION), Vol.11, No.3, Jun .2010

[5] Fangyong Tan, Fusheng Yu, The Deployment of the Active Defense System Based on Campus Network, Computer Knowledge and Technology, Vol.6,No.1,January 2010

[6] Changyi Wang, Zhuo Zhang, and Xianhua Song, Research on the Information Security Technology of University Campus Network, D. Jin and S. Lin (Eds.): Advances in CSIE, Vol. 2, AISC 169, pp. 217–221.springerlink.com © Springer-Verlag Berlin Heidelberg 2012

[7] Xingang Zhang, Baoping Wang. Analysis of campus network security emergency response linkage system [C] Proceedings of 2010 International Conference on Information Technology and Industrial Engineering: World Academic Press, 2010: 1016-1020.

[8] Xingang Zhang, Wang yan. Analysis of Active Defense System on Digital Campus, Research and Exploration in Laboratory, Vol.31,No.1, Jan.2012