Brief Introduction of Network Security Asset Management for Banks

Yumo Wang^(✉) and Qinghua Zhang

China Everbright Bank CO., Ltd, Beijing 100034, China
wangyumo@cebbank.com

Abstract. During the digital development process, enterprises have accumulated a lot of network asset including hardware, software and websites. Effective management of network asset can reduce the internet risk. Network asset is the primary object of information security. Therefore, the essential content of enterprise information security operation is ensuring the security of network assets sufficiently. This paper has investigated researches about detection, management and applications of network assets. The difficulty and current solutions have been summarized by the review. Moreover, this paper puts forward a solution of network asset management according to the bank situation.

Keywords: Network asset · Host detection · Security management

1 Introduction

With the development of technologies in information security, the demand of management of network assets is increasing in banks. During the digital construction of banks, many network assets have been accumulated including domain name, IP, system, application and so on. The network assets are the main object of information security management in banks. The purpose of managing security assets is to support the information security operation of banks, so it is essential to collect and analyze the security information of network assets. This paper conducts the research on network asset management from three aspects: detection, management and applications. A construction method of security network assets management for bank is proposed (Fig. 1).

According to the controllability of assets, the network security assets of banks are usually divided into two parts: internet and intranet. From the perspective of safety management, both of internet and intranet assets are protection objects that need to be focused on. In the management of network security assets, there are generally three aspects: detection, management and application. Detection means to discovery the security assets in cyberspace. Effective management of assets can only be achieved by timely and accurately detection. At the same time, the method of detection and monitoring are similar. Periodic updating of asset information is also an important part of safe asset management. Management means to clearly counting the proven safety assets, accumulating the detection results, so as to form an asset library that can support information security operation and provide data support for the further development of security works. The

Fig. 1. Network asset management process

most important part of asset management is conducting two aspects of constructions: information and regulation. Application means using the managed network security asset data in multiple dimensions in order to embody value of it. The most typical application scenario is active risk discovery. The ability of active risk discovery for security assets can make security operation more accurate and targeted.

In view of the previous three aspects of network security asset management design, this paper conducts a literature review.

2 Detection of Network Security Assets

Detection is the starting point of network security asset management. At present, there are three common asset detection methods: active, passive and information hunting based on search engine. With the help of network scanning tools, the active way can obtain information by scanning the host, which has strong pertinence, but it will occupy part of the resources of the target host. The passive way means to the aggregation of transaction information through the carding of network traffic, which an important method in the asset discovery of intranet. Information hunting based on search engine is a non-invasive asset detection method, which can expand the collection field. However, it also depends on the data collection ability of the searching platform [1]. The detection work needs to consider different levels of assets. For the IaaS level, it mainly relies on scanners, network detection, NAT mapping table and other methods to detect network security assets. For PaaS and SaaS level, methods like traffic carding, DNS domain name aggregation are used to gather asset application information [2]. Through the acquisition of network fingerprints, the details of assets can be collected in order to identify website components, application services, communication protocols, which is able to assist the identification of vulnerabilities [3]. The design of active scanning scanner for IP requires different port scanning of TCP and UDP protocols to obtain more comprehensive host information [4, 5]. There are four scanning methods for asset discovery: ICMP, TCP connect, TCP SYN and TCP FIN. In practice, these methods are usually combined to obtain more accurate asset opening information [6]. The complex and changeable asset information needs to be monitored dynamically, and the comprehensive information including multiple dimensions as host, system, internal information should be gathered [7]. In the complex network environment, big data technology can support the asset discovery process and provide technical means for the excavation of massive information [8]. At the same time, vulnerability is also a key information in asset scanning. Periodically vulnerability

mining is very important for banks [9]. In order to discovery vulnerability efficiently, automatic tools like Nmap, Xscan, Goby, Nessus are needed to discover the assets and vulnerabilities [10, 11].

3 Management of Network Security Assets

Management is the core content of network security asset management. The method of network security asset management can be divided into two aspects: technology construction and regulation construction. Empirically regulation is more important than technology in network asset management. At present, there are many problems in network security asset management, including insufficient handover, lack of sharing mechanism between different systems, untimely updating, and lack of evaluation process [12]. Though, it is very important for banks to overcome many obstacles in asset management, the management work should be appropriate considering the current situation of banks [13]. Technology construction is an indispensable method for the current network security asset management, which makes the assets fine management and strengthens the achievements of regulation construction [14]. Cloud platform is able to make the deployment of network asset management system more efficient and enable the dynamic monitoring update of asset information [15]. The integrated asset management platform usually includes account management, IP address information, resource check, electronic reminder, baseline verification, vulnerability scanning and other functions to achieve comprehensive technical function support [16, 17]. The management of network security assets needs to cover the whole life cycle of assets. The detection and monitoring needs to contain several processes like asset addition, allocation, change and invalidation. Network security assets need dynamic management, especially focusing on the changes of assets in its whole life cycle. In particular, it is necessary to check and recover the assets in time when it is out of use [18, 19]. The asset information management system based on block-chain technology makes the asset information more complete and consistent. The unchangeable characteristic of block-chain makes the asset data management process more reliable and controllable [20]. The management of network security asset data also requires multi-source fusion technology to integrate data from different sources in order to gather comprehensive information of the asset. Based on the segmentation and vectorization of address information, the cosine similarity between feature vectors is applied to assist the automatic matching and fusion of asset information [21, 22].

4 Applications of Network Security Assets

Application for security operations reflects the true value of network security asset management. The purpose of network security assets management is to find risks actively. Situational awareness system is a very practical tool in the current information security operation whose construction progress is highly associated with asset management. To enable active risk detection, many functional parts rely on the network asset management including attack detection, software and hardware information collection, external threat information and so on [23, 24]. This kind of active risk discovery has a good effect on the security of dumb terminals. For example, asset monitoring for dumb terminals such

as video monitoring equipment can assist in detecting network intrusion [25]. Artificial intelligence is a potential technology in situation awareness in which asset data plays an important role and can provide data materials for situation awareness work [26]. Big data technology can also assist the network asset management in security operation. Big data technology provides sufficient storage and rapid searching for massive asset information data and enables multiple applications [27]. Big data technology provides an over-all support for comprehensive asset information management and risk discovery [28]. Vulnerability management also needs network asset management system. The whole processes of vulnerability management starts from discovering assets and includes classification, scanning, repair, tracking, compliance and periodically repetition. In the case of the asset management of FIFTH THIRD BANK in the United States, both management of network security assets security and level of compliance continuity should be paid attention in order to provide a more comprehensive guarantee for the business [29]. Asset lifecycle management can also make each data clear and controllable by assisting the work of data privacy protection which should cover the process generation, use and extinction [30]. Based on the analysis of the network flow, asset baseline is established in order to focus on the dynamic changes in data to guarantee the security of assets [31].

5 Design of Network Security Assets Management System

Based on the analysis of the relevant literature on network security asset management, current technologies and theories of network security asset management are isolated, which may be caused by the complexity of asset. Discrete management can be flexibly applied in small-scale and relatively monotonous information management but it is difficult to support complex scenarios such as information security operation with many factors. Therefore, the key of effective management of network security assets is the fusion of multi-source data. Large number of fragmented asset data need to be gathered and mixed together in order to obtain the whole picture of assets. Common asset information includes hardware, software, network, application system, organization management and so on, which involves many aspects of information about network assets (Fig. 2).

Key marking of security assets need to be focused on and be supplemented when necessary. The lack of key attribute marks will hinder the of asset management. For instance, the lack of information of the person in charge of a system will make the responsibility identification unclear. Information attributes can be roughly divided into five aspects: network, software, application, management and vulnerability. In practice, due to the partial accumulation of asset information, the management of security assets does not need start with nothing. Asset information with different attributes is generally stored in different departments of a bank. Therefore, the core problem of banks in asset management is to integrate the fragmented information comprehensively and integrate it to support the security operation. For the supplement of asset information, both detection and docking should be considered. Detecting and supplementing asset information is as important as integrating asset information from multiple channels. Moreover, asset detection is also a method of asset monitoring, which is the most important step in the whole life cycle management to protect asset information timely and accurately.

Fig. 2. Design of network asset management

The purpose of safety asset management is to find risks actively. In the multi-dimensional application of network assets, it can include: asset governance, asset full perspective, vulnerability warning, compliance inspection and so on. Asset governance means to discover unregistered assets, which is the most practical application in safe asset management. The asset full perspective means the association and display of asset data from different sources in order to provide multi-directional information for security operation. Vulnerability warning means to match the system, middleware, database, framework and other asset data in vulnerability notification. Auto POC verification tool can make the vulnerability matching more effectively. Compliance inspection means using the recorded asset information to automatically check whether assets meet the baseline regulation. With the support of comprehensive, timely and accurate asset information, security operation can be carried out more effectively.

6 Conclusions

Based on the literature review of bank safety asset management, this paper summarizes the detection, management and multi-dimensional application of asset information. A network asset management method suitable for banks is put forward. The conclusions are as listed as follows:

- 1) The detection of network security assets is the starting point. Comprehensive, timely and multi-dimensional detection methods can make the asset management work more effective.
- 2) Management of network security assets is the core. With the support of technology construction and regulation construction, network security assets can make the information security operation easier.
- 3) The aim of asset management is to discover risks actively and multi-dimensional application reflects the true value of management achievement. The network risk facing banks can be minimized.

- 4) At present, banks need to take the problem of fragmental management of data into consideration in network security asset management. It is a practical solution to fully and timely docking and fusing multi-source information from different systems.

References

1. Wang, C., Guo, Y., Zhen, S., Yang, W.: Research on network asset detection technology. *Comput. Sci.*, 24–31 (2018)
2. Zhang, H., Wang, S., Jin, H., Deng, X.: Detection of operator network asset security management and control technology and solutions. *Guangdong Commun. Technol.* 5–9 (2019)
3. Yao, M., Lu, N., Bai, Z., Liu, Y., Shi, W.: Building method of device fingerprint search engine for network asset vulnerability assessment. *J. Electron.* 2354–2358 (2019)
4. Pei, Z., Li, B., Wang, X.: Logic processing design of IP and port scanning system. *Network Secur. Technol. Appl.* 26–27 (2017)
5. Ding, Y., Gao, Q., He, L.: Design and realization of assets sacn system based on complement protocol. *J. Shanghai Univ. Technol.* 196–200(2010)
6. Yu, X.: Design and realization of TCP/IP network scan strategy. *J. Wuhan Vocational Techn. College*, 54–56 (2009)
7. Li, J., Liu, P., Cai, G.: Dynamic network asset monitoring based on traffic perception. *Inf. Secur. Res.* 523–529 (2020)
8. Deng, X., Jin, H., Wang, S., Zhang, H.: Research on active discovery of IP assets in enterprise open network environment. *Guangdong Commun. Technol.* 2–4 (2019)
9. Lin, P.: Research on web risk scanning of internet information assets of postal enterprises. *Postal Res.* 15–17 (2008)
10. Chen, Z.: Case analysis and practice of web penetration. *Network Secur. Technol. Appl.* 22–24 (2020)
11. Wang, K., Li, Z., Wang, R., Gao, W., Wang, W., Wang, J.: Vulnerability scanning based on Nmap&Nessus. *Commun. Power Technol.* 135–136 (2020)
12. Zou, H.: Exploring the strategy of strengthening network asset management in the communication industry. *Modern State-owned Enterprise Res.* 49–50 (2015)
13. Li, Y.: On the role and importance of IP address planning and management in large and medium-sized enterprises. *Commun. World*, 20–21 (2019)
14. Wang, W.: Study on computer network security management and maintenance in hospital informatization construction. *Technology*, 115–116 (2020)
15. Zhang, X., Yuan, S., Ma, Z., Zhang, M., Gao, F.: Cloud-oriented asset security management scheme. *Post Telecommun. Des. Technol.* 12–15 (2019)
16. Xiao, Y., He, M., Wang, L.: Application research and practice of telecom operators' network asset security management technology. *Guangdong Commun. Technol.* (2018)
17. Song, J., Tang, G.: Research and application of network security situational awareness technology. *Commun. Technol.* 1419–1424 (2018)
18. Yang, X.: Thoughts on implementing dynamic management of network assets in the communication industry. *Chinese Foreign Entrepreneurs*, pp. 68–69 (2014)
19. Xie, R.: Lean management of optical network assets. *Commun. Enterprise Manage.* 24–27 (2017)
20. Zhang, S.: Network security technology based on blockchain. *Inf. Technol. Inform.* 129–131 (2019)

21. Chen, J.: Pre-matching scheme of network asset resources based on weighted cosine similarity. *Telecommun. Technol.* 46–49 (2018)
22. Lei, B.: About operation and maintenance management of IP addresses in enterprise networks. *Network Secur. Technol. Appl.* 106–107 (2019)
23. Yue, J.: Building an e-government network health evaluation platform based on situational awareness technology. *Inform. China*, 44–48 (2018)
24. Xia, Z., Li, L.: Research and design of network security situational awareness system. *Inf. Commun.* 147–148 (2017)
25. Li, H., Huang, X.: Illegal access detection of wireless routing equipment based on asset identification technology. *China Secur.* 101–105 (2019)
26. Xiao, X., et al.: A review of research on security situation prediction technology based on artificial intelligence. *Inf. Security Res.* 506–513 (2020)
27. Zhao, C., Sun, H., Wang, G., Lu, X.: Network security analysis of power information system based on big data. *Electron. Des. Eng.* 148–152 (2019)
28. Ma, Y.: Research on information security and protection of computer networks in the era of big data. *Wind Sci. Technol.* 82 (2020)
29. Hua, R.: Vulnerability management five: ten best practices. *Instrument and Instrument*, 60–62 (2016)
30. Liu, Z.: Theory and practice of Internet finance users' privacy data security. *Secur. Cyberspace*, 11–15 (2020)
31. Cai, G., Liu, P., Li, C.: Analysis of traffic security baseline of government websites. *Inf. Secur. Res.* 537–542 (2020)

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.