Research on Hierarchical Cyber Security Threat Situation Quantitative Assessment and Security Prevention Measures Based on Information Technology

Rui Mai[1], Mingzhu Wu[1,*]

[1]Hainan College of Economics and Business, China, 571127

*Corresponding author e-mail: mairui@hceb.edu.cn

Abstract. With the rapid development of information technology and the rapid changes in network security, traditional network security technology has been very easy for hackers to find loopholes, hackers crack the corresponding cryptographic algorithm formula, and steal a large number of user information and data, resulting in the network in recent years Security has created a crisis of trust. Therefore, in order to enable massive data to operate safely and effectively in the network, this article has carried out a quantitative assessment of the threat situation of the network. The quantitative assessment of the threat situation of the network is divided into support evaluation and credibility evaluation. In addition to the three levels of evaluation and severity evaluation, some network security-related precautions are listed. The experimental results show that these hierarchical security precautions can increase the security rate of Internet users' information by 4%-5%.

Keywords: Information Technology, Network Security Threat Situation, Hierarchical Network, Quantitative Assessment, Security Precautions

1. Introduction

Network security situation assessment refers to the perspective of risk management, using scientific methods and techniques, and analyzes network situation elements, analyzes the security threats faced by network systems and the vulnerability in the network. By evaluating the hazard of the threat event through the risk quantization method, it is proposed to reduce the protection measures and defense countermeasures to reduce, avoid or resist risks, and control the risk within the system tolerance. Network security threats quantitative assessment can usually be divided into quantitative evaluation and qualitative assessment. Qualitative assessment refers to the result of describing the status assessment using the descriptive language [1]. Quantitative assessments apply to risk classification, and interpretation of the results can be understood and are easy to calculate. At the same time, quantitative assessment avoids significant differences between results due to human allocation, but quantitative assessment results are not accurate and subjective [2]. Quantitative evaluation is a method of evaluating the evaluation target using evaluation indicators, which represent the results of the status assessment in mathematical form [3]. The evaluation method is still based on subjective factors, and the cost is higher [4].

2. Methods and related concepts

2.1. Cybersecurity situational awareness

Network security situation awareness first understands and objectively evaluates the security status factors that affect network operations under specific time and space conditions, and then analyzes the current network security status. A series of network security prevention strategy procedures can be specifically determined by predicting growth trends and appropriate trends [5].

2.2. Situational quantitative assessment

Common trend quantitative evaluation methods include hierarchical analysis, causal relationship analysis and Octave methods. The hierarchical analysis process decomposes different levels of complex problems, decomposes the elements associated with decision-making into targets, standards, plans, and other levels, and is a pair of elements that are compared to the same parent node finally get a pair of factors. The top layer affects the weight of each layer, and finally use weights and methods to obtain the weight of each pattern on the target. Situation evaluation technology Evaluate the security status of the network based on the information that combines the information obtained by the combined number of secure data sources. It helps administrators for comprehensive evaluation of the overall security situation of the network, thus adopting appropriate safety measures to ensure the safety of the network. It has a comprehensive risk and threat to the network by analyzing the log information generated by various system security tools to get the network security status, thereby having a comprehensiveness of the risks and threats faced by the network. In addition to the first time, the results obtained by entering the status assessment when the future security status changes. Therefore, the assessment of the security situation of the network is an important one ring in the field awareness is also a core one ring. The research on trend assessment is usually a hierarchical assessment, constructing a situation assessment system framework, and the collection of massive safety elements will be analyzed by data fusion, related analysis and other technical analysis, considering the stage and complexity of network security incidents, except It is necessary to quantify the credibility of the intrusion attack, but also to authenticate the type of security event. On this basis, it is necessary to take into account the condition that the attack is successful and the degree of matching with the operational environment and configuration of the target host. Further, a quantitative evaluation of the successful invasion of the attack, and finally, its severity is determined from the nature of the attack [6]. The trend quantitative evaluation model is shown in Figure 1:

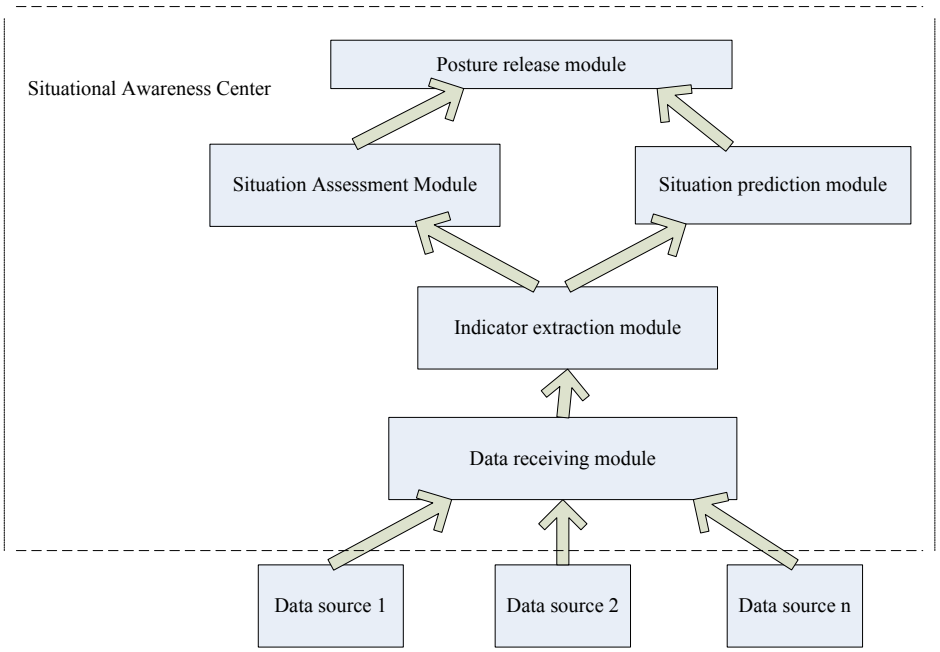

Figure 1. Situational quantitative assessment model

2.3. Network security situation assessment algorithm

The network security situation assessment algorithm uses the network security information of each server node in the network (including intrusion information, network node topology information, vulnerability information performance information service information, and log information) to obtain the vulnerability situation, threat situation, and System operation situation, combined with the distribution of nodes in the network cluster to determine the vulnerability situation, threat situation and the degree of influence of the system operation situation on different nodes, then the security situation assessment value of the entire network can be expressed by formula (1):

$$Y = \sum_{j=1}^{k} (D_j, E_j, F_j) * (U_{jD} U_{jE} U_{jF}) \tag{1}$$

3. Quantitative assessment and experimental design of safety methods and measures

3.1. Support evaluation

The purpose of support evaluation is to quantify the support of successful attacks, which is an important part of security threat evaluation [7]. The network environment is full of a large number of false alarms and false alarms, so that the truly threatening security events are hidden in these traffics, and whether the intrusion attack can be successfully implemented has a lot to do with the matching conditions. The dependent conditions include the configuration information of the target host and the running status of the service. For example, for the FTP server program Wu -ftpd remote overflow attack, this attack uses exhaustive methods to search for the correct overflow point and generate a shell, but it has no attack effect on hosts that do not provide FTP services, or when setting the buffer size more than Max Path Len, it also has no attack effect. IDS will report a very high severity alarm information for the detected Wu - ftpd remote overflow attack, but when the target host does not have specific operating conditions and configuration information, the system should quantify the low support for this alarm [8].

3.2. Severity assessment

The severity of the attack is classified according to the degree of damage to the target network environment according to the attack intent, from 0 to 9 divided into ten levels, the higher the level, the higher the severity of the consequences of the attack [9]. The classification is mainly based on the destructiveness of the attack and the purpose and means of the invasion. The classification of threat attack severity levels is shown in Table 1:

Table 1. Classification of attack severity

Grade	Evaluation Criteria
0	Get OS, apply version information.
1	Get system sensitive information.
2	Read the unrestricted file and data.
3	Read more important or limited files and data.
4	Make a restricted file and data.
5	Move a restricted important document and data.
6	For unrestricted important documents, data is modified, or DOS attacks on ordinary services.
7	Execute the command or perform the system as a normal user, the network-level DOS attack.
8	Execute commands as managed (limited, not easy to use).
9	Execute commands as managed (not limited, easy to use).

3.3. Credibility assessment

Credibility evaluation refers to the evaluation of the possibility of intrusion attacks in the network. Many references introduce D-S evidence theory to assess the credibility of threats. D-S evidence theory belongs to the feature-level and decision-level fusion in data fusion. It combines the results of related evidence classification and is currently widely used in the field of data fusion and target recognition [10].

4. Feasibility analysis of hierarchical network security threat situation quantitative assessment

The data sources needed for network security situation assessment include asset value assessment results, vulnerability assessment results, credibility, support and severity results in the threat assessment process [11]. The probability of successful execution of the attack is calculated from the threat credibility and the threat support degree, and the possibility of intrusion of the security event is calculated based on the vulnerability assessment result [12]. At the same time, the loss level caused by the security incident can be calculated from the threat severity and asset value evaluation results, and the intrusion probability and loss level of the target system are substituted into the matrix to calculate the security situation assessment results, and finally the security situation can be graded [13]. The whole evaluation method is based on warnings as clues, based on quantitative indicators of threat elements, and the process of gradual fusion of the values of various indicators, and the result is a real-time threat situation map of the evaluation object [14]. Therefore, it is feasible and necessary to construct a hierarchical network security threat situation quantitative assessment model and propose corresponding security precautions.

5. Conclusion

This article focuses on the related concepts of the hierarchical quantitative assessment of cyber security threat situation, and gives the indicator system and corresponding theory for large-scale network situation assessment. The network security threat situation assessment is divided into credibility assessment, support assessment, and seriousness assessment. The experimental results show

that the hierarchical quantitative assessment of network security threat situation can reduce the online risk of netizens and provide netizens with a green and reliable network environment [15].

References

[1] V, Sambamurthy, S, et al. The design of information technology planning systems for varying organizational contexts [J]. European Journal of Information Systems, 2017, 2 (1): 23-35.

[2] Begovi B. Book Review: The Great Convergence: Information Technology and the New Globalization [J]. Panoeconomicus, 2017, 64 (5):645-655.

[3] Singh H, Sittig D F. Measuring and improving patient safety through health information technology: The Health IT Safety Framework [J]. Bmj Quality & Safety, 2016, 25 (4): 226-232.

[4] Farajollah R, Zahra A. The effect of information technology on organizational agility in the light of organizational culture [J]. Molecular Carcinogenesis, 2016, 45 (8): 561-571.

[5] Muda I, Wardani D Y, Erlina, et al. The Influence of Human Resources Competency and the Use of Information Technology on the Quality of Local Government Financial Report with Regional Accounting System as an Intervening [J]. Journal of Theoretical & Applied Information Technology, 2017, 95(20):5552-5561.

[6] Mocetti S, Pagnini M, Sette E. Information technology and banking organization [J]. Journal of Financial Services Research, 2017, 51 (3): 313-338.

[7] Jorgenson D W, Ho M S, Samuels J D. The impact of information technology on postwar US economic growth [J]. Telecommunications Policy, 2016, 40 (5): 398-411.

[8] Guido, Schwarz. Enabling Global Trade above the Clouds: Restructuring Processes and Information Technology in the Transatlantic Air-Cargo Industry [J]. Environment and Planning A, 2016, 38 (8): 1463-1485.

[9] Luftman J, Lyytinen K, Zvi T B. Enhancing the measurement of information technology (IT) business alignment and its influence on company performance [J]. Journal of Information Technology, 2017, 32 (1): 26-46.

[10] Salehi-Sangari E. Management of information technology in Swedish firms : An empirical study [J]. Gut, 2016, 7 (1): 1-13.

[11] Lioukas C S, Reuer J J, Zollo M. Effects of Information Technology Capabilities on Strategic Alliances: Implications for the Resource-Based View [J]. Journal of Management Studies, 2016, 53 (2): 161–183.

[12] Schermann M, Dongus K, Yetton P, et al. The role of Transaction Cost Economics in Information Technology Outsourcing research: A meta-analysis of the choice of contract type. [J]. Journal of Strategic Information Systems, 2016, 25 (1): 32-48.

[13] Lefley F, Sarkis J. Applying the FAP Model to the Evaluation of Strategic Information Technology Projects [J]. International Journal of Enterprise Information Systems, 2017, 1 (2): 69-90.

[14] P. H, Shylesh S, Aithal P S. Information Technology Innovations in Library Management: A Case of SIMS [J]. Social Science Electronic Publishing, 2016, 1 (1): 657-676.

[15] Han S, Rezaee Z, Ling X, et al. The Association between Information Technology Insvestments and Audit Risk [J]. Journal of Information Systems, 2016, 30 (1): 93-116.