Pisco Med Publishing

Learning & Education
ISSN：2251-2802

Key Issues and Solutions of Security Auditing in Network Security Management

Sijun Wang, Yiming Dai*

College of Information and Electrical Engineering, Hebei University of Engineering, Hebei 056009, China

Abstract: With the rapid development of information technology, network security faces increasingly severe challenges. Security auditing, as a critical component of network security management, plays an indispensable role. This paper analyzes the current status of security auditing in network security management and explores the primary issues it faces, including the complexity of processing massive data, the inadequacy of auditing technologies and tools, and the weakness of security awareness within both personnel and organizations. A series of solutions is proposed, encompassing the innovation of auditing technologies, the improvement of auditing processes, and the enhancement of personnel qualifications, aiming to provide both theoretical support and practical guidance for improving the effectiveness of network security auditing, thereby ensuring the security and stability of the network environment.

Keywords: Security Auditing; Network Security Management; Auditing Technologies; Solutions

Introduction

With the comprehensive arrival of the information society, network security issues have increasingly become a focal point of global concern. Network attacks, data breaches, system vulnerabilities, and other security threats are occurring with growing frequency and complexity, posing significant risks to the operations of various organizations. As an indispensable component of the network security management system, the role of security auditing has become more pronounced. Security auditing not only aids in identifying potential security threats but also ensures the integrity and availability of data, thereby enhancing an organization's ability to defend against security breaches. In practice, however, security auditing faces numerous challenges, including the exponential growth of data, the lag in technological capabilities, and the lack of sufficient human resources. This paper will delve into these challenges and propose feasible solutions to optimize and enhance network security auditing.

1. Overview of Security Auditing in Network Security Management

1.1 Definition and Importance of Security Auditing

The evolution of information technology has significantly increased the complexity of network systems, driving a corresponding exponential rise in security threats and potential risks. In this context, security auditing, as a vital component of the network security management framework, assumes the crucial responsibilities of monitoring, evaluating, and optimizing security measures. It encompasses key aspects such as the monitoring of data flow, the recording of system behavior, the verification of policy execution, and the traceability of anomalous activities. Its primary objective extends beyond identifying potential security vulnerabilities, placing greater emphasis on evaluating the effectiveness of existing security strategies, thereby providing a precise foundation for adjusting security defenses[1]. Within the realm of network security governance, security auditing serves multiple roles; it enhances compliance by ensuring that systems align with relevant laws and regulations while also assisting security managers in optimizing resource allocation, improving operational security efficiency, and bolstering the system's resilience to attacks. As information assets increasingly become a core competitive advantage, the value of security auditing becomes ever more pronounced, as its contributions to maintaining data integrity, safeguarding business continuity, and addressing emerging security threats determine its irreplaceable position within the network security management system.

1.2 Core Objectives of Network Security Management and Auditing Requirements

The core objectives of network security management focus on the confidentiality, integrity, and availability of information systems,

ensuring that data remains protected from unauthorized access, tampering, or destruction, while simultaneously maintaining business continuity and system stability. In the face of increasingly sophisticated attack methods, relying solely on static security policies proves inadequate to cope with the dynamic and evolving risk landscape. A robust security auditing mechanism becomes a necessary means of achieving these objectives. The auditing requirements span multiple facets, including log analysis, anomaly detection, access control management, and policy execution oversight, all aimed at achieving a comprehensive understanding of system operation and ensuring that potential threats are identified and addressed before they escalate[2]. Within a risk management framework, security auditing not only provides accurate data support, enabling managers to optimize defense strategies based on objective evidence but also enhances an organization's ability to perceive the security landscape, improving the accuracy and timeliness of response efforts. As the importance of data assets continues to rise, the scope of auditing needs expands to include privacy protection, cross-system collaborative monitoring, and intelligent anomaly analysis, thus deepening its role within the network security management framework.

1.3 Basic Processes and Methods of Security Auditing

The implementation of security auditing relies heavily on rigorous process design and a scientific methodology. Its core processes involve data collection, analysis, risk assessment, report generation, and the proposal of corrective actions. During the data collection phase, the integration of multi-source data, including system logs, access records, and user behavior trajectories, ensures the comprehensiveness and reliability of the audit foundation. In the analysis phase, leveraging big data analytics, pattern recognition, and behavior modeling technologies enables the extraction of anomalous patterns from vast information flows, allowing for the precise identification of potential security risks. Risk assessment centers on quantitative analysis, evaluating the severity of security incidents and their potential cascading effects based on factors such as threat level, impact scope, and attack chain metrics. This evaluation provides scientific evidence for subsequent adjustments to defense strategies. The report generation phase not only involves presenting the audit findings but also integrates historical data and industry benchmarks to produce trend analysis and improvement recommendations, driving the dynamic optimization of security policies. With the continuous advancements in automation technologies and artificial intelligence, auditing methods are progressively evolving towards more intelligent and adaptive frameworks, facilitating more efficient and precise security monitoring and protection mechanisms.

2. Main Challenges Facing Network Security Auditing

2.1 Vast and Complex Nature of Security Data

With the relentless advancement of information technology and the rapid expansion of network environments, the first challenge that network security auditing encounters is the exponential growth of data volume and the increasing complexity of data structures. In modern network architectures, the massive data flows, distributed information sources, and the integration of various devices have made the collection, processing, and analysis of data for security auditing increasingly arduous. The convergence of diverse information types—such as security logs, user behavior records, and network traffic data—creates a complex hierarchical structure while also demanding multi-dimensional spatial-temporal analysis. The surge in data volume directly amplifies the pressure on auditing tools regarding data storage and processing, rendering traditional manual auditing methods incapable of meeting the demands of real-time analysis and struggling to detect latent threats effectively. The inconsistency in data formats and standards across different systems, platforms, and applications further complicates data integration and comparison, making it exceptionally challenging to consolidate information across various sources. A critical task within security auditing is the effective filtering of large amounts of heterogeneous data, ensuring that the focus remains on potential security events, thereby mitigating the interference of redundant information on the audit outcomes.

2.2 Inadequacy of Auditing Tools and Technologies

As network attack techniques continuously evolve, existing security auditing tools and technologies frequently fail to adapt to the emerging threat landscape. In many instances, traditional auditing tools focus primarily on the collection of static data and report generation, while their ability to detect and respond to real-time threats remains insufficient. The increasing diversification of network attack methods,

spanning across platforms, applications, and protocols, means that traditional auditing tools are ill-equipped to handle the complexity of modern attacks. Moreover, existing auditing technologies often lack the necessary intelligence to monitor and identify dynamic behaviors within big data environments effectively. This deficiency is especially evident when attempting to detect highly covert attack methods, such as zero-day vulnerabilities and internal network attacks, which cannot be adequately preempted using traditional rule-based or pattern recognition techniques. Furthermore, many current auditing tools lack adaptive capabilities, making them unable to dynamically adjust to the ever-evolving network environments, rendering the auditing process inefficient in responding to emerging types of cyberattacks.

2.3 Insufficient Security Awareness Among Personnel and Organizations

The effectiveness of network security auditing is not only dependent on technical tools and data processing capabilities but is also profoundly influenced by the security awareness of both personnel and organizations. Despite the increasing potential dangers of network security threats, many organizations and individuals still fail to recognize the critical importance of security auditing. Security auditing is often viewed merely as a post-incident accountability measure rather than an effective mechanism for preventing and detecting security vulnerabilities in a timely manner, leading to insufficient attention and investment in the execution of auditing activities. The absence of a strong security culture within organizations further exacerbates this issue, resulting in employees failing to consistently adhere to security auditing protocols in their daily tasks. Essential procedures, such as logging and data protection, are frequently neglected, which in turn undermines the integrity and accuracy of auditing information[3]. The professional expertise and technical proficiency of auditing personnel also directly impact the quality of the audit process; many auditing tasks require highly specialized technical support, but the training and skill enhancement of current auditing personnel often lag behind the rapidly evolving cyber threats. The lack of security awareness not only diminishes the level of cooperation within the organization during the auditing process but also leads to the ineffective detection and response to potential security risks.

3. Solutions for Enhancing the Effectiveness of Security Auditing

3.1 Strengthening the Research and Development of Security Auditing Technologies and Tools

As the network environment continues to evolve, the technological challenges faced by security auditing have become increasingly intricate, making the development of intelligent and automated auditing tools an urgent necessity. The incorporation of artificial intelligence (AI) and machine learning (ML) technologies into auditing tools enables them to perform pattern recognition, anomaly detection, and trend analysis at a far more efficient level, thereby enhancing the accuracy and flexibility of the auditing process[4]. In comparison with traditional tools, these intelligent tools are better equipped to adapt to the ever-changing network environment, allowing for real-time analysis of data flows across multiple dimensions, identifying potential security vulnerabilities, and making dynamic adjustments. Big data-based auditing tools can also process and integrate heterogeneous data from diverse systems and devices, addressing issues related to data fragmentation and varying formats, thereby enabling seamless cross-platform and cross-device monitoring. These technological advancements not only enhance the precision and responsiveness of auditing tools but also significantly reduce the burden of manual analysis. With the application of blockchain technology, the transparency and reliability of audits are further strengthened, ensuring the traceability of auditing outcomes and the immutability of the data. Strengthening the innovation and development of auditing technologies and tools can not only enhance auditing efficiency but also fortify defenses against complex attack methodologies.

3.2 Improving Auditing Processes and Management Systems

Beyond technological advancements, the improvement of auditing processes and management systems is equally crucial for enhancing the effectiveness of security auditing. Security auditing is not merely a technical task but also involves organizational coordination and systemic arrangements. The auditing process should be thoroughly reviewed and optimized to ensure its scientific rigor and adaptability. A well-designed auditing process can provide comprehensive, multi-dimensional monitoring of information systems, facilitating the timely identification of security risks and preventing the spread of vulnerabilities or attacks. Auditing efforts must be closely integrated with routine

network security management, forming a closed-loop mechanism for early warning, feedback, and remediation. Auditing results should not only be communicated to relevant departments but also be translated into specific corrective measures aimed at enhancing the overall resilience of the security defense system. Regarding management systems, the establishment of robust auditing standards and protocols is equally essential. The absence or inadequacy of systems often results in auditing activities being ineffective or unable to prompt targeted improvements. In system development, it is critical to refine and clarify auditing procedures, creating corresponding standards and evaluation metrics to ensure the operability and effectiveness of auditing practices. Strengthening cross-departmental cooperation ensures that all stakeholders are engaged in the auditing process, enhancing the comprehensiveness of audits and ensuring that corrective actions are swiftly implemented. Through these enhancements, the improvement of auditing processes and management systems contributes significantly to the overall efficacy of network security management.

3.3 Enhancing Personnel Qualifications and Security Awareness

The successful implementation of network security auditing is not solely reliant on technological and managerial frameworks but is also profoundly influenced by the qualifications and security awareness of the personnel involved. While the effectiveness of technical tools and the rationality of auditing processes are undeniably important, if auditing personnel lack sufficient expertise and operational capabilities or if organizations fail to recognize the importance of auditing, even the most advanced technologies and systems cannot achieve the desired outcomes. Improving personnel qualifications begins with targeted skills training for auditors, particularly in the context of dealing with increasingly complex network threats and the constant evolution of technical tools. By reinforcing education in emerging technologies such as artificial intelligence and big data analytics, auditors can enhance their proficiency with advanced tools, ensuring their adaptability to ever-shifting network security challenges. The enhancement of security awareness should also begin at the organizational level, fostering a culture of security across all personnel. Organizations must regularly conduct network security training, ensuring that employees understand data protection principles, cybersecurity regulations, and auditing protocols, thereby reducing human error and noncompliance with auditing standards. Effective security awareness education ensures that employees adhere strictly to security procedures in their daily tasks, providing high-quality data support and collaboration for the auditing process. Leadership must cultivate a strong security awareness, incorporating security auditing into organizational strategic decisions and driving the advancement of the organization’s security culture. Improving personnel qualifications and security awareness enhances not only the quality and efficiency of auditing activities but also the overall security defenses of the organization, ensuring the stability and security of its information systems.

CONCLUSION：

In the current, ever-evolving network environment, security auditing serves as the cornerstone of network security management, and its role cannot be underestimated. Faced with the growing security risks, the vastness and complexity of audit data, and the lag in technological advancements, it is imperative to implement effective measures to address these challenges. By strengthening the research and development of auditing technologies and tools, improving the real-time performance and accuracy of auditing tools, significant improvements in auditing efficiency can be achieved. Enhancing auditing processes and management systems, ensuring the uniformity of auditing standards, can effectively remedy gaps in existing procedures. Furthermore, improving the security awareness and technical capabilities of personnel is an essential safeguard to ensure the smooth execution of security auditing tasks. A comprehensive enhancement of security auditing effectiveness is crucial to bolster the overall defensive capabilities of network security management.

REFERENCES

[1]Li, W. (2024). The Role of Security Auditing in Security Risk Management. Confidentiality Science and Technology, 2024(3), 65-70.

[2] Song, H. (2023). A Versatile Tool: Network Situation Awareness Empowering Network Security Management. Computer Campus, 2023(9), 11418-11419.

[3] Peng, D., & Li, Y. (2024). Gushi County Audit Bureau Holds 2024 Network Security Training Session. Finance (Audit), 2024(8), F0002.

[4] Chen, L., Li, H., & Liu, C. (2024). Research on 5G-R Network Security Auditing System Based on eBPF and ConvLSTM. Railway Standard Design, 2024(004), 068.

Author Introduction:

Sijun Wang(2004-), male, from Qinhuangdao, Hebei Province, is a student at the School of Information and Electrical Engineering, Hebei University of Engineering. His research direction is computer science and technology.

Corresponding author:

Yiming Dai (2002-), male, from Tangshan, Hebei Province, a student at the School of Information and Electrical Engineering, Hebei University of Engineering, with a research focus on computer science and technology