Journal of Electronics and Information Science (2023)
Clausius Scientific Press, Canada

DOI: 10.23977/jeis.2023.080406
ISSN 2371-9524 Vol. 8 Num. 4

Research on the Application of Network Security Technologies in the Network Security Operations and Maintenance Process

Zhenping Zhang, Xuan Guo

Henan Technical Institute, Zhengzhou, 450042, China

Keywords: Network security operations and maintenance; network security technologies; application research

Abstract: This study focuses on the key issues of network security operations and maintenance, exploring the application and prospects of network security technologies. The importance of network security operations and maintenance is analyzed, and the significance of common security threats and vulnerability analysis is introduced. The application of technologies such as access control, data protection, and threat detection in operations and maintenance is discussed, and the prospects of innovative technologies like artificial intelligence and blockchain in network security are highlighted. The conclusion emphasizes the significance of technological innovation, calling for continuous research and innovation to ensure the construction of a safer and more reliable digital environment.

1. Introduction

With the rapid development of information technology and the widespread use of the Internet, networks have become the core infrastructure for people's daily lives and business activities. However, this has brought forth various complex and ever-changing network security threats, which may lead to the leakage, damage, or even catastrophic consequences of critical personal, organizational, and national information. In this digital age, safeguarding network security and ensuring stable operations have become exceptionally important. In the future, as technology continues to advance, new security threats will constantly emerge, alongside more innovative and efficient security technologies. Through in-depth research and practical application of network security technologies, contributions are anticipated to be made towards establishing a more secure and trustworthy network environment.

2. Network Security Operations and Maintenance Overview

2.1. Definition and Importance

Network security operations and maintenance refer to the use of a series of strategies, processes, and technological measures throughout the entire lifecycle of an information system to protect network infrastructure from various security threats. In this era of information, the significance of network security operations and maintenance is self-evident. As activities of enterprises, governments, and individuals on the network increase, network security issues have become one of the main bottlenecks hindering digital development. Effective implementation of network security operations and maintenance can ensure the protection of confidential data, business continuity, and user privacy security, providing a solid foundation for the sustainable development of the information society.

2.2. Operations and Maintenance Processes and Methods

Network security operations and maintenance encompass a wide range of processes and methods aimed at achieving the continuity and robustness of network security. Firstly, conducting periodic risk assessments is a critical initial step in network security operations and maintenance, requiring the identification of system vulnerabilities, weaknesses, and potential attack paths to take early measures to mitigate risks. Subsequently, based on the results of risk assessments, appropriate security strategies and policies are formulated and implemented, covering aspects such as access control, data protection, and identity authentication to ensure overall system security. Building a real-time monitoring system on this basis can rapidly detect potential security events. Once anomalies are detected, swift action must be taken to investigate and respond to security threats to minimize potential damages. As the field of network security continues to evolve and attack methods change rapidly, network security operations and maintenance also need to continually learn and improve to adapt to new threats. To achieve this, regular training and drills can enhance the security team's responsiveness and crisis handling skills, ensuring the continuous secure operation of the network.[1]

3. Security Threats and Vulnerability Analysis

3.1. Common Security Threats

There are various security threats in the network environment that can have a severe impact on systems and data. Here are some common security threats: Malware and virus attacks involve malicious software such as viruses, worms, trojans, etc., which can disrupt systems and data through the spread and implantation of malicious code. They might steal sensitive information, damage files or systems, posing a serious threat to network security. DDoS attacks, or Distributed Denial of Service attacks, flood target systems with a large number of false requests, rendering them unable to function properly. This can lead to service unavailability and significantly impact business operations. Social engineering attacks exploit psychological and social skills to deceive and obtain sensitive information. For instance, phishing attacks use forged trustworthy communication to deceive users into revealing usernames, passwords, and other information.[2]

3.2. Vulnerability Analysis and Assessment

Vulnerabilities are security weaknesses present in systems that malicious attackers can exploit. Vulnerability analysis and assessment is the process of identifying and understanding these weaknesses to facilitate early repair and reinforcement. The types and severity of vulnerabilities vary based on their exploitability and potential impact, including code defects, configuration errors, and insecure network communication. Vulnerability assessment usually employs automated tools and manual reviews to discover potential vulnerabilities within the system. This is done by scanning code, configurations, and network communications, identifying potential issues, and generating reports for analysis and remediation. These measures help enhance system security and reduce the risk of being compromised.[3]

4. Application of Network Security Technologies in Operations and Maintenance

4.1. Access Control and Identity Authentication

Access control and identity authentication are crucial technologies in network security, preventing unauthorized access and ensuring the legitimacy of user identities. By effectively implementing robust access control strategies, systems can precisely limit access permissions for specific users or roles, significantly reducing the potential risks of malicious behavior. These technologies play an indispensable role in building network security defenses, ensuring the integrity and confidentiality of systems and sensitive data. Access control ensures that only authorized users can access system resources. By carefully designing and implementing access control policies, system administrators can manage user, process, and device access to resources. This can be achieved through various methods such as Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), and Mandatory Access Control (MAC).[4] The key to access control is to balance security and convenience at an appropriate level to meet the needs of different users and roles. Identity authentication is the process of confirming the authenticity of user identities to ensure that only authorized users can access the system. Traditional single-factor authentication is typically achieved through usernames and passwords, but this method has gradually become susceptible to attacks. To enhance the reliability of authentication, Multi-Factor Authentication (MFA) has become increasingly important. MFA combines multiple authentication factors such as passwords, biometrics (fingerprint, facial recognition, etc.), and hardware tokens to strengthen the authentication process. This layered identity verification can significantly reduce the likelihood of unauthorized access and enhance the overall security of the system.

4.2. Data Protection and Encryption

In network security operations and maintenance, data protection and encryption technologies play a crucial role in ensuring the security of sensitive information during transmission and storage. These technologies not only help prevent data leaks and malicious data acquisition but also provide an additional layer of security to safeguard user privacy and business confidentiality. Data protection refers to measures taken to ensure the integrity, availability, and confidentiality of data. Data is susceptible to various risks during transmission and storage, such as theft, tampering, and destruction.[5] Applying data protection technologies can effectively mitigate these risks. Encryption is one of the core methods of data protection. By transforming data into ciphertext, encryption makes data difficult to decipher without authorization. Encryption technology can protect data from theft during transmission and prevent data leaks during storage. Only individuals with decryption keys can decrypt the ciphertext, ensuring data security. When applying encryption technology, choosing appropriate encryption methods and algorithms is critical. Data classification and encryption strategies allow the selection of suitable encryption methods based on the sensitivity and value of the data. Generally, more sensitive data can use stronger encryption methods, while less sensitive data can use lighter encryption methods. Such strategies can ensure data security while minimizing the impact of encryption on performance.[6]

4.3. Threat Detection and Response

In network security operations and maintenance, threat detection and response technologies are critical to preventing and addressing network security threats. As network threats continually evolve and become more sophisticated, the adoption of threat detection and response technologies such as Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) has become a crucial aspect of ensuring network security. Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are vital components of threat detection and response. IDS can monitor network traffic in real-time, identifying abnormal behavior and potential intrusions by analyzing and comparing network activities with known attack patterns. Once anomalies are detected, IDS issues alerts to notify the security team to take appropriate measures. IPS not only monitors abnormal activities but also automatically takes defensive actions when potential threats are detected, such as blocking malicious traffic or disconnecting connections, to prevent the further spread of attacks. The utilization and analysis of threat intelligence are also integral to threat detection and response. Threat intelligence includes information about current and emerging threats, helping the security team identify and assess potential threats early. By subscribing to various threat intelligence sources, analyzing and understanding the patterns and motivations behind threats, organizations can determine appropriate response strategies to safeguard against unknown threats.

4.4. Security Auditing and Log Management

In network security operations and maintenance, security auditing and log management technologies play a critical role in tracking, recording, and analyzing system operations and events. These technologies not only help identify potential security issues but also provide compelling evidence for investigating security incidents and ensure compliance requirements are met. Security auditing is a method of monitoring and recording system activities to identify potential security risks and violations. By recording user operations, system configuration changes, and network traffic, security auditing provides real-time, traceable activity records for the security team. These records can be used to analyze the causes of security incidents, identify potential threats, trace attack paths, and provide necessary information for legal and compliance reviews. Log management involves collecting, storing, analyzing, and retaining generated log information. Through effective log management, system administrators can examine the timing, location, and participants of events, revealing attack patterns and trends. Detailed log records can assist in tracking the source and impact of security incidents, better preparing for similar threats. Additionally, log management aids in meeting various compliance requirements such as GDPR and HIPAA. In practical application, attention must be given to privacy and data protection when employing security auditing and log management technologies. Ensuring that collected log information complies with relevant regulations while also taking measures to secure sensitive information is essential.

4.5. Virtualization and Container Security

With the widespread adoption of virtualization and container technologies, ensuring the security of virtualized and containerized environments has become critically important. Virtualization and container security technologies not only enhance environment isolation but also effectively prevent the propagation of malicious code between different instances, improving the overall security of the environment. Virtualization technology allows multiple virtual machines to run on the same physical server, each with its independent operating system and applications. The isolation provided by virtualization helps reduce the attack surface, but attention must also be paid to security vulnerabilities between virtual machines and host machines. For virtualization environments, a series of security measures need to be implemented, such as network isolation, access control, vulnerability management, etc., to ensure mutual isolation of virtual machines and the security of host machines. Container technology is more lightweight; containers can run multiple instances on the same host machine, sharing the operating system kernel, thereby providing higher resource utilization and deployment efficiency. However, sharing the kernel between containers brings certain security challenges. Consequently, container security technologies aim to establish isolation between containers, preventing the spread of malicious code between them. Employing container isolation technologies can limit container access to host machines and other containers, preventing lateral movement attacks. Image security is also a significant consideration in the container environment. Images serve as the foundation of containers, and an insecure image can lead to vulnerabilities across the entire container environment. Therefore, reviewing, validating, and hardening images are critical tasks in container security. In the fields of virtualization and container security, new technologies and solutions continue to emerge to address the ever-changing network threats.

5. Prospects of Innovative Technologies in Network Security Operations and Maintenance

5.1. Application of Artificial Intelligence and Machine Learning in Security Operations

The emergence of Artificial Intelligence (AI) and Machine Learning (ML) technologies brings new possibilities to network security operations, showcasing their immense potential through the fusion of these technologies with big data analysis and automation in the field of network security. The key direction is the application of AI and ML in threat detection and prediction. Compared to traditional rule-based security detection methods, these technologies are better equipped to handle emerging unknown threats. AI and ML can identify potential anomalous patterns and threat behaviors by analyzing large volumes of security data, even automatically detecting unusual activities such as zero-day vulnerability attacks. This adaptability allows these technologies to respond to ever-changing threat scenarios, achieving more accurate threat predictions and assisting security teams in identifying and responding to potential threats earlier. Another significant application is automated threat response. AI and ML technologies enable automated triggering of response mechanisms after threat detection, thereby rapidly accelerating the threat handling and mitigation process. This automated response not only saves time but also enhances response consistency and efficiency by blocking suspicious activities, cutting off malicious traffic, etc., reducing the impact of attacks. Moreover, AI and ML play a significant role in intelligent analysis and decision-making. They can analyze vast amounts of security data, uncover hidden patterns and correlations, and help security teams better understand attackers' behavior and strategies. This intelligent analysis aids in making wiser decisions and improves the responsiveness of security teams.

5.2. Potential of Blockchain Technology in Security Operations

The introduction of blockchain technology brings innovative methods and solutions to security operations, further enhancing network security and trustworthiness. One primary application is distributed identity authentication and access control systems. Traditional authentication methods are susceptible to single points of failure and data breaches. However, blockchain's decentralized nature makes it an ideal choice for building more secure identity authentication and access control systems. Storing user identity information on the blockchain enables decentralized identity authentication, effectively reducing potential attack risks. This approach not only enhances security but also lowers the threats of impersonation and identity theft. Blockchain technology can also help address single points of failure in network security. Single points of failure in network security can lead to system-wide crashes, whereas blockchain's decentralized nature ensures that data is distributed across multiple nodes in the network. This means that even if certain nodes are attacked or fail, other nodes can continue to function normally. This design architecture of distributed storage enhances system robustness, overall stability, and security.

5.3. Development of Adaptive Defense Technologies

The emergence of adaptive defense technologies will bring revolutionary changes to network security by enhancing defensive capabilities and efficiency through real-time monitoring and automatic adjustments. Adaptive defense technologies are based on real-time threat conditions and dynamic changes in the network environment. They can autonomously adjust defense strategies to more accurately address various threats. Traditional defense methods are typically static, and once established, they are not adjusted with changing threats, which can result in overly conservative or overly aggressive defense measures. However, adaptive defense technologies can dynamically adjust defense strategies based on real-time threat intelligence and network status information, enabling better responses to ever-evolving threats. One key advantage is that adaptive defense technologies can significantly reduce the false positive rate. Traditional security systems might identify legitimate activities as threats due to overly strict rule settings, which can affect normal business processes. Adaptive defense technologies can dynamically adjust based on actual circumstances, reducing false positives and improving the accuracy and credibility of threat identification.

5.4. Edge Computing and Security

Edge computing pushes data processing to the network's edge, supporting IoT devices and real-time applications, thereby reducing data transmission latency and network congestion. However, ensuring security in the edge environment has become more challenging due to its decentralization, heterogeneity, and complexity. Security issues in edge computing environments involve multiple aspects. First, since data is processed on edge devices and nodes, the edge environment is more vulnerable to physical and network-level attacks. Second, edge nodes are often distributed across multiple geographic locations and may face challenges in physical access control, increasing the risks of data leakage and device intrusion. Additionally, devices and sensors in edge computing often have limited computing and storage capabilities, restricting the application of traditional security measures. To address these challenges, innovative edge security technologies are rapidly developing. Among them, secure container technology is a critical solution. Secure containers isolate different edge applications and services, preventing malicious software from spreading from one container to another, thus protecting the overall security of the edge environment. Furthermore, virtualization technology can also be used to isolate virtual machines on edge nodes, achieving resource isolation and protection. The security of the edge environment also emphasizes identity authentication and access control. Due to the distributed nature of edge nodes, ensuring the identities and permissions of legitimate users becomes especially important. Multi-factor authentication and role-based access control can ensure that only authorized users can access edge devices and data.

6. Conclusion

This study delved into the application of network security technologies in network security operations and maintenance, highlighting the urgency and significance of safeguarding network infrastructure in today's information age. Through a detailed elucidation of the network security operations process, it's understood that it plays a pivotal role in risk assessment, security policy formulation, event monitoring and response, as well as continuous improvement. The analysis covered common security threats such as malware attacks, DDoS attacks, social engineering attacks, and emphasized the criticality of vulnerability analysis and assessment. Regarding technological applications, the utilization of techniques such as access control and identity authentication, data protection and encryption, as well as threat detection and response, provides multiple layers of defense for network security. The prospective exploration of innovative technologies, including artificial intelligence and machine learning, blockchain technology, as well as adaptive defense technology and edge computing security, paints a picture of a more intelligent, efficient, and robust future for network security operations. Overall, the significance of network security operations lies not only in technological challenges but also in safeguarding societal information security.

Acknowledgement

"Chief Technician" of Henan Vocational College of Applied Technology, Project No.: 2020-SXJS-XX05; Education Science, Employment and Entrepreneurship of Henan Education Department: Research on the implementation path of cloud computing technology based on 1 + X certificate system, Project No.: 2021YB0560; 2020-GGJS-X001 Young backbone teacher of Henan Vocational College of Applied Technology, 2023-SXJS-XX02 Chief Technician of Henan Vocational College of Applied Technology.

References

[1] Bai, T. Y. (2023). Application Exploration of Computer Network Security Technology in Network Security Maintenance. Changjiang Information Communication, 36(2), 3.
[2] Jiang, K. (2022). Hidden Dangers and Improvement Strategies of Network Security Operations in China. Wireless Interconnect Technology, 2022(019-003).
[3] Han L. (2019) Computer network operation and security management design. Electronic Technology and Software Engineering (23), 2.
[4] Zhou, Y. B. (2023). Exploration of the Application of Computer Network Security Technology in Network Security Maintenance. Science and Technology Innovation and Productivity, 2023(1), 75-77.
[5] Guo, Y. Q. (2023). Analysis of the Application of Network Security Technology in Network Security Maintenance. Regional Governance, (7), 0137-0140.
[6] Cui, L. (2023). Construction and Application of Wireless Network Security Operation System. Network Security Technology and Application, 2023(3), 2.