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

DOI: 10.23977/jeis.2023.080611
ISSN 2371-9524 Vol. 8 Num. 6

The Application of Information Technology Empowering Management in Cybersecurity Construction for Higher Education

Chengxin Wei

Guangxi University of Chinese Medicine, Nanning, 530200, China

Keywords: Empowering management, information technology, higher education network security, strategic planning, technology training, monitoring and response

Abstract: Network security in higher education holds significant importance in today's era of informatization. This paper aims to explore how to enhance network security in higher education through empowering management with information technology. Firstly, it introduces the challenges and threats faced by network security in higher education and discusses the concept of empowering management through information technology and its application in higher education network security. The paper then presents three key sections, addressing strategic planning, technology, personnel training, monitoring, and response mechanisms in the construction of network security in higher education. Finally, through the analysis of existing cases, it summarizes the significance of empowering management through information technology in the development of network security in higher education and proposes directions for future research.

1. Introduction

With the rapid development of information technology, university networks have become the core infrastructure for education, research, and administration. However, this has been accompanied by a growing wave of network security threats, presenting universities with significant challenges in the form of cyberattacks, data breaches, and malicious software. Consequently, the effective enhancement of network security in higher education has become an urgent task.

Empowering management through information technology is an emerging concept that emphasizes the fusion of management and technology to achieve more efficient network security management. This paper aims to delve into the principles and methods of empowering management through information technology and explore its application in the context of enhancing network security in higher education.

2. Challenges and Threats in Higher Education Network Security

2.1. The Importance of Network Security

The significance of network security in the higher education environment cannot be underestimated. University networks serve as the core infrastructure for education, research, and

management, and the security of these networks is crucial for the normal operation and comprehensive development of universities.

The importance of network security is evident in several aspects. Firstly, university networks serve as a bridge for information exchange among students, faculty, and administrators, encompassing academic research findings, educational resources, and personal data. Leakage or tampering of this information can have a significantly detrimental impact on the reputation and credibility of universities.

Secondly, university networks are essential infrastructure for supporting online education and remote learning, making their stability and security crucial for maintaining educational quality. Network attacks, vulnerabilities, or improper management can lead to interruptions and disruptions in the learning process.

Furthermore, university networks are also the target of hackers, cybercriminals, and other malicious actors. Evolving threats like malware, ransomware, and phishing attacks pose risks of data loss, personal privacy breaches, and financial losses.

The security of university networks is vital, as it not only affects internal university operations but also the quality and continuity of academic research and educational activities. In this context, it is imperative to take the challenges and threats to network security seriously and implement proactive and effective measures to safeguard university networks.[1]

2.2. Challenges in Higher Education Network Security

Higher education network security faces multiple challenges, one of which is the continuous growth of network attack threats. Attackers are becoming increasingly sophisticated, employing various means, such as malicious software, social engineering, ransom attacks, and zero-day vulnerability exploitation, to infiltrate university networks. These attacks may result in data breaches, service interruptions, and substantial economic losses. To address this challenge, universities need to continually upgrade and enhance network security defenses to ensure the protection of network systems from various threats.[2]

Another challenge is the lack of security culture and awareness within higher education institutions. Many network security incidents stem from careless actions by staff or students, such as clicking on malicious links, using weak passwords, or sharing sensitive information. Universities need to strengthen network security training and education to raise awareness of network risks among all members and reduce the risk of internal threats.

Higher education also faces the challenge of increasingly complex network architectures and applications, which add to the complexity of network security. The introduction of new technologies such as mobile devices, cloud computing, and the Internet of Things (IoT) widens the attack surface and makes university networks more susceptible to breaches. To address this challenge, universities need to implement comprehensive security strategies, including device management, network monitoring, vulnerability management, and emergency response.

Moreover, compliance and regulatory requirements are also a challenge for network security in higher education. Universities need to comply with various regulations, such as data protection laws, privacy laws, intellectual property laws, to safeguard personal data and intellectual property. This necessitates the establishment of compliance frameworks and systems to ensure the legality and security of university networks.[3]

Higher education network security faces challenges from evolving threats, internal security culture issues, complex network architectures, and compliance with regulations. Universities need to implement comprehensive network security measures to address these challenges and protect their information and network resources while maintaining the continuity and quality of education and

research.

2.3. Threats in Higher Education Network Security

Higher education network security faces a diverse and complex array of threats in today's digital environment. Here is a detailed analysis of some of the key threats:

2.3.1. Malware and Virus Attacks

Malware and viruses are common threats to higher education network security. Attackers can spread these malicious codes through email attachments, malicious downloads, or infecting network servers. Once infected, malware can steal data, compromise systems, encrypt files for ransom, or serve as a launching point for attacks spreading across the network.

2.3.2. Ransomware Attacks

Ransomware is a popular network threat, where attackers threaten higher education institutions by encrypting the victim's data and demanding a ransom. This can result in data loss and service interruptions, significantly impacting academic and administrative activities.

2.3.3. Social Engineering Attacks

Social engineering attacks exploit deception and fraud in an attempt to gain sensitive information, such as usernames, passwords, and access privileges. Attackers may impersonate internal university personnel and use deceptive tactics to obtain information, facilitating larger-scale attacks.

2.3.4. Zero-Day Vulnerability Exploitation

Zero-day vulnerabilities are security flaws that have not yet been patched. Attackers may exploit these vulnerabilities to infiltrate university networks. Such attacks typically require a high level of expertise and can lead to severe security vulnerabilities.

2.3.5. Internal Threats

Internal staff or students can pose network security threats by accidentally or intentionally disclosing sensitive information, abusing privileges, or engaging in malicious activities. Universities need to establish monitoring and response mechanisms and enhance network security awareness training for staff and students.

2.3.6. Internet of Things (IoT) Security Issues

The proliferation of IoT devices in higher education institutions often lacks adequate security measures. Attackers may compromise IoT devices, gaining access to university networks, potentially introducing vulnerabilities and risks.[4]

Higher education network security faces multiple threats, including malware, viruses, ransomware, social engineering, zero-day vulnerabilities, internal threats, and IoT devices. These threats can result in data breaches, service interruptions, reputation damage, and financial losses. As a result, universities need to adopt comprehensive network security strategies encompassing prevention, detection, response, and recovery measures to effectively mitigate these threats.[5]

3. Application of Empowering Management through Information Technology in Higher Education Network Security

3.1. Concept of Empowering Management through Information Technology

Empowering management through information technology is a comprehensive management approach that integrates information technology with management practices to enhance the efficiency of network security in higher education. This concept emphasizes the following key elements:

Empowering management through information technology views network security as a comprehensive task, encompassing not only the technical aspects but also management, policies, organization, personnel, and processes. By integrating these elements, universities build a comprehensive network security management system to address complex and ever-changing network threats.[6]

Data-driven decision-making is a crucial feature of empowering management through information technology. Universities can more accurately identify potential threats, assess risks, and formulate effective network security strategies through data analysis, monitoring, and evaluation of network activities. This helps universities make fact-based decisions to enhance network security levels.

Furthermore, empowering management through information technology emphasizes the continuous improvement of network security. Universities should establish a culture of continuous learning, adapt to emerging threats and technological trends, and improve network security strategies and practices to maintain the effectiveness and adaptability of network security.

Lastly, compliance and governance are key components of empowering management through information technology. Universities need to ensure that network security policies align with regulatory and standard requirements while establishing effective governance structures to ensure the transparency and effectiveness of network security. These concepts together form the theoretical framework of empowering management through information technology, providing universities with a comprehensive, data-driven, continuously improving, and compliant governance approach to address evolving network security challenges.

3.2. Advantages of Empowering Management through Information Technology

The application of empowering management through information technology in higher education network security offers multiple advantages:

3.2.1. Comprehensive Solution

Empowering management through information technology provides a comprehensive network security management approach that covers various aspects, including technology, management, and personnel training. This helps universities address a wide range of threats comprehensively, rather than focusing solely on specific technical vulnerabilities or attack methods.

3.2.2. Data-Driven Decision-Making

Through data analysis and monitoring, empowering management through information technology can help universities more accurately identify potential threats, take proactive measures, and reduce network security risks. Data-driven approaches enable timely responses to potential network security issues, thus reducing potential losses.

3.2.3. Continuous Improvement and Learning

Empowering management through information technology encourages universities to establish a learning organization that continuously improves and adapts to the evolving threat landscape. This ensures that network security strategies and practices remain aligned with the changing threat environment, maintaining the sustainability of network security.

3.2.4. Compliance and Governance

This concept emphasizes the importance of compliance and governance. Universities need to establish robust network security policies, processes, and audit mechanisms to ensure that network security aligns with regulatory and standard requirements. Effective governance structures help supervise and manage network security, enhancing the credibility of universities' network security. The application of empowering management through information technology in higher education network security provides a comprehensive, data-driven, continuously improving, and compliant governance network security solution. This enables universities to better protect their network environments, reduce potential risks, and enhance the reliability and effectiveness of network security.

3.3. Application Cases of Empowering Management through Information Technology in Higher Education Network Security

In the practical implementation of network security in higher education, empowering management through information technology has been widely applied and has yielded significant results. The following is a brief case illustrating the application of empowering management through information technology in higher education network security. Case: ABC University is a large-scale higher education institution with a substantial student and staff population and a complex and diverse network environment. Faced with the increasing network threats, ABC University adopted the approach of empowering management through information technology to strengthen network security. The application of empowering management through information technology at ABC University includes the following key aspects:

Strengthened Monitoring and Response Mechanisms: The university introduced advanced monitoring tools and a Security Information and Event Management (SIEM) system to track network activities in real-time and detect anomalous behavior. This allows the university's network security team to rapidly identify potential threats and take appropriate actions.

Threat Intelligence Analysis: The university established a threat intelligence team responsible for collecting and analyzing information from various threat intelligence sources. This helps the university better understand threat trends and formulate effective network security defense strategies.

Technical Training and Awareness Enhancement: ABC University conducted extensive training for both staff and students, raising their awareness of network security and improving their skill levels. The training covered best practices in network security, the identification of social engineering attacks, and more.

Emergency Response Plan Development: The university established a robust emergency response plan, outlining response procedures and responsibility assignments for different network security incidents. This helps maintain orderly collaboration during emergency situations. Through the application of empowering management through information technology, ABC University achieved a significant improvement in network security. The time for detecting network security incidents significantly shortened, threat intelligence analysis helped prevent threats in advance, the network security awareness of staff and students significantly increased, and the development of emergency response plans enhanced the university's response capabilities.

This case highlights the crucial role of empowering management through information technology in higher education network security. It not only provides technical tools but also emphasizes the importance of staff training and threat intelligence analysis. Through these comprehensive measures, ABC University better protected its network assets and sensitive data, ensuring the smooth operation of academic and research activities and laying a solid foundation for future development. This case provides valuable insights for other universities to reference and apply.

4. Strategies and Practices for Enhancing Higher Education Network Security

4.1. Strategic Planning and Strategy Formulation

Strategic planning and strategy formulation are crucial steps in ensuring the successful implementation of network security in higher education. This process encompasses several key aspects:

Higher education institutions need to first define the long-term goals and vision for network security, clearly articulating the importance of network security in the institution's operations. This helps provide a clear direction and guidance for subsequent strategy formulation.

Before formulating strategies, higher education institutions need to conduct a comprehensive threat analysis to gain a deep understanding of current network threats and potential risks. This includes identifying potential sources of attacks, attack methods, and potential targets to guide the focus areas of the strategy. Based on goal and threat analysis, institutions should develop comprehensive network security strategies. These strategies should include various measures, such as prevention, detection, response, and recovery, to ensure comprehensive network security. Additionally, the strategies should consider compliance requirements, such as regulations and standards.

Higher education institutions need to establish a clear network security framework, encompassing network security policies, processes, technical measures, and personnel training. This framework should be consistent to support the effective implementation of strategies. Strategic planning also requires resource allocation. Institutions need to specify the budget and resources required for network security to ensure the feasibility and sustainability of the strategy. Higher education institutions should develop network security communication and awareness programs, including awareness training for staff and students. This helps ensure that all members actively participate in network security practices.

Finally, institutions should establish monitoring and evaluation mechanisms to regularly review the execution of network security strategies, make timely adjustments, and improve strategies to address new threats and challenges. This ensures the continuous effectiveness and adaptability of the strategies. By considering these aspects comprehensively, higher education institutions can better formulate and implement network security strategies, ensuring the security of information and resources.

4.2. Technical Training and Capacity Building

Technical training and capacity building are essential for higher education network security. This practice encompasses various aspects, including:

In terms of all-staff training, institutions should develop comprehensive training plans to ensure that all staff possess the necessary network security knowledge and skills. This includes training courses at different levels and in various professional fields to meet the needs of different staff members.

Technical training is not just about imparting technical knowledge but also about raising staff

awareness of network security. Staff members need to understand network threats, best practices, password management, social engineering attack recognition, and more to increase their vigilance and behaviors in network security.

Network security teams and technical experts also need to continuously enhance their technical skills. To do so, institutions should provide in-depth technical training, including courses in advanced technical areas such as network defense, intrusion detection, malware analysis, vulnerability management, and more.

Training programs should not be limited to theoretical knowledge but should also include practical experience and simulated exercises. Institutions can organize network security drills to test the team's emergency response capabilities and improve methods for responding to threats.

To adapt and learn continually in the face of evolving network security threats, institutions should encourage the development of a learning organizational culture. This includes regularly updating training plans, tracking technological trends, and encouraging staff to actively engage in the network security community, collaborate with other experts and organizations, and share knowledge and experiences. By considering the above aspects comprehensively, institutions can establish a robust technical training and capacity-building system, enhancing the preparedness and responsiveness of staff and technical teams in network security. This helps reduce network security vulnerabilities and potential risks for higher education institutions.

4.3. Establishing Monitoring and Response Mechanisms

Establishing effective monitoring and response mechanisms is critical for network security in higher education. This practice covers several key aspects to ensure the continuity and timely response to threats.

In terms of monitoring network activities, higher education institutions should establish continuous mechanisms to detect any possible anomalies or suspicious behavior. This includes using advanced Security Information and Event Management (SIEM) systems to collect, analyze, and report events and log data related to network security in real time. By monitoring network traffic, access patterns, and system behaviors, potential threats can be quickly identified.

Real-time alerting and notification systems are crucial for timely responses to network security events. Institutions need to ensure that security teams and key stakeholders receive alert notifications immediately when security events occur. This helps take prompt actions to minimize potential losses. Through automated alerts and notifications, response speed and efficiency can be improved.

Actively obtaining and analyzing threat intelligence is an important step in predicting and preparing for network threats. Institutions should establish threat intelligence analysis teams responsible for monitoring and analyzing intelligence information from various sources to understand current threats and attack trends. This allows institutions to better identify potential risks, formulate corresponding defense strategies, and take preventive measures to reduce the impact of threats.

Establishing response procedures is crucial to ensure network security. Higher education institutions should clearly categorize security events, define response processes, and coordinate responses in case of emergencies. This includes designating responsible individuals, specifying communication channels, and establishing coordination mechanisms to ensure timely information sharing and decision-making.

In summary, establishing monitoring and response mechanisms is a critical element of network security for higher education. Through continuous monitoring, real-time alerts, threat intelligence analysis, and response procedures, institutions can better respond to network security events, promptly identify and address potential threats, and reduce network security risks and potential losses. These practices help improve the level and sustainability of network security in higher education and

protect the security of sensitive data and information assets.

5. Conclusion

This paper, through an analysis of the challenges and threats faced by higher education institutions in terms of network security, as well as the concepts and advantages of empowered management informatics, emphasizes the importance of empowered management informatics in the construction of network security for higher education. In summary, empowered management informatics is an effective approach to enhance the level of network security in higher education, and institutions should actively embrace this concept, continually improve their network security systems, and ensure the sustainable development of academic research and educational activities. Future research can delve deeper into the specific application methods of empowered management informatics in network security for higher education and continuously enhance network security strategies to adapt to evolving threats and technological environments.

References

[1] Zhou, L., & Zhu, S. M. (2020). Practice and Reflection on the Construction of Network Information Security System in Higher Education. Journal of Shenzhen University (Science and Engineering), 37(S1), 73-77.
[2] Zhu, S. C. (2020). Exploration and Thinking on the Construction of Network Security in Higher Education. Computer and Telecommunications, 2020(Z1), 49-53.
[3] Ha, L., & Zhang, H. (2020). Reflection on the Construction of Network Security in Higher Education. Fujian Computer, 36(01), 46-47.
[4] Ding, F. L. (2023). Empowering School Educational Reform in the Context of Digital Transformation. School Principal, 2023(08), 19-22.
[5] Yang, K. P., & Li, W. F. (2022). Research on Computer Network Information Security in Higher Education Based on Artificial Intelligence. Changjiang Information and Communication, 35(09), 137-139.
[6] Gong, P. (2022). Higher Education Network Information Security and Protection in the Context of Big Data. Network Security Technology and Applications, 2022(06), 78-79.