NETWORK SECURITY SOLUTIONS AND INFORMATION SECURITY AT VIETNAM UNIVERSITIES IN THE DIGITAL AGE

Bui Van Nam[*], Nguyen Phu Quang

Hanoi Metropolitan University

Abstract: *With the development of information technology in universities in Vietnam today, information network at the campus are more and more important, and gradually become an essential infrastructure for teaching, scientific research, personnel management, finance and international cooperation at the University. However, using the network on campus still has potential risks of cyber attacks. Therefore, ensuring network security and database information security has become the most important issue in the construction and development of the university. In this article, the author presents existing problems in information security and confidentiality at Vietnamese universities and propose measures for cybersecurity and information in the current Digital age.*

Keywords: *Cybersecurity, precautions, information security, university of Vietnam.*

Received 15 June 2021

Revised and accepted for publication 23 August 2021

(*) Email: bvnam@daihocthudo.edu.vn

1. INTRODUCTION

In the current information era, the Internet penetrates into all aspects of human life and production. With the continuous development of the internet, crimes using high technology have arisen, existed and developed rapidly, which seriously threatens network information security. Currently, Universities in Vietnam have applied information technology more often and serves an important role in increasing the management of teaching, scientific research, personnel management, finance and international cooperation. However, universities are also faced with major security risks, such as data leaks, hacker attacks and other problems, Which impact negatively on teaching activities and development of the school. Faced with these issues, the Ministry of Education and Training has issued Decision No.5809/QD-BGDĐT on "Promulgating the Regulation on ensuring information security in information technology application activities of units under the Ministry of Education and Training”. Thereby, higher education institutions need to comprehensively understand the current security situation of the network of current members, build a team of experts on information security and privacy, create a reasonable and confidential security system, improve applications on the network environment, increase security education and awareness about online databases, ensure network and information security among staff, lecturers and students in the university. In this article, the author presents the problems that exist in security and information security at the University of Vietnam and propose measures to the problem of network security and information in the Digital era.

2. BODY

2.1. Threats to Cybersecurity and Information Security in Universities in Vietnam

The issue of safety and security become the main concern of the current university. The rapid rise of technology deployment, security, network security has become a necessity in an effort to adjust the protective measures, either directly or indirectly, to prevent the system from attacks on the network environment. However, even if the network has installed anti-virus and firewall, it is difficult to prevent hackers stealing, forgery, destruction and other attacks on the data or information of the server. Additionally, staff, faculty and college students inadvertently access sites that are not secure or inadvertently downloaded software can’t be determined hackers uploaded with embedded viruses on them, making the whole the campus network at risk.

- There are two main reasons why hackers like to attack university networks:

• First, the information and data resources in the University are very large, and the value is relatively high. For this reason, some hackers do not break the media networks, and try to use all sorts of loopholes in the university's network to steal illegal and destructive;

• Second, the protective measures of network security universities relatively slow, along with the campus network. Network architecture and user mode is adopted basically the same, this makes cybercriminals can infiltrate the different users of the campus network in a similar way.

- In addition, there are many software supports Internet hackers, such as remote access tools, web attack tools, port scanners, overflow tools, network snooping tools, and port redirection tools. Some of these tools are easy to use and highly destructive. As long as people with a little knowledge of the Internet can basically use them. This also makes some students, out of curiosity or self-disclosure, use these hacker software to attack the school's network and application system. In fact, in 2021, the incident of a hacker selling 300,000 personal information of university students in Vietnam was recorded. In addition to student information such as age, name, address and phone number, the data file also contains a variety of information such as bank account, parent ID card, lost link address... Therefore, it can be seen that the campus network of universities is in fact at risk of being attacked by hackers at any time.

2.2. Measures to strengthen network security and information security at universities in Vietnam nowaday

To ensure network security and information security at universities in Vietnam nowaday, the author proposes a number of measures as follows:

2.2.1. Develop a comprehensive information security policy

Many university managers believe that ensuring information security belongs to the technical team. In fact, this has to be a combination of the technical team and the managers. Schools need to develop plans and security solutions network system to respond when an emergency incident occurs. When there is a plan when an emergency occurs with the school's network system, it will proactively prevent and minimize the damage to its system. A network security solutions comprehensive, appropriate to each type of organization is the optimal choice for both operating costs and ensure maximum security.

2.2.2. Improve the technical level of network safety and security of network administrators

With the upgrading of network security issues, is difficult to avoid the existence of security gaps. University network management technology is generally low, hackers can penetrate and attack university networks quite easily.

Along with the strengthening of upgrading of network and information security options in universities, it is necessary to fundamentally improve the technical level of network administrators in universities through technical exchange between the university and security agencies, organizations and enterprises specializing in security systems, security, network security, and professional technology.

2.2.3. Raise awareness of information security for officials, lecturers and students in educational institutions

The implementation of the technical means and set the standards system is the most basic measures to ensure the safety of internal information of the university. How to implement effective security systems in the security system and continuously enhance the safety awareness of all staff, faculty and students is key. Therefore, the importance of university network management is the management of people. On the one hand, it is necessary to strengthen the training of professional skills of the establishment.

On the other hand, network administrator staff needed to increase the security awareness on campus network application of network users. In particular, we need to help develop good online habits and increase cybersecurity awareness, such as changing passwords frequently, setting passwords that are not too simple (like 123456, 123456@oke,...), do not visit malicious websites and unsafe websites at will, patch the system in time, do not download large-scale P2P,do not download and install unknown software at will, do not disclose personal privacy information, etc. In addition, they should be especially reminded to data and important information in your computer or network equipment, data backup must be done well, otherwise, once encountered network status suddenly lost the data will lead to unimaginable consequences are.

2.2.4. Developing measures to enhance network security and information security database

Through the previous introduction, the author realized that it is necessary to build network and information security measures to strengthen network security and database information security in universities. However, the development of preventive measures should be combined with network security technologies available today. At present, general network security technology means mainly including network infrastructure virtualization technology, access control technology, intrusion detection technology, artificial intelligence technology, firewall technology.

• **The network infrastructure virtualization**: Virtualization technology infrastructure is to simulate complete physical network infrastructure based on software. Virtualized network infrastructures provide the same features and guarantees as physical networks, they provide the operational and hardware-independent benefits of virtualization - rapid resource allocation, rapid resources, continuous deployment, automated maintenance, and support for both existing and new applications. Virtualization technology introduces network infrastructure equipment and network infrastructure services logic - ports, switches, routers, firewalls, load balancers, VPN and more to connect the blocks work. Virtualization technology introduces network infrastructure equipment and network infrastructure services logic - ports, switches, routers, firewalls, load balancers, VPN and more to connect the blocks work. Applications running on virtualized network infrastructure are similar to running on physical network infrastructure. Users can create highly scalable network infrastructures, bring the level operation more efficient, more flexible, allocate resources more quickly, troubleshooting and cloning, the process of monitoring, QoS (Quality of Service) and security, all supported by part network infrastructure virtualization software.

• **Access control technology**: The main purpose of access control technology is to prevent unauthorized access to any resources and to ensure that the operation and use of external computer systems is within the legal scope. Access control technology through the network authorization mechanism, through different authorizations for different campus network users, to restrict or prohibit unauthorized users from accessing.

• **Intrusion detection technology**: Intrusion Detection technology analyzes actions, security logs, data audits, or other information available on the network to try to understand the hacker's intent and purpose of intrusion. Intrusion detection technology is a type of technology designed and configured to ensure the security of the system computer that can detect and report unauthorized or unusual phenomena in the system in a timely manner. It is a technology used to detect violations of security policy in the computer network. Through this technology, it can discover the intention of the attacker attack and timely attack mode, and the corresponding measures to prevent attacks.

• **Artificial intelligence technology**: As the number and complexity of cyberattacks continues to increase, artificial intelligence (AI) has begun to help under-resourced security operations analysts learn about threats early on. threat and quick response. It can do everything faster and more accurately with large amounts of data which is time consuming for humans. AI can automatically use the tool complex pattern recognition to identify the signs of a malicious program.Although it is not omnipotent and can't identify all the threats, but it's an essential tool to help reduce the amount of time that IT professionals need to investigate warnings.

• **Firewall technology**: A firewall is a type of technical measures to protect the security of computer networks. It can be used as a barrier between the internal network of the campus and external network security, to prevent the intrusion of the outside world. It can manage the user access to the network of the campus, on the other hand, it can scan the data packets entering the network on campus, so it can effectively prevent the attack and the virus entry.

3. CONCLUSION

In the information age, cybersecurity and information security Security has been entering every corner of social life and has gradually become an important part of each organization and individual. In the process of network management on campus, to build a secure system and network security systems on campus stability. It is necessary to conduct real-time monitoring and analysis of network activities on the network environment, promptly detect abnormal network activities, and continuously update and develop new network security solutions on the strategy. management technology and management technology, to gradually improve the school's network security system.

Develop a plan to plan and promote the technical level of network management staff, increase the security awareness of network users in universities, and prevent and mitigate any illegal access , operate and use through network technical means and management methods as much as possible, minimizing unsafe factors to a minimum to help build and develop technological information at university in Vietnam.

REFERENCES

1. Narayana, I.N.C.S., Gopinath, G., Mogan, K.P.C. et al. (2014), "A multilevel thrust filtration defending mechanism against DDoS attacks in cloud computing environment", *International Journal of Grid and Utility Computing*, Vol. 5, No. 4, pp.236–248.
2. Naser, S., Kamil, S. and Thomas, N. (2015), "A case study in inspecting the cost of security in cloud computing", *Electronic Notes in Theoretical Computer Science*, Vol. 318, No. 11, pp.179–196.
3. Stuttard D, PintoM (2012), *The web application hacker's handbook*, 2nd Ed, ISBN-13: 978-1118026472, ISBN-10: 1118026470.
4. Thomson, G. (2012), "BYOD: Enabling the chaos", *Network Security*, 2012(2), pp.5–8, DOI:10.1016/S1353- 4858(12)70013-2.
5. Vance, A., Siponen, M., & Pahnila, S. (2012), "Motivating IS security compliance: Insights from habit and protection motivation theory", *Information & Management*, 49(3-4), 190–198, DOI:10.1016/j.im.2012.04.002.

GIẢI PHÁP AN NINH MẠNG VÀ BẢO MẬT THÔNG TIN TẠI CÁC TRƯỜNG ĐẠI HỌC VIỆT NAM TRONG KỶ NGUYÊN THÔNG TIN

Tóm tắt. *Với sự phát triển của công nghệ thông tin trong các trường đại học tại Việt Nam hiện nay, mạng lưới thông tin tại khuôn viên trường ngày càng có vai trò quan trọng hơn, và dần trở thành cơ sở hạ tầng quan trọng cho việc giảng dạy, nghiên cứu khoa học, quản lý nhân sự, tài chính và hợp tác quốc tế tại các trường Đại học. Tuy nhiên, còn tiềm ẩn những nguy cơ rủi ro bị tấn công không gian mạng. Vì vậy việc đảm bảo an ninh mạng và bảo mật thông tin cơ sở dữ liệu đã trở thành vấn đề quan trọng nhất trong việc xây dựng và phát triển đại học. Trong bài viết này, tác giả trình bày các vấn đề tồn tại trong vấn đề an ninh và bảo mật thông tin tại các trường Đại học Việt Nam và đề xuất các các biện pháp cho vấn đề an ninh mạng và thông tin trong kỷ nguyên thông tin hiện nay.*

Từ khoá: *An ninh mạng, biện pháp phòng ngừa, Bảo mật thông tin, Đại học Việt Nam.*