 DOI: https://doi.org/10.12349/iser.v5i6.2958

Research and Analysis of Computer Network Security in Higher Vocational Colleges

Limin Zhu

Jilin General Aviation Vocational and Technical College, Jilin, Jilin, 132011, China

Abstract

Computer network security in higher vocational colleges is the basis and premise of carrying out education, teaching and scientific research work. The network architecture is open. Although relying on the Internet can greatly improve the daily work, study and life of college teachers and students, the various network security problems it faces can not be ignored. Universities as an important place to cultivate talents, must give enough attention to network security management, in the daily management and technical level, ensure the implementation of data encryption processing measures, strengthen the network monitoring, strengthen teachers and students awareness of network security risks, strengthen the construction of security system, strengthen the construction of infrastructure, strengthen the cultivation of network security, to ensure the network security of colleges and universities. Based on this, this paper analyzes and studies the problem of computer network security in higher vocational colleges.

Keywords

higher vocational college; computer network security; research; analysis

高职院校计算机网络安全研究与分析

朱立民

吉林通用航空职业技术学院，中国 · 吉林 吉林 132011

摘　要

高职院校计算机网络安全是开展教育、教学和科研工作的基础和前提。网络架构是开放的，虽然依托互联网可以极大地改善高校师生的日常工作、学习和生活，但是它所面临的各种网络安全问题也不容忽视。高校作为培养人才的重要地方，必须对网络安全管理给予足够的重视，在日常管理和技术层面上，保证数据加密处理措施的落实，加强网络监控，增强老师和学生对网络安全风险的防范意识，加强安全系统的建设，加强基础设施的建设，加强对网络安全方面的人才的培养，确保高校的网络安全。基于此，论文针对高职院校计算机网络安全问题进行分析与研究。

关键词

高职院校；计算机网络安全；研究；分析

1 高职院校计算机网络安全内容分析

随着新时代的来临，计算机技术已广泛应用于各个领域，彰显了信息资源的价值。尤其是随着网络技术的发展与普及，信息资源成为了社会经济发展中至关重要的组成部分，对高职院校的现代化建设起到了积极的推动作用。为了确保自身信息数据的安全性和可靠性，必须加强对高职院校计算机网络信息的保护，以确保其能够受到有效的管理。

2 高职院校计算机网络安全问题分析

2.1 计算机系统存在漏洞

这些漏洞可能源于系统设计时的缺陷、软件编码的错误，或是后期维护不当等原因。漏洞的存在使得黑客或恶意用户有机会利用这些弱点，对系统进行非法访问、数据窃取或破坏。它们为黑客提供了可乘之机，黑客可以通过利用这些漏洞，轻易地绕过系统的安全防护措施，进而获取敏感信息或执行恶意操作。漏洞可能导致数据的泄露或篡改，对个人隐私和高校商业机密构成严重威胁。漏洞还可能被用于发起拒绝服务攻击，导致系统崩溃或无法正常运行，从而对社会经济秩序造成破坏。

2.2 黑客与网络病毒攻击

黑客是指那些利用计算机和网络技术非法侵入他人计算机系统，窃取、篡改或破坏数据的行为者。而网络病毒则是一种能够自我复制、传播的恶意程序，它可以在计算机系统中潜伏，等待时机发作，对系统造成破坏。黑客攻击带来的坏处是巨大的。黑客可能利用系统漏洞或社交工程手段，窃取用户的敏感信息，如银行账号、密码等，进而实施金融诈骗或其他非法活动。黑客还可能对关键基础设施进行攻击，如电力、交通等系统，导致社会运行受阻，甚至引发严

【作者简介】朱立民（1974–），男，中国吉林吉林人，本科，讲师，从事网络技术、网络安全研究。

重的安全事故。网络病毒可以在计算机之间快速传播，感染大量设备，导致系统性能下降、数据丢失甚至系统崩溃。一些病毒还可能携带恶意负载，如勒索软件，对用户数据进行加密并索要赎金。

2.3 计算机网络操作人员操作不当

随着信息时代的到来，互联网技术已逐渐应用于人们生活和工作中。然而，由于部分用户缺乏专业技能知识和操作经验等原因，使得其在使用计算机网络时出现了一系列问题。如：部分用户在使用计算机网络时过于依赖网上银行、网上购物等应用软件及游戏软件等，其在使用过程中所选择的应用软件和游戏软件都是存在安全漏洞的。此外，部分用户在进行数据操作时不注意操作规范或不当操作等原因也会导致计算机网络系统受到攻击和破坏。

2.4 安全对策缺乏统一标准

高校计算机网络防护系统的陈旧也是一个亟待解决的问题。由于技术的迅猛发展和网络威胁形势的不断演变，传统的网络安全防护手段往往难以应对新型的网络攻击和安全威胁。传统的防火墙、入侵监测系统等安全设备已经显得力不从心，无法有效应对大规模的网络攻击、高级持续性威胁（APT）。此外，高速计算机网络规模庞大，网络流量巨大，对网络安全设备的性能和扩展性也提出了更高的要求。

3 高职院校计算机网络安全技术

3.1 计算机网络安全防御技术

物联网、大数据、云计算是即将到来的人工智能时代的必然趋势。人工智能的发展依赖于数据、算法和计算能力。其中，数据是基础，算法是主体，计算能力是核心。首先，必须有准确的数据，因为数据是人工智能的基础。如果数据源错误或数据源被污染，则使用算法对数据进行分析，这将大大降低算法的准确性。其次，为了在当前计算量下获得最佳结果，需要在获得准确的数据后对算法进行优化。最后，要提高计算能力，理论上，计算能力越强，功能越强大。在这个人工智能时代，攻击者可以攻击数据、算法或设备，这些都是攻击中的通配符。因此，在这个人工智能时代，人们需要考虑的不再是技术对抗，而是各种复杂的攻击方式来解决问题，有必要建立一个完整的网络安全防护体系。

3.2 网络系统安全监控技术

随着大数据技术的发展，互联网上各类信息变得越来越复杂。但是，为了增强高校计算机网络的安全性，进一步促进计算机的使用，必须加强对网络的维护，以确保网络的良好运行。从高速计算机网络系统的安全监控入手，可以增强政府和相关单位的参与，从而达到净化网络环境的目的。新的监控技术可以分析网络中的数据，识别潜在的安全风险，并打击网络犯罪。简而言之，需要加快高校计算机网络环境的净化，使人们更容易接触到计算机和其他高科技服务。

3.3 网络防火墙技术

高校计算机网络防火墙是一种经常采用的技术手段，其设计需要考虑系统安全性和实用性两个方面的因素。除了能有效地防御各类病毒和木马入侵，通过持续的更新还可以提升防护性能。另外，防火墙具有安装简便、推广容易和操作便捷等优点，因此受到了广大用户的认可和接受。目前，在中国大多数高校中都采取了基于防火墙的安全策略。该款防火墙不仅具有相对较低的成本，同时还具备广泛的应用潜力。它能够监视、分析和限制数据流，并在需要时采取适当的防护措施，以确保网络的安全。在互联网上，经常有一些病毒或恶意代码通过多种途径侵入系统内，导致系统无法正常运行。许多用户对个人信息安全的保护了解不够深入。当用户下载此类软件时，病毒可能会入侵计算机，给其正常工作带来潜在的风险。

4 高职院校计算机网络安全防护策略

4.1 建立健全的网络安全防护策略

为有效应对信息化背景下的高校计算机网络安全威胁，除了采用先进的网络安全技术外，还需要建立健全的防护策略，包括多层防御体系建设、安全意识教育与培训、安全漏洞管理与应急响应、合规性与法律法规遵循等方面。多层防御体系建设是指在网络安全防护中采用多种技术手段和措施，从不同层面、不同方向对高校计算机网络安全进行全方位的保护。

常见的多层防御措施包括网络边界防火墙、入侵检测与防御系统（IDS/IPS）、安全网关、终端安全软件等，通过防火墙、入侵检测系统等技术设备对外部威胁进行防护，通过安全策略、权限管理等措施对内部威胁进行防范，形成密不透风的网络安全防护体系。安全意识教育与培训是提高网络用户对安全问题的认识和防范能力的重要途径，可以帮助用户了解常见的网络安全威胁和防范措施，增强他们的安全意识和自我保护意识。安全意识教育与培训内容包括网络安全政策、安全风险认知、安全操作技巧等，可以通过培训课程、宣传教育、安全演练等方式进行开展，全员参与，持续推进。

安全漏洞管理与应急响应是及时发现和处理网络系统中存在的安全漏洞和安全事件，减少安全漏洞对系统安全性的影响，降低安全事件的损失和影响。安全漏洞管理包括漏洞扫描、漏洞修补、安全补丁管理等活动，可以通过自动化工具和人工审核相结合的方式进行；应急响应则是在安全事件发生后迅速采取措施，阻止事件扩大化，减少损失。合规性与法律法规遵循是指高校计算机网络安全工作必须符合相关法律法规和政策要求，保障网络安全工作的合法合规性。

4.2 定期更新操作系统和软件

高职院校需要定期更新操作系统和软件，及时修复漏

洞，是保护计算机网络安全的重要措施。通过更新，可以获得最新的安全补丁和功能改进，提升系统的安全防护能力。这些补丁通常包括修复已知漏洞的代码，增强系统的稳定性和安全性。新版本的软件还可能引入更先进的安全机制，如更强大的加密技术或更智能的威胁检测功能，从而进一步提升高职院校网络安全防护水平。定期更新还有助于防止恶意软件的利用。恶意软件往往利用过时的系统或软件漏洞进行传播和攻击。通过保持系统和软件的最新状态，可以降低高职院校计算机网络被感染的风险，保护计算机免受恶意软件的侵害。更新操作也需要谨慎处理。在更新前，确保备份重要数据，以防万一更新过程中出现问题导致数据丢失。还应选择可信赖的更新源，避免下载和安装来自不明来源的更新文件，以免引入新的安全风险。

4.3 防火墙和入侵检测系统

防火墙作为网络安全的第一道关口，其主要功能是监控和控制进出网络的数据包。通过设定安全规则，防火墙能够阻止未经授权的访问和恶意软件的传播，从而保护内部网络免受外部威胁。现代防火墙不仅具备基本的包过滤功能，还融入了状态监测、应用层网关等先进技术，以应对日益复杂的网络攻击。入侵检测系统则是对防火墙的重要补充。它能够实时监测网络流量和系统行为，一旦发现异常或可疑活动，便会立即发出警报并采取相应的防御措施。入侵检测系统通过收集和分析各种日志信息、网络流量数据等，能够发现潜在的安全威胁，如未授权的访问、恶意软件的植入等。通过与防火墙的协同工作，高职院校计算机网络入侵检测系统能够进一步提高网络的安全防护能力。在部署防火墙和入侵检测系统时，需要根据网络环境的实际情况和安全需求进行合理配置。例如，可以根据业务需求和风险评估结果，设定不同的安全策略和访问控制规则；高职院校还需要定期更新和升级防火墙和入侵检测系统的软件和数据库。

5 结语

高职院校计算机网络安全与防护策略的研究与实践，是一项长期而艰巨的任务。需要不断创新技术手段，完善防护策略，提高应对能力，以应对日益复杂的网络安全威胁。够构建更加安全、可靠、高效的计算机网络环境，为人类的进步与发展提供坚实的保障。

参考文献

[1] 陈晓镕.计算机网络病毒与计算机网络安全防范的研究[J].网络安全技术与应用,2021(6):2.

[2] 刘昱红.计算机网络安全与计算机病毒防范措施研究[J].中国新通信,2020(8).

[3] 陈明.高职院校计算机网络安全技术概述[J].计算机技术与发展,2020,15(3):21-25.

[4] 李晓宇,王伟.高职院校网络安全技术的发展与应用[J].信息安全与通信保密,2019,10(2):45-50.

[5] 张磊,赵小虎.深度学习在高职院校网络安全中的应用研究[J].计算机科学与技术,2018,20(4):60-65.