高校网络安全建设体系研究
——以武汉轻工大学为例

肖志雄

（武汉轻工大学，湖北 武汉 430023）

摘要：本文基于高校网络安全的发展趋势，通过分析武汉轻工大学网络安全体系建设现状，总结出高校网络安全建设面临的挑战与痛点。并对网络安全建设体系理论加以研究，明确网络安全建设的目标与原则，重点介绍信息安全的CIA模型、PDRR模型和零信任等模型，构建了一套切实可行的高校网络安全建设体系。同时对高校网络安全体系建设过程中普遍存在的问题，提出相应的措施，保障高校教学、科研等工作的顺利开展，也为其他高校的网络安全建设提供有益的借鉴和参考，具有重要的现实意义和实践价值。

关键词：高校网络安全；CIA模型；PDRR模型；零信任模型

一、引言

高校网络承载着海量的教学资源、科研数据、师生个人信息以及学校的各类管理数据，网络安全性直接关系师生的财产安全、高校的业务运转以及学校教育数字化发展。近年来，网络安全事件频发，给学校和师生带来了极大的困扰。教务系统遭受攻击，造成选课混乱、成绩篡改等问题，扰乱教学秩序；信息泄露事件导致师生的生命财产安全受到威胁。这些事件无不凸显当前高校网络安全面临的严峻挑战，也敲响了加强高校网络安全建设的警钟。

武汉轻工大学作为一所具有重要影响力的高等学府，高度重视网络安全建设。积极采取一系列措施加强网络安全防护，构建了较为完善的网络安全建设体系。然而随着网络技术的不断发展和网络安全形势日益复杂，学校在网络安全建设方面仍面临诸多挑战。

二、武汉轻工大学网络安全建设现状

2.1 政策与战略布局

武汉轻工大学严格依据国家相关政策和行业标准，积极构建网络安全战略体系。学校深入贯彻落实《中华人民共和国网络安全法》《网络安全等级保护制度2.0》等法律法规，将网络安全纳入学校整体发展战略规划。学校制定了《2023年度网络安全工作要点》，明确“坚持党建引领网络安全工作，完善学校各二级单位网络安全工作责任制度，实施网络和信息安全综合治理、加强网络安全保障、防范化解网络安全风险，全面提升网络安全管理水平”的总体目标。

2.2 组织与管理架构

学校成立网络安全工作领导小组，筹协调全校网络安全工作，研究制定网络安全政策和重大决策，解决网络安全工作中的重大问题。学校网络与信息中心专门负责网络安全工作，承担全校网络安全的规划、建设、管理和维护并制定网络安全工作计划和管理制度。中心下设信息安全部、网络运维部等多个部门，各部门人员岗位职责明确，分工协作。中心配备了专业的网络安全技术人员，形成了一支结构合理、素质过硬的网络安全管理团队。

2.3 技术设施建设

为了提升网络安全防护能力，武汉轻工大学部署了一系列先进的网络安全设备。高性能防火墙对进出校园网络的流量进行实时监控和过滤，有效阻止外部非法网络访问和攻击；入侵检测系统（IDS）和入侵防御系统（IPS），能够及时发现并防范网络入侵行为，如端口扫描、漏洞攻击等；网络安全态势感知平台，通过对网络流量、系统日志、安全事件等数据的采集和分析，实时掌握校园网络的安全状况，及时发现潜在的安全威胁；漏洞扫描系统，定期对校内信息系统和网络设备进行漏洞检测，及时发现并修复安全漏洞，降低安全风险。

为了保障数据安全，学校建立了数据备份与恢复系统，定期对关键数据进行备份，并制定了完善的数据恢复策略，确保在数据丢失或损坏的情况下能够及时恢复，保障业务的连续性。为了维护学校数据中心机房的稳定运行，学校建有大功率柴油发电机，确保在紧急情况下机房设备的正常工作，校园业务不中断。

2.4 人才培养与团队建设

学校高度重视网络安全人才培养，通过多种途径提升师生的网络安全意识和技能。网络与信息中心的技术人员定期开展内部培训和技术交流活动，不断提升自身的技术水平和业务能力。同时积极参加省教育厅组织的网络安全培训，如教育系统网络安全保障专业人员（ECSP）等专业培训，打造一支技术过硬的网络安全管理团队。

三、高校网络安全建设面临的挑战与问题

3.1 外部网络威胁形势严峻

在数字化时代，网络攻击手段日益多样化和复杂化，给高校的网络安全防护带来了巨大挑战。

黑客攻击是最为常见的外部威胁之一。黑客常常利用系统漏洞、弱密码等薄弱环节，通过端口扫描、暴力破解等方式进行攻击，入侵学校的网络系统，窃取敏感信息、篡改数据或破坏网络服务。某高校曾遭受黑客攻击，导致其教务系统瘫痪，学生成绩数据被篡改，严重影响教学秩序。

恶意软件传播也是外部网络威胁的重要形式。病毒、木马、蠕虫等恶意软件通过网络传播，感染学校的计算机和服务器，窃取用户信息、控制设备或进行其他恶意活动。如一种名为“WannaCry”的勒索病毒，会加密用户的文件，并要求用户支付赎金才能解密。

网络钓鱼也是不容忽视的威胁。攻击者通过发送虚假的电子邮件、短信或即时通讯消息，诱使用户点击链接或提供个人信息，如账号、密码、身份证号等。这些信息一旦被获取，攻击者就可以利用它们进行进一步的攻击或诈骗活动。高校师生由于社会经验不足，往往容易成为网络钓鱼的目标。

3.2 技术更新与维护难题

网络安全技术的快速发展和更新迭代，给高校的网络安全建设带来了诸多难题。

一方面，学校需要不断跟进最新的网络安全技术，以应对日益复杂的安全威胁。需要投入大量的资金和人力，购买先进的安全设备、软件授权，聘请专业的技术人员进行技术培训和系统维护。另一方面，技术更新还带来系统兼容性和稳定性的问题。随着学校网络环境的不断变化和升级，新引入的安全技术和设备可能与现有系统不兼容，导致系统运行不稳定。此外，网络安全运维也

是一项常态化的任务。安全设备和软件需要定期进行更新、升级和维护，以修复漏洞、增强防护能力。高校的网络安全技术人员数量有限，难以对所有设备和软件进行及时有效的维护，存在网络安全风险。

3.3 安全与发展的平衡困境

在推进数字化建设的过程中，高校面临着如何平衡网络安全与业务发展的困境。

随着学校信息化程度的不断提高，各类数字化业务不断涌现，如在线教学、科研协作平台、智能校园管理系统等。这些业务的发展极大地提高了学校的教学、科研和管理效率，但同时也带来了更多的网络安全风险。为了保障业务的正常运行，学校需要在网络安全方面投入更多的资源，加强安全防护措施。然而，过于严格的网络访问控制策略可能会影响校外师生对某些教学资源和科研数据的获取，降低工作效率。

四、高校网络安全建设体系的理论探索

4.1 网络安全建设的目标和原则

高校网络安全建设的总体目标是构建一个全方位、多层次、动态发展的网络安全防护体系，确保校园网络的机密性、完整性、可用性、可控性和可审查性，为学校的教学、科研、管理等各项工作提供安全、稳定、可靠的网络环境。

机密性要求防止未经授权的访问和数据泄露，确保教学资料、科研数据、师生个人信息等敏感数据的保密性；完整性要求保证数据在传输、存储和处理过程中不被篡改、破坏或丢失；可用性是指网络系统和服务能够随时正常运行，满足师生的使用需求；可控性强调对网络活动和信息的有效控制，确保网络行为符合法律法规和学校的规章制度。学校可以通过网络访问控制策略，限制师生对某些非法或不良网站的访问；可审查性则要求能够对网络操作和事件进行记录和审计，以便在出现安全问题时能够追溯和调查。

为了实现这些目标，高校网络安全建设应遵循以下五个原则：

一是系统性原则。从网络架构设计、安全设备部署，到人员培训、安全策略制定，都要综合考虑，形成一个有机的整体。二是动态性原则。建立动态的安全管理机制，及时跟踪最新的安全技术和威胁情报，定期评估和调整安全策略，确保网络安全防护的有效性。三是预防性原则。采取积极的预防措施，提前识别和消除安全隐患，降低安全事故发生的概率。四是分层防护原则。采用多层次的安全防护体系，对网络进行纵深防御。在网络边界、内部网络、信息系统等不同层面分别部署相应的安全设备和措施，形成多道防线，提高网络的整体安全性。五是最小权限原则。为用户和系统分配最小的操作权限，使其仅能访问和执行其工作所需的资源和功能，减少因权限过大导致的安全风险。

4.2 相关理论基础与模型

网络安全的相关理论模型为高校网络安全建设提供了方向。信息安全的 CIA 模型是最为基础和核心的理论之一。CIA 模型由保密性（Confidentiality）、完整性（Integrity）和可用性（Availability）三个要素组成，这三个要素相互关联、相互制约，共同构成了信息安全的基本框架；PDRR 模型（Protection、Detection、Reaction、Recovery）强调网络安全是一个动态的过程，需要通过防护措施来阻止攻击，通过检测手段及时发现安全威胁，在发现攻击后迅速做出响应，并在遭受破坏后进行恢复；零信任模型也是近年来备受关注的网络安全理念。该模型打破了传统的“信任边界”概念，不再默认内部网络是安全的，而是对所有的访问请求进行严格的身份认证和权限验证，无论访问来自内部还是外部网络。在高校网络中应用零信任模型，可以有效防范内部人员的违规操作和外部攻击者利用内部网络漏洞进行攻击的风险。

五、网络安全建设体系的构建策略

5.1 技术层面的强化措施

升级网络安全设备：高校应加大对网络安全设备的投入，定期评估现有设备的性能和防护能力，及时更新网络安全设备。如升级新一代防火墙，除了访问控制功能，还能实现深度包检测、入侵防御、应用识别等功能，有效应对日益复杂的网络攻击。增加入侵检测系统（IDS）和入侵防御系统（IPS）的数量和覆盖范围，多点部署，实时监测网络流量，及时发现并阻止入侵行为。

结合人工智能技术：积极引入人工智能、大数据等先进技术，提升网络安全防护的智能化水平。如利用人工智能技术对网络安全数据进行分析和挖掘，建立异常行为检测模型，自动识别和预警潜在的安全威胁。借助大数据技术对海量的网络安全日志和事件数据进行存储、分析和处理，快速定位安全事件的根源，为安全决策提供数据支持。

加强网络安全防护体系建设：构建多层次、全方位的网络安全防护体系，实现对校园网络的纵深防御。除了部署边界防火墙，还可以采用反向代理、堡垒机等技术，将校园网络与外部网络进行隔离，确保只有认证后的用户和设备才能访问校内资源。在校园内网实施 VLAN 隔离管理，根据不同的业务需求和安全级别，将网络划分为不同的区域，如教学区、办公区、宿舍区、家属区等，并在各个区域之间设置访问控制策略，限制不同区域之间的网络访问，防止安全风险的扩散。

5.2 管理机制的优化完善

进一步完善网络安全管理制度，明确各部门和人员在网络安全工作中的职责和权限。建立健全网络安全事件应急响应机制，制定应急预案，明确应急响应流程，确保在发生网络安全事件时能够迅速、有效地进行处置；建立全面的安全审计机制，对校园网络中的各类操作和事件进行记录和审计，及时发现潜在的安全问题，追溯安全事件的发生过程，为安全事故的调查和处理提供依据。审计内容应包括用户登录行为、网络访问记录、系统操作记录、数据修改记录等。采用专业的安全审计软件，对审计日志进行实时分析和预警。定期对审计结果进行总结和分析，发现网络安全管理中存在的薄弱环节，及时采取相应措施。

六、结论与展望

本文基于高校网络安全的发展趋势，通过分析武汉轻工大学网络安全体系建设现状，总结出高校网络安全建设面临的挑战与痛点。并对网络安全建设体系理论加以研究，明确网络安全建设的目标与原则，重点介绍信息安全的 CIA 模型、PDRR 模型和零信任等模型，构建了一套切实可行的高校网络安全建设体系。同时对高校网络安全体系建设过程中普遍存在的问题，提出相应的措施，保障高校教学、科研等工作的顺利开展。

未来高校网络安全发展将呈现出技术创新驱动、管理优化协同、人才培养支撑、文化营造助力态势，高校需要不断加强技术创新、优化管理机制、培养专业人才、营造安全文化，才能够有效应对日益复杂的网络安全挑战，为高校的信息化建设和教育数字化转型提供坚实的网络安全保障。

参考文献：

[1] 陈金木，陈峰，郑少朋 . 高校计算机网络信息安全问题及其防范措施研究 [J]. 网络空间安全 ,2023,14(01):85-90.

[2] 程子颢，毛冲 . 等保 2.0 下高校网络安全主动防御体系建设探究 [J]. 网络安全技术与应用 ,2023,(04):96-97.

[3] 郭倩，张桦，何岚岚 . 高校数字校园网络信息安全保障体系建设 [J]. 数字技术与应用 ,2022,40(03):224-227.DOI:10.19695/j.cnki.cn12-1369.2022.03.71.

[4] 陈莹 . 基于网络信息化下的高校网络安全建设 [J]. 网络安全技术与应用 ,2021,(07):93-94.

[5] 李萌昕 . 高校智慧校园建设中的网络安全建设现状与分析——以山东大学为例 [J]. 电脑知识与技术 ,2022,18(07):31-33.DOI:10.14004/j.cnki.ckt.2022.0430.