校园网网络安全治理：挑战与应对策略

者明伟
昆明医科大学　云南　昆明　650500

摘　要：本文在分析当前校园网络安全现状及其主要威胁的基础上，探讨了网络攻击行为模式，并构建了涵盖技术防御、管理机制优化和安全文化培育的三维治理策略体系。通过实证研究，本文验证了该治理策略在提升高校网络安全防护能力方面的有效性，并结合未来技术发展趋势提出改进建议，以期为高校网络安全治理提供理论支撑和实践指导。

关键词：校园网；网络安全治理；三维治理体系

引言

随着信息技术的迅猛发展，校园网络已成为高校教学、科研和行政管理的重要基础设施。然而，数字化进程的加速也带来了日益严峻的网络安全挑战，校园网络正面临多种复杂的安全威胁。

首先，网络攻击手段不断演变，高校面临的高级持续性威胁(APT)、勒索软件攻击和钓鱼攻击攻击等愈发频繁。高校网络系统因其开放性和海量数据存储的特点，成为黑客组织和不法分子的重点攻击目标。其次，数据安全隐患严重，师生个人信息、科研数据和管理系统数据库均可能成为黑客窃取或破坏的对象，而数据外泄更是屡见不鲜，不仅对个人隐私造成危害，而且对学校的声誉造成了很大的危害。此外，内外部安全管理机制尚不完善，部分高校的安全防护技术滞后，管理制度不健全，用户安全意识薄弱，进一步加剧了校园网络的安全风险。

有鉴于此，研究网络安全治理在校园中面临的挑战与应对，是一个战略性的课题，对治理网络安全具

有现实意义。本文将从网络攻击行为模式、校园网安全治理现状及其困境入手，探讨构建三维治理策略体系的必要性，并结合实际案例分析治理成效，以期为高校网络安全防护体系的优化提供参考。

1 校园网络安全治理现状分析

校园网络作为高校教学、科研和管理的重要基础设施，其安全性直接关系到学校的正常运转和社会声誉。然而，当前在校园网络安全治理方面仍存在诸多挑战，主要体现在以下几个方面：

1.1 威胁态势分析

（1）攻击特征演变：

随着网络技术的不断进步，针对校园网的攻击方式变得更加多样化和复杂。传统的病毒、木马等攻击方式仍然存在，同时，勒索软件、钓鱼邮件、高级持续性威胁（APT）等新型攻击手段也频繁出现。这些攻击不仅影响校园网络的正常运行，还可能造成敏感数据泄露，给学校带来严重损失。

（2）系统脆弱性：

校园网络系统的复杂性和高开放性使其更容易受到攻击。许多高校的网络设备和应用系统存在未修补的漏洞，部分自建网站缺乏安全防护措施，增加了被攻击的风险。此外，校园网中大量使用的开源软件，如果管理不善，也可能成为攻击者的突破口。

1.2 治理困境

（1）技术防御滞后：

部分高校在网络安全防护技术的投入和更新等方面相对滞后，缺乏先进的防火墙、入侵检测系统等安全设备，导致校园网络在面对复杂多变的网络攻击时自身的防御能力有所欠缺。此外，对新兴威胁的监测和响应机制不足，导致安全事件难以及时发现和处置。

（2）管理机制缺陷：

校园网络安全管理机制不健全，责任分工不明确，缺乏有效的安全管理制度和应急响应预案。一些高校的信息资产管理不到位，存在资产梳理不清、备案不及时等问题，增加了安全管理的难度。

（3）用户安全素养：

师生的网络安全意识普遍不足，缺少必要的安全防护知识。例如，使用弱密码、随意点击不明链接、下载未知来源的软件等行为，容易导致个人信息泄露或设备被感染，进而影响整个校园网络的安全。

综上所述，校园网络安全治理现状不容乐观，需要从技术防御、管理机制和用户教育等多个方面进行改

基金项目：昆明医科大学2023年宣传思想文化立项课题项目（编号：X12110001304）

作者简介：者明伟（1983.09-），男，云南玉溪人，硕士研究生，工程师，研究方向：网络安全、计算机网络通信。

进，以提升整体安全水平，保障校园网络的健康运行。

2 网络攻击行为模式分析

2.1 攻击生命周期模型

网络攻击生命周期模型描述了攻击者从最初的侦查到最终达成攻击目标的整个过程。其中，洛克希德·马丁公司提出的“网络杀伤链”（Cyber Kill Chain）模型是常见的代表之一，该模型将网络攻击划分为以下七个阶段：

侦查阶段：攻击者对目标网络进行信息收集，以寻找潜在漏洞和可利用的入侵点。包括域名、IP地址、员工信息等关键数据。

武器化阶段：根据收集到的信息，攻击者开发或定制恶意软件或攻击工具，以便在后续攻击过程中加以利用。

交付阶段：攻击者将恶意代码传递给目标，常用的方法包括钓鱼邮件、恶意链接、受感染的附件等。

利用阶段：恶意代码在目标系统上执行，利用系统或应用程序的漏洞，取得初步控制权。

安装阶段：攻击者在目标系统中植入后门或其他恶意软件，以维持对系统的长期控制和持续访问权限。

命令与控制阶段：攻击者通过已建立的通信渠道，远程控制受感染的系统，执行进一步的操作。

目标达成阶段：攻击者实现其最终目的，如窃取数据、破坏系统或传播恶意软件。

2.2 典型攻击场景建模

为了更好地理解攻击者的策略和手段，以下是一个典型的高级持续性威胁（APT）攻击场景：

背景：某大学科研部门存储了大量敏感资料，引起了攻击者的重视。攻击者攻击步骤如下：

侦查：攻击者收集科研部门的公开信息，包括研究项目、人员名单和联系方式。

武器化：基于收集的信息，攻击者制作了包含恶意宏的假冒科研合作邀请文档。

交付：攻击者将假冒的邀请文档通过钓鱼邮件发送给目标研究人员。

利用：研究人员打开文档，启用宏功能，导致恶意代码在其计算机上执行。

安装：恶意代码在受感染计算机上安装后门程序，允许攻击者远程访问。

命令与控制：攻击者通过后门与受感染计算机建立通信，进一步探查内部网络结构。

横向移动：攻击者利用受感染计算机作为跳板，尝试获取更高权限并访问其他关键系统。

数据窃取：攻击者定位并窃取敏感科研数据，通过加密通道将数据传输至外部服务器。

3 三维治理策略体系

为有效应对校园网络安全挑战，构建涵盖技术防御、管理机制优化和安全文化培育的三维治理策略体系。该体系依托多层次、多维度的综合措施，有效提升校园网络的安全防护能力。

3.1 技术防御体系

（1）网络边界防护：在校园网出口部署防火墙、入侵检测与防御系统(IDS/IPS)，严格管控南北向流量，监测并拦截异常流量，有效防止外部攻击渗透校园网络。

（2）数据中心安全：在数据中心区域部署运维审计系统、数据库审计系统、漏洞扫描系统、Web应用防火墙（WAF）和网页防篡改等安全设备，保障核心业务系统的安全稳定运行，防止数据泄露和被篡改。

（3）终端安全管理：加强对终端设备的安全防护，采用统一的终端安全管理平台，对终端进行实时监控，防止恶意软件感染和数据泄露。

（4）态势感知与预警：部署网络安全态势感知系统，整合全网安全日志和告警信息，实时分析网络安全状况，及时发现潜在威胁，形成一体化的安全立体防护体系。

3.2管理机制优化

（1）信息资产管理：制定完善的信息资产管理制度，部署信息资产安全治理平台，实现对校园内信息资产的主动检测与识别，建立健全网站及业务系统备案机制，实施全生命周期管理，确保资产的安全性与合规性。

（2）安全策略制定与执行：根据国家相关标准和法规，制定校园网安全管理策略，涵盖访问控制、数据保护、应急响应等方面，确保网络安全工作的规范化和制度化。

（3）应急响应机制：建立健全网络安全事件应急响应预案，明确各部门职责和处置流程，定期组织演练，提高应对突发安全事件的能力，确保在安全事件发生时能够迅速且高效地处理，尽可能减少损失。

（4）第三方服务管理：对于引入的第三方云服务，确保数据和个人信息存储于中国境内，未经授权不得使用或扩散，保障数据的安全和合规。

3.3 安全文化培育

（1）安全意识培训：定期开展面向师生的网络安全培训，提高其对网络安全风险的认知，增强防范意识，培养良好的网络使用习惯，减少因人为因素导致的安全事件。

（2）安全责任制度：明确各级人员在网络安全中的责任，建立问责机制，促使全体成员共同维护校园网络的安全环境。

（3）信息共享与合作：加强与其他高校、科研机构和网络安全企业的合作，分享安全威胁情报和最佳实践，共

同提升网络安全防护能力，形成协同防御的良好局面。

4 实证研究

案例：构建网络安全综合防护平台—昆明医科大学

4.1 背景依据

昆明医科大学作为智慧校园建设示范单位，依据《网络安全法》、《数据安全法》要求，构建覆盖"人、技、管"三维度的网络安全综合治理体系。

4.2 治理措施体系化建设

4.2.1 资产全生命周期管理

（1）采用自动化资产测绘工具，建立包含13,000+台终端、500+台服务器的动态资产台账。

（2）实施分级分类管理，对科研系统、教务系统等关键资产进行重点防护。

（3）建立资产变更审计机制，实现新增/退役资产的闭环管理。

4.2.2 智能化风险防控体系

（1）部署AI驱动的漏洞扫描系统，年发现并修复高危漏洞4,300+个

（2）构建威胁情报分析平台，实现对0day漏洞的72小时预警响应。

（3）实施"红队-蓝队"攻防演练机制，年度开展4次实战化演练。

4.2.3. 立体化技术防护体系

（1）边界防护：部署下一代防火墙集群，日均拦截超过10GB的恶意流量。

（2）内网监控：利用流量指纹识别技术，监测异常的横向移动行为。

（3）数据保护：建立分级加密机制，核心数据库加密率达100%

4.2.4 主动式应急响应机制

（1）制定12类专项应急预案，建立"半小时响应-2小时处置-24小时复盘"的SLA标准。

（2）组建跨部门应急响应小组，实现技术部门与行政部门的协同作战。

4.2.4.5 安全文化生态建设

（1）实施"金盾工程"培训计划，年开展培训15场次，覆盖师生1.1万人次。

（2）建立网络安全志愿者队伍，发展学生安全员80余人。

4.3 治理成效评估

（1）安全事件下降：2024年安全事件同比减少78%，未发生重大数据泄露事件

（2）防护能力提升：在教育厅网络安全攻防演练中获"优秀防守单位"称号。

（3）管理效能优化：资产核查效率提升5倍，漏洞修复周期缩短至48小时。

5 未来展望

信息技术日新月异，校园网络安全面临空前挑战和机遇。未来，以下技术前沿领域将在校园网络安全治理中发挥关键作用：

（1）人工智能在网络安全中的应用：人工智能（AI）正逐渐应用于网络安全领域，提高威胁检测与响应的效率。AI 可以通过对海量网络数据的实时分析、识别异常行为、预测潜在攻击、实施自动化防御措施。

（2）零信任安全架构的实施：传统的网络安全策略基于边界防护，但随着云计算和移动设备的普及，边界变得模糊。零信安全架构强调“永不信任，永远验证”的原则，对每一个访问请求进行严格的验证和授权，确保只有经过认证的用户和设备能够访问资源，从而有效防范内部和外部的安全风险。

（3）安全态势感知与动态防御：建立安全态势感知体系，实时监控校园网络的安全状况，已经成为高校网络安全建设的关键方向。通过动态防御策略，针对攻击方法和途径的变化，实现网络安全状态的持续监测和及时反馈，根据不断变化的安全威胁，灵活调整防御策略、技术和手段。

（4）数据安全与隐私保护：在大数据时代，校园网络中存储了大量师生的个人信息和科研数据。为了提升数据安全管理，应采用数据加密、访问控制、数据脱敏等技术，确保敏感信息在存储、传输和使用过程中得到有效保护，防止数据泄露和滥用。

综上所述，未来的校园网络安全治理将依赖于先进技术的应用和持续创新。高校应紧跟技术发展的步伐，构建一个全面而高效的安全防护体系，确保校园网络的安全性与稳定性。

参考文献

[1]何海涛.中山大学网络安全态势感知体系建设[J].中国教育网络, 2023(8): 23-25.

[2]卞海彤.江苏大学打造网络安全综合治理平台[J].中国教育网络, 2024(6): 68-70.

[3]魏顺平.数字化转型背景下教育系统网络安全研究[J].中国教育信息化, 2024,30(2):35-47.