基于主动防御的高校网络安全策略研究

范向军，赵小芳
常州工程职业技术学院，江苏 常州 213002
DOI:10.61369/EDTR.2026080008

摘　　要： 在我国信息化进程不断加快的背景下，我国高等学校是我国科学技术创新与人才培育的重要基地，其信息系统的安全保护水平正受到越来越多的关注。2022年起，国家相继发布了《网络安全审查办法》和《数据出境安全评估办法》等相关法律法规，对"三化六防"进行了详细阐述，提出了基于可信计算、态势感知、自动化响应等多种方法，建立“事前防范—事中拦截—事后追溯”的全方位安全防护系统。但是高校网络应用中的Struts2漏洞和勒索软件攻击等问题仍然频繁发生。在这种情况下，利用威胁智能分析、行为建模和自动化编排等手段，由传统的“被动封堵”向“主动预判”转变，是解决高校信息安全困境的重要途径。

关 键 词： 高校网络建设；数字应用技术；信息化建设

Research on Cybersecurity Strategy for Colleges and Universities Based on Proactive Defense

Fan Xiangjun, Zhao Xiaofang
Changzhou Engineering Vocational & Technical College, Changzhou, Jiangsu 213002

Abstract: Against the backdrop of China's accelerating informatization process, colleges and universities serve as vital hubs for scientific and technological innovation and talent cultivation in China, with their information system security protection levels garnering increasing attention. Since 2022, the state has successively issued relevant laws and regulations, such as the "Measures for Cybersecurity Review" and the "Measures for Security Assessment of Data Exit," which elaborate on the "Three Transformations and Six Defenses" and propose the establishment of a comprehensive security protection system featuring "pre-event prevention, in-event interception, and post-event traceability" through various methods such as trusted computing, situation awareness, and automated response. However, issues such as Struts2 vulnerabilities and ransomware attacks continue to frequently occur in college network applications. In this context, leveraging intelligent threat analysis, behavioral modeling, and automated orchestration to transition from traditional "passive blocking" to "proactive anticipation" represents a crucial approach to addressing the information security dilemmas faced by colleges and universities.

Keywords: college network construction; digital application technology; informatization construction

高校互联网环境中蕴含着教学、科研、数据资产、用户隐私等诸多核心因素，其安全性和保密性是保障我国信息基础建设的重点。当前，我国高校校园网络安全面临着严峻的形势，如高级持续威胁（APT）通过零点缺陷进行有针对性的攻击，以及基于学术研究的精确勒索、跨国移动和分享环境下的个人隐私泄漏的危险日益增加，因此构建以“态势感应—情报解析—积极应对”为主线，融合威胁情报共享、行为基准建模和自动编排响应等手段，使之由“漏洞修补”向“风险预判”转变，由“单点防御”向“体系协同”转变。其特点与我国高等教育信息化建设中“主动识别风险、精准阻断攻击链条、持续优化防护”的迫切要求相吻合，是解决当前安全困境、构建主动免疫防御系统的重要途径。

一、基于主动防御的高校网络安全构建优势

（一）实时威胁识别和反应速度的即时性

建立基于“威胁智能”的信息安全探测框架，以达到毫秒级的信息安全感知和自动应对，缩短了攻击潜伏期。主动防御可以利用SIEM和TIP的深入融合，对包括CNCERT等在内的多个主要渠道（如恶意IP、漏洞利用特征代码等）进行在线监测和分析，构建对现有威胁进行实时拦截的能力。与此同时，结合机器学习等方法，建立基于行为基准的动态行为基准模型，实时监控用户端的访问和网络流量，一旦发现超出基线3个sigma的异常，

课题信息：本文系常州工程职业技术学院教改课题课“高职院校数字化资产安全自动防御平台的建设与应用研究”课题编号：25JY032。

就会自动启动“安全组织自动应答”实施风险隔离。在“双一流”大学开展的一项自主防护工作中发现，一个 APT 通过假冒学术交换的方式，将其插入到网络中，并通过对其附加文件的哈希值进行比对，在15分钟之内切断链接，比常规防护措施早72个小时就能确定其存在的危险，从而防止研究人员盗取信息[1]。

（二）数据泄漏风险大幅下降

以高校科研数据和师生隐私为研究对象，建立一套完整的三维数据保护系统，从传输、存储和访问三个方面实现数据安全保护。在传输层面，通过 SM4 保密协议和动态密码通道对跨校区和跨机构传输的重要信息进行了强制性的加密。在数据存储层面，采用自然语言处理等方法对科研论文和试验数据进行自动分类和分类，然后采用 DDM 对敏感域（例如使用屏蔽代码替代身份标识等）进行提取，并采用区块链方法对数据进行运行日志保存，从而达到全链条可追溯性。Gartner 研究显示，将基于主动加密和精细存取控制相结合的方法，可以将信息泄露所带来的经济损失降低78%以上，特别适合大学多学科协同的高频率信息分享（例如：医疗成像和附属医院之间），从根本上解决“越权访问”“未经许可传递”等关键问题。

（三）适配校园复杂场景，降低全网漏洞存续风险

高校网络体系结构相较于企业、政府网络更为开放、复杂、多元，具备业务系统多、开放权限大、入网终端杂乱、人员流动性强等特点。高校既要保障教务办公、学生选课、校园服务等公共业务稳定开放，又要保证实验室科研平台、涉密课题数据、附属医院医疗数据的安全性，传统被动防御模式只能在攻击发生后进行事后处置，无法提前排查隐藏在全网中的各类安全隐患。而主动防御体系以常态化巡检、全覆盖扫描、持续性自查为核心，能够对校园门户网站、教务管理系统、学工平台、图书馆资源服务器、各院系科研主机以及师生自由接入的无线终端、私人设备进行全方位风险监测。系统可精准排查长期存在的高危漏洞、系统未修复补丁、端口过度开放、中间件配置错误、数据库弱口令、老旧业务系统遗留缺陷等各类常见问题，做到隐患早发现、早整改、早闭环。结合多所高校长期运维实践来看，部署主动防御机制后，校园高危漏洞暴露时长大幅缩短，彻底改变了以往漏洞长期暴露、被恶意扫描批量利用的问题，能够在不影响校园正常教学科研网络使用的前提下，持续净化校园网络环境，全面适配高校开放式、多场景、高并发的网络运行特点[2]。

二、基于主动防御的高校网络安全策略应用策略

（一）构建全局感知、智能分析、动态响应”机制

以“全局感知、智能分析、动态响应”为中心的信息安全探测模型为研究对象，以多维信息融合为手段，对可能存在的危险进行精确感知。在技术体系上，依据《信息安全技术关键信息基础设施安全保护要求》（GB/T 39204-2023）对“动态防御，主动防御”的需求，将 SIEM、 TIP、 NetFlow/IPFIX 等流量分析引擎和行为基准模型等集成起来，构建“数据收集 - 关联分析 - 风险评估”的闭环监测体系[3]。

例如，高校网络信息中心可配备 Tenable Nessus 专业版漏洞扫描器，设定符合教育产业特性的扫描策略范本。可在周三凌晨2:00-5:00对全校158个 C类地址进行自动扫描，主要针对缺少补丁的 Windows/Linux 操作系统、不正确的中间件配置和数据库弱密码等问题进行检测。扫描工作采取分层授权机制，由网管中心直接扫描核心业务系统，由培训过的二级管理员进行分布式扫描。通过 API 将扫描结果自动同步到安全运维平台，并将其与 CMDB 资源库进行关联分析，生成完整的报告，包括 IP 地址、主机名、部门归属、弱电等级等。对于发现的高风险脆弱性（CVSS 分值≥7.0），系统会自动产生工作任务，并分配给相关人员，要求其24小时内完成故障修复或者制定减轻措施。为检验修复效果，系统会在修复期限届满时自动启动一次复查扫描，并将未修复的缺陷上报给相关部门领导进行监督。在入侵检测方面，学校可将 Suricata 入侵检测系统部署到核心节点上，使用多维度检测规则集。基于特征点的检测规则每周更新一次，并对攻击工具的特征进行识别。同时，利用机器学习方法构建网络流量基线模型，识别 DDoS 攻击等行为。

（二）构建高效预警机制，提前防范安全风险

对各种安全数据源进行整合，包括检测工具输出和安全智能信息等，构建智能预警平台。采用大数据分析和机器学习等方法，对采集到的数据进行深度挖掘和关联分析，建立高精度的安全风险预测模型。当模型监测到数据的异常形态，预示着可能发生的安全事件时，可以快速启动预警机制。学校安全管理系统通过邮件、短信、弹窗等多种渠道向网络安全管理员推送预警信息。根据不同的紧急程度，设置不同的预警等级，管理者可以根据不同的预警等级启动相应的应急预案，提前做好预防工作，把安全风险控制在萌芽状态[4]。

例如，高校可建设网络安全态势感知平台，平台集成12种类型的数据源，包括防火墙日志，IDS 警报，终端安全事件等，平均每天处理45G 的日志。数据采集层采用 Fluentd 日志采集架构，将日志收集设备部署到校园36个区域内，利用 Kafka 消息队列实现高并发性数据处理。在此基础上，采用基于 ELK 技术栈的实时分析模块，结合 Spark 平台上的离线计算模块，构建面向高校应用场景的威胁检测算法库。在账户异常检测方面，构建用户行为画像模型，综合分析用户登录时间、位置、设备指纹等20多个特征维度，识别出37个疑似账号共享的教师账户。如在网络攻击预警方面，系统经关联分析，发现某实验室主机在三个小时内定期向境外 IP 发起定期连接，经判断，已植入的挖矿木马正与 C& C 服务器进行通信，安全小组立即对该主机进行隔离，对攻击路径进行追踪，确定为钓鱼邮件渗透进入内网。该平台创新性地引入威胁智能订阅服务，实时访问5种威胁情报源，如 CNVD、AlienVault 等，一旦发现校园 IP 与恶意域名进行通信，就会自动触发警报。

（三）应用分层机制，构建基于威胁智能的全领域监控

以“分层探测 - 协同防御 - 动态演化”为主线，通过集成不同层次的技术堆栈，达到对多种威胁的精确防御。根据网络安全等级保护2.0和关键信息基础设施安全保护要求，我国高等院校需

要构建基于威胁智能的全领域监控，利用国家智能系统和商务威胁情报资源，建立涵盖 IP声誉、脆弱性特征、恶意代码指纹在内的多维情报库，从而对未知的攻击进行及时预警和拦截。动态加密和数据脱敏，针对科研数据和师生隐私等敏感财产，在数据传输层上配置SM9加密通道，通过动态数据脱敏（DDM）去除数据的敏感域，在分享层通过联合学习，达到“数据可用不可视”的目的[5]。

例如，高校可实施“零信任”安全体系结构，在校园网络出口处部署 PaloAlto下一代防火墙集群，并配置应用身份识别、用户身份识别和内容识别三重保护机制。在应用层，防火墙对多个网络应用进行准确的识别，对非教学应用如 P2P下载和游戏加速器进行带宽限制；在用户层，采用 Radius认证系统实现对业务部门的差别化访问控制；在内容层，部署深度包侦测引擎，阻断包含恶意程式码的办公文件传送。为保障科学研究数据的安全，学校应建立一个统一的加密服务平台，以国家加密算法为基础，为各个业务系统提供标准化的加密接口。文件传输加密模块利用SM4算法加密学术论文和实验数据等敏感文件，密钥采用 HSM对其进行统一管理。

（四）完善常态化运维与安全教育机制，夯实主动防御人为防线

主动防御体系不能只依靠软硬件设备，还需要配套运维管理制度与全员安全意识作为支撑，从管理、人员层面填补技术防护存在的短板，形成技术 + 管理协同防护的完整体系。高校需要建立标准化安全运维流程，同步搭建覆盖全体师生的常态化安全教育体系，定期开展风险排查、安全培训与实战演练，持续降低人为操作带来的安全隐患[6]。

例如，高校网络中心制定“日巡检、月复盘、学期演练”标准化运维制度，每日自动导出全网终端弱口令、违规外联、越权访问记录，每月汇总漏洞整改完成情况并形成态势分析报告，每学期联合各院系开展网络安全实战演练。针对教职工、研究生重点开展科研数据保密培训，面向新生开设校园网络安全必修课，讲解钓鱼邮件识别、私人设备入网规范等内容。学校每半年组织一次校内红蓝对抗渗透测试，安全团队模拟钓鱼攻击、内网横向渗透等常见入侵手段，主动挖掘教务系统、实验室服务器存在的隐性漏洞；同时搭建线上安全考试平台，要求全校教职工每年完成安全知识考核，考核不通过限制业务系统登录权限。针对运维工作建立完整整改台账，对演练、巡检中发现的权限冗余、设备策略老旧等问题划分整改时限，逾期未完成整改的部门同步推送安全督办通知，将人员管理、日常运维纳入主动防御闭环流程，减少因人为疏忽引发的网络安全事件。

三、结束语

综上所述，以主动防御理论为基础，对高校网络安全策略进行研究，不仅可以有效地提高高校网络的安全防护能力，为高校的信息化建设提供安全保障，而且可以为高校的教育教学、科研创新和管理服务提供可靠的网络安全保证。未来，随着信息技术的不断发展，网络安全威胁日趋复杂，高校网络安全中的主动防御策略将越来越受到重视。高校应该进一步加强主动防御技术的研发和应用，对网络安全管理系统进行优化，培养高素质的网络安全人才，才能适应新形势的变化，促进高校的高质量发展。

参考文献

[1] 程子颖，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.

[2] 罗敏，陈洋 . 基于等保2.0高校网络安全主动防御体系建设探析 [J]. 信息与电脑 (理论版),2021,33(21):197-199.

[3] 史蕊 . 等保2.0下的高校网络安全治理探索 [J]. 网络安全技术与应用 ,2021,(10):94-95.

[4] 汤湘林 , 陈方兵 .5G时代下高校网络安全研究与应用 [J]. 网络安全技术与应用 ,2021,(06):89-90.

[5] 孔垂煜 . 等保2.0下高校网络安全主动防御体系建设方向探析 [J]. 湖南科技学院学报 ,2021,42(02):66-68.

[6] 裴建廷，于谦，孙斌，王金民 . 基于等保2.0高校网络安全主动防御体系建设探析 [J]. 信息通信 ,2020,(02):166-167.

