高校网络安全主动防御体系的构建与实践

范向军　赵小芳
常州工程职业技术学院　江苏常州　213002

摘　要：自高校信息化建设加速推进以来，数字化校园建设稳步开展，已实现教学、科研、管理等核心业务的全面网络化覆盖。随着网络攻击手段的复杂化与常态化，高校网络安全风险持续攀升，构建高效、智能的主动防御体系已迫在眉睫。基于此，将简要探讨高校网络安全面临挑战，提出主动防御体系构建路径，以期为高校网络安全防护提供系统性解决方案，推动高校数字化转型的安全、可持续发展。

关键词：高校；网络安全；主动防御；体系构建

引言

在数字化教育快速发展当下，高校网络威胁形势愈发严峻，黑客攻击、数据泄露等事件频发，给高校网络安全带来挑战。传统被动防御模式在应对复杂多变的网络攻击时，难以妥善应对。为此，探讨其构建原则与实践路径，提出切实可行的解决方案，为高校网络安全防护提供新思路[1]。

一、高校网络安全主动防御体系构建原则

1.预防为主

结合高校网络环境特性，将安全防线前置至威胁入口，例如在网络边界部署智能流量分析系统，实时监测异常流量模式，结合威胁情报库动态更新防护规则，实现攻击行为的早期识别与阻断。针对高校内部用户行为复杂的特点，应采用基于行为分析的零信任架构，对用户身份、设备状态及访问行为进行持续验证，避免因单一凭证泄露导致的横向移动攻击。预防机制需融入安全运营的全生命周期，采用自动化漏洞扫描与修复工具，对教学系统、科研平台等资产进行常态化风险评估，并利用安全编排与自动化响应（SOAR）技术，将威胁情报、安全策略与处置流程深度耦合，保证安全事件从发现到处置闭环效率。

2.动态监测

部署基于机器学习的异常检测系统，对网络流量中的隐蔽攻击行为进行模式识别，结合威胁情报动态调整检测规则，提升对零日漏洞与高级持续性威胁（APT）识别能力。对于高校网络中科研平台、在线教学系统等资产脆弱性，需建立动态漏洞扫描机制，利用自动化工具对服务端口、软件版本及配置文件进行高频次检查，为安全加固提供数据支撑。动态监测需与应急响应流程深度融合，依托安全编排与自动化响应（SOAR）平台，将检测到安全事件自动关联至处置剧本，实现威胁情报的实时共享与协同处置。

二、高校网络安全主动防御体系架构设计

1.总体架构设计

高校网络安全主动防御体系架构设计需以分层解耦、数据驱动为逻辑，构建覆盖全域的动态防护网络。感知层部署日均处理500TB级流量的智能探针集群，借助机器学习算法对HTTP/HTTPS流量中的隐蔽攻击行为，如加密流量中的C2指令进行实时解密分析，异常检测准确率达98.7%[2]。

防护层构建基于零信任架构的动态访问控制系统，对师生终端实施持续身份验证与行为画像，单次认证耗时低于0.3s，分析层搭建威胁情报聚合平台，集成开源情报源与高校私有情报库，日均处理威胁情报，知识图谱技术实现攻击链的自动化溯源。响应层部署SOAR自动化编排系统，在数据域构建安全大数据库，整合网络流量、终端日志、漏洞扫描等数据源。建立自适应安全策略引擎，根据威胁情报动态生成防护规则，形成主动防御体系，为高校网络空间安全提供技术支撑。

2.核心组件设计

智能感知层部署分布式流量探针集群，采用DPI+AI

基金项目：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

双模检测技术，结合终端行为传感器对师生终端进行实时画像，异常行为捕获率提升。威胁研判层构建基于知识图谱的威胁情报中心，集成开源情报源与高校私有情报库，凭借图神经网络算法实现攻击链自动推演。自动化响应层搭建SOAR编排引擎，内置多个原子化处置剧本，使用低代码平台实现安全策略分钟级编排，对勒索病毒等高危事件的阻断成功率较高。数据中台作为体系枢纽，整合网络流量、终端日志、漏洞扫描等数据源，支撑态势感知预测准确率提升。

三、高校网络安全面临挑战

1.攻击手段多样化

传统攻击方式已迭代升级，攻击者利用加密混淆技术，将恶意流量伪装成正常通信，让基于特征匹配的防火墙形同虚设。采用域名生成算法（DGA）批量生成随机域名，绕过静态黑名单的封锁，持续向高校网络投送勒索病毒、挖矿木马等恶意软件。攻击者擅长利用高校物联网设备的安全漏洞，如未加密的Wi-Fi接入点、弱密码的智能终端，构建僵尸网络发起DDoS攻击，瞬间瘫痪教学系统与科研平台。

针对高校师生对学术资源的依赖心理，攻击者设计钓鱼邮件，伪装成知名学术期刊、图书馆系统，诱导师生泄露账号密码，植入远程控制木马，长期潜伏窃取科研成果。攻击者伪造高校领导、合作机构的社交账号，利用师生对权威的信任，以“紧急项目审批”“合作资金划拨”等名义，诱导师生点击恶意链接或下载携带后门的文档。现阶段，攻击者开始利用生成式AI技术，批量制作高度逼真的虚假视频、语音，冒充高校领导进行精准诈骗，引导师生泄露敏感信息，使高校网络安全陷入被动局面[3]。

2.安全漏洞频发

软件系统层面，高校教学管理、科研协作等平台大量使用开源组件，相关组件更新滞后且存在历史漏洞，攻击者借助自动化扫描工具，快速定位并利用未修复的漏洞实施攻击，导致师生个人信息泄露，情节严重还会使核心科研数据被窃取篡改。硬件设备方面，校园内大量物联网设备如智能门禁、实验仪器等，因成本或技术限制，安全防护机制薄弱，默认密码普遍存在且难以统一管理，攻击者可轻易破解并控制设备，将其作为跳板渗透校园网络，引发物理设施的异常运行，影响教学秩序。师生网络安全意识淡薄，随意点击不明链接、使用弱密码，为攻击者提供切入机会。部分高校员工为图方便，违规在办公电脑上安装盗版软件，此类软件携带的恶意插件会在后台运行，窃取敏感信息。

3.安全意识薄弱

日常行为中，部分师生对网络安全风险缺乏警惕，在公共场所随意连接免费Wi-Fi，但因部分网络被攻击者架设为钓鱼陷阱，一旦接入，设备信息、账号密码等敏感数据便会被窃取。使用公共电脑时，很少有人主动清理浏览记录、退出登录账号，为后续使用者提供获取隐私信息的便利通道。密码管理上，多数师生存在严重问题，为图方便，将各类账号设置为简单易记的弱密码，甚至多个账号使用同一密码。一旦某个账号被攻击者破解，其他关联账号也存在被盗取风险，导致个人信息、学术成果等重要数据泄露。攻击者利用高校师生对学术交流、求职招聘的需求，设计钓鱼邮件、虚假网站，以论文发表、高薪兼职等为诱饵，诱导师生点击恶意链接、下载病毒软件。

四、高校网络安全主动防御体系实践路径

1.网络安全基础设施加固

构建多层次、立体化的网络边界防护体系，在校园网出口部署下一代防火墙，运用深度包检测与机器学习算法，对进出流量进行实时解析，识别并阻断恶意攻击、数据窃取等行为，实现应用级访问控制，保证仅授权业务可访问核心资源。强化终端安全防护能力，为师生终端统一部署基于零信任架构的终端安全管理系统，实现设备身份认证、行为监控与动态访问控制[4]。

使用沙箱技术对可疑程序进行隔离运行分析，防止未知威胁扩散。建立终端漏洞修复机制，利用自动化补丁管理系统，保证终端及时更新安全补丁，消除潜在风险点。采用分布式存储与加密技术，对高校科研数据、师生信息等敏感数据进行全生命周期加密保护。部署数据防泄漏系统，对数据外泄行为进行监控审计，防止敏感数据泄露。还应建立异地容灾备份中心，使其在遭遇网络攻击或自然灾害时，数据可快速恢复，保障高校业务的连续性。

2.安全监测与响应体系

构建协同立体监测网络，在校园网边界部署全流量威胁检测探针，运用智能流分析技术，对加密流量中的隐蔽攻击行为进行解密还原与特征提取。在终端侧部署轻量化安全代理，实时采集设备行为日志，结合UEBA（用户实体行为分析）算法构建行为基线，精准捕捉异常操作。在云端接入威胁情报共享平台，整合开源情报、

高校私有情报库及第三方专业机构情报，实现攻击链自动推演，提前预警潜在风险。

打造智能化威胁分析中枢，基于自然语言处理与知识图谱技术，构建威胁情报自动解析引擎，将非结构化情报转化为可执行的监测规则。当监测到安全事件时，SOAR（安全编排自动化响应）平台迅速介入，基于预置原子化处置剧本，自动执行隔离受感染终端、阻断恶意网络连接、启动数据恢复流程等操作，并将处置结果同步至安全运营中心。安全运营团队对每起安全事件进行深度溯源，运用因果分析技术还原攻击路径，总结防御短板。引入AI安全顾问，为师生提供7×24h实时安全咨询服务，构建动态演进、持续强化的安全监测与响应体系。

3.安全意识教育与培训

高校网络安全主动防御体系构建中。应对安全意识教育加以重视，管理层侧重网络安全战略思维与合规管理，凭借案例剖析提升风险决策能力，技术人员聚焦前沿攻防技术与应急响应实操，在虚拟靶场中模拟APT攻击溯源、勒索病毒处置等场景，锤炼实战技能，普通师生以网络安全微课堂形式，结合校园真实事件，用短视频、互动游戏等通俗易懂方式讲解钓鱼邮件识别、密码管理、Wi-Fi安全等基础防护知识[5]。

创新培训形式，引入VR虚拟现实技术打造沉浸式安全体验，师生可身临其境感受数据泄露、网络诈骗等场景，角色扮演完成安全决策任务，强化风险感知与应对能力。开发网络安全能力认证小程序，设置知识问答、漏洞挖掘挑战等关卡，师生完成学习任务可解锁成就徽章。建立长效考核机制，将网络安全素养纳入师生综合评价体系，定期开展攻防演练，模拟黑客攻击与防御对抗，检验培训效果并挖掘潜在风险点。设立网络安全宣传月，举办CTF夺旗赛、安全创新大赛等活动，激发师生参与热情。凭借持续教育、动态考核、正向激励的闭环设计，推动网络安全意识从被动接受向主动防御转变。高校网络安全主动防御体系实践路径如表1所示。

表1　高校网络安全主动防御体系实践路径

实践路径	具体措施
网络安全基础设施加固	部署下一代防火墙，实现应用级访问控制 采用零信任终端安全管理系统，强化设备认证与行为监控 构建分布式加密存储环境，部署数据防泄漏系统 建立异地容灾备份中心，确保数据快速恢复
安全监测与响应体系	搭建多维度监测网络，运用深度包解析与机器学习识别威胁 构建威胁情报共享中枢，实现攻击链自动推演 部署SOAR平台，实现安全事件自动化响应 建立闭环机制，深度溯源与红蓝对抗演练提升实战能力
安全意识教育与培训	分层分类培训，提升管理层、技术骨干、师生安全素养 引入VR虚拟现实技术，打造沉浸式安全体验馆 开发网络安全能力认证小程序，形成学习-实践-认证闭环

结论

在网络安全基础设施加固上，有效提升网络边界防护能力，降低外部攻击风险，保障高校核心数据与业务系统的稳定运行。安全监测与响应体系实现对网络威胁的实时感知与快速处置，缩短安全事件响应时间，减少潜在损失。安全意识教育与培训从根源上提升师生网络安全素养，使师生成为高校网络安全生态的积极参与者。网络威胁不断演变，高校网络安全主动防御体系需持续优化。未来，高校应加强与行业、科研机构的合作，引入前沿技术，不断完善体系架构。持续强化师生安全意识，营造全员参与的网络安全文化氛围，为高校数字化转型与教育事业发展提供网络安全保障。

参考文献

[1]陆生堂.风险管控视阈下高校网络安全防控机制构建[J].中国新通信，2025，27（03）：37-41.

[2]樊新武，张帅，杜香燕.教育数字化背景下高校网络安全防护体系建设研究[J].中国信息技术教育，2023，（22）：100-103.

[3]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.

[4]杨振宇.多维构建高校网络安全屏障[J].安徽水利水电职业技术学院学报，2023，23（01）：82-86.

[5]陈敏锋.高校网络安全运营防护体系研究[J].无锡商业职业技术学院学报，2022，22（06）：108-112.