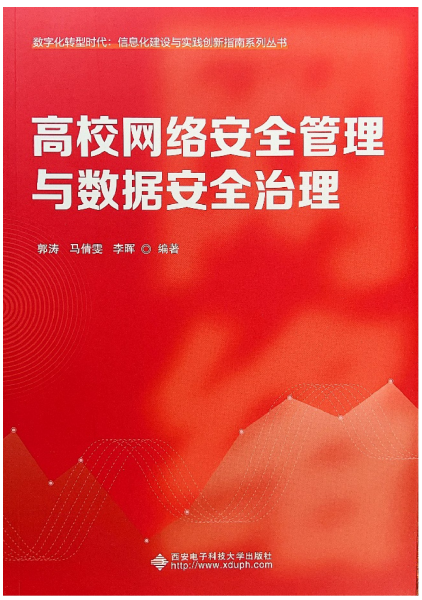
高校数字化资产安全管理策略
——评《高校网络安全管理与数据安全治理》

随着高校数字化进程加速,教学科研数据、师生信息、智慧校园系统等数字化资产规模呈指数级增长。然而,网络攻击频发、数据泄露风险攀升,对高校资产安全管理提出严峻挑战,因此,有必要加强数字化资产安全管理,构建安全可信的数字校园。

《高校网络安全管理与数据安全治理》一书立足国家安全战略高度,系统梳理了从法规政策到技术实践的完整知识体系,理论严谨,逻辑清晰,且案例解读深刻。第一章阐释了网络安全基本概念、重要性及法律法规发展脉络;第二章深入剖析了网络安全模型、框架、架构及技术产品应用;第三章聚焦网络安全管理策略与实践,强调信息策略的协同作用;第四章针对机房环境、应用系统、数据个人等安全威胁,提出具体防范措施与应急处置流程;第五章围绕数据安全管理与分类分级展开,构建科学的数据治理体系。



书名:高校网络安全管理与数据安全治理
作者:郭涛,马倩文,李晖
出版社:西安电子科技大学出版社
ISBN:9787560674964
出版时间:2025年1月
定价:42元

作者指出,高校数字化资产安全管理需立足数据全生命周期,构建从采集、存储、传输、使用到销毁的全流程闭环防护机制。第一,数据采集阶段需建立严格的数据来源审核制度,确保教学科研数据、师生个人信息等敏感信息,必须通过合法合规渠道获取,如学生成绩、学籍信息等核心数据,一定通过校内认证系统采集,避免第三方平台随意抓取。第二,在存储环节需实施分级分类存储策略:①核心数据如科研成果、财务数据应采用加密存储,并部署访问控制列表,仅授权人员通过双因素认证方可访问;②一般数据采用常规存储方案,但需定期进行完整性校验。对于存储数据的存储设备,需按照国标建立安全机房,配备恒温恒湿、防雷防静电、门禁监控等物理防护措施,同时,建立7×24小时运维监控体系,确保完全。第三,传输过程中必须采用国密算法加密通道,禁止明文传输敏感数据,如校内跨部门数据共享应通过教育专网进行,外部传输需通过虚拟专用网络或安全网关。对于数据的使用,应基于最小权限原则,通过角色权限管理实现“按需知密”,如教务系统仅向授课教师开放学生成绩查询权限,科研团队仅向项目组成员开放试验数据访问权限,其余情况下不得跨部门查询访问。第四,销毁环节要建立数据销毁审计机制,到期数据应通过物理销毁(如硬盘消磁)或逻辑销毁(如覆盖写入)方式彻底清除,并留存销毁记录备查。整个生命周期需嵌入安全审计模块,对异常访问、越权操作等行为自动告警并留存日志,确保可追溯可问责。

笔者认为,高校数字化资产安全管理需构建“人员-技术-制度”三位一体的动态防御体系。人员管理方面应建立专职安全团队与兼职安全员相结合的管理架构。专职团队负责安全策略制定、系统运维、应急响应等核心工作,兼职安全员由各部门信息联络员担任,负责本部门日常安全巡检、风险上报等工作。技术防护需构建多层次立体防护网。网络层应部署下一代防火墙、入侵检测系统、流量清洗装置等设备,构建纵深防御体系。应用层需实施代码安全审计,对教务系统、办公自动化系统等关键应用进行安全漏洞扫描,及时修补高危漏洞。数据层应部署数据库防火墙、数据泄露防护系统,防止结构化查询语言注入、拖库攻击等常见威胁。终端层需强制安装杀毒软件、主机监控系统,对教师办公终端、学生实验室设备实施统一安全管理。制度建设需完善安全管理制度体系。学校应制定《高校数字化资产管理规范》《数据分类分级实施细则》《安全事件应急预案》等制度文件,明确各部门安全职责、操作流程、考核标准。需建立安全事件分级响应机制,对一般安全事件24小时处置,重大安全事件立即启动应急预案,成立专项工作组进行处置。动态防御强调持续监测与快速响应。需部署安全态势感知平台,实时分析网络流量、系统日志、用户行为,通过大数据建模识别异常行为模式。建立威胁情报共享机制,及时获取最新漏洞信息、攻击特征,动态调整防护策略。定期开展渗透测试、红蓝对抗演练,检验防御体系有效性,形成“监测-预警-处置-反馈”的闭环管理机制,确保数字化资产安全防护始终处于动态优化状态。

高校数字化资产安全需以全生命周期防护为基,以“人、技、制”动态防御为盾。唯有持续完善策略、强化协同、迭代技术,方能筑牢安全防线,护航数字校园行稳致远,让教育数字化成果真正惠及师生、赋能未来。

(李强/大连交通大学国有资产与实验室管理中心/副教授)