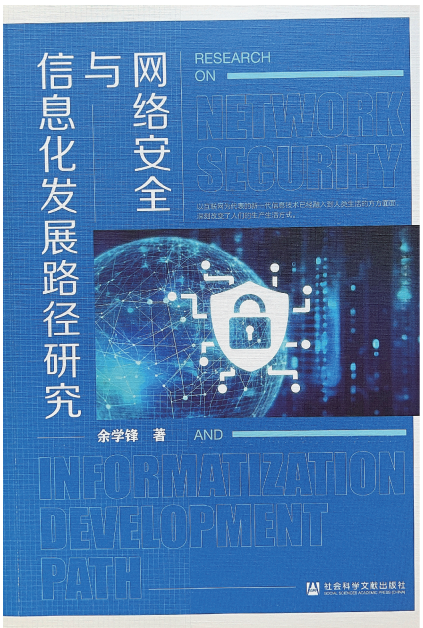
教育信息化发展中的网络安全管理策略
——评《网络安全与信息化发展路径研究》



书名:网络安全与信息化发展路径研究
作者:余学锋
出版社:社会科学文献出版社
ISBN:9787522824901
出版时间:2023年10月
定价:98元

教育信息化已成为教育现代化的重要标志,然而在教育信息化进程中,网络安全问题日益凸显,制约教育信息化可持续发展。网络安全事关学校教学秩序,以及师生的个人隐私信息安全。因此,加强教育信息化发展中的网络安全管理势在必行。

笔者在开展2023年度广西高等教育本科教学改革工程(2023JGA406)研究过程中,认真地阅读了《网络安全与信息化发展路径研究》。该书紧扣时代脉搏,围绕网络强国建设这一核心主题,深入剖析互联网信息技术对人类社会生活的深远影响。书中系统梳理了我国网络安全和信息化工作的现状与挑战,从安全、产业、人才、文化、技术、法律等多个维度进行了全面剖析。针对存在的问题,作者提出一系列具有前瞻性和可操作性的方法路径,如健全网络安全保障体系、坚持“人民至上”的发展思想、构建网络综合治理体系等,旨在全面提升我国网络安全和信息化水平。本书集理论性、实践性于一体,指向明确,旨在推动网信事业创新发展。

作者指出,技术层面防护是网络安全管理的基石。面对新型的网络攻击手段,教育机构要与时俱进更新安全防护技术,尤其是智能化数据安全技术。大数据技术为教育机构的网络安全防护提供全新的视角和手段,通过流量、行为、日志、业务、设备等方面海量大数据进行建模分析与研究,可及时发现异常行为和潜在威胁。在数据解析基础上,利用机器学习模型回溯和分析历史数据,总结出网络攻击的规律和特征,帮助教育机构建立用户行为画像,实现对用户行为的精细化管理和控制,进一步提高网络安全防护的针对性和有效性。人工智能技术使网络安全防护更加智能化和自动化,通过训练深度学习模型,教育机构可实现对网络流量的实时监测和智能识别,及时发现并阻断恶意攻击。深度学习模型可自动学习和提取网络流量的特征,智能识别和分类未知攻击,提高安全响应的速度和准确性。人工智能技术亦可辅助安全人员进行安全事件的分析和处理,提供智能化的决策支持。态势感知技术作为一种新兴的网络安全技术,能够为教育机构提供全面的网络安全态势视图。通过整合多种数据源,态势感知技术可实时展示网络的安全状态,利用可视化技术将复杂的网络安全数据以直观、易懂的方式呈现出来,帮助安全人员及时了解网络的安全状况,发现潜在的安全风险。

笔者认为,教育信息化过程中,数据的生命周期管理对于确保数据的安全性和可用性至关重要,每一个阶段都应设置网络安全保护机制。数据采集阶段,学校需建立严格的数据采集规范,明确数据采集的目的、范围和方式,确保采集过程符合相关法律法规的要求,并对采集到的数据进行分类和标识,便于后续的管理和使用。为进一步提升数据采集的安全性,学校可采用区块链技术确保数据的不可篡改性和可追溯性,增强数据的可信度和可靠性。在数据存储阶段,学校应采用更加安全、先进的存储设备和存储方式,如云存储、分布式存储等新型存储方式。学校可选择具有高强度加密功能、访问控制机制和容灾备份能力的云存储服务,确保数据在存储过程中的安全性和可用性,并脱敏处理存储中的敏感数据,即使数据被非法访问,也无法直接识别个人信息,进而可保护隐私。在数据处理阶段,学校需在安全的设备上进行数据处理,并提升安全授权等级。学校需要建立严格的数据访问控制机制,可采用生物识别技术进行授权,确保只有经过授权的人员才能访问和处理数据。在数据传输阶段,学校通过各种先进的加密技术传输数据,如采用端到端加密技术,确保数据在传输过程中不被窃取或篡改,亦可采用量子密钥分发等前沿技术,提供理论上无条件安全的通信方式,进一步增强数据传输的安全性。在数据销毁阶段,学校采用安全的销毁方式和流程,确保数据无法被恢复和滥用,包括物理销毁、数据擦除等多种方式。

综上,在教育信息化进程中,网络安全管理至关重要。通过安全防护技术升级,以及数据生命周期管理等措施,可有效保障教育数据的安全性和完整性,提升教育信息化水平,为教育事业创新发展提供坚实保障。

(杨丽/桂林学院教育与音乐学院/讲师)