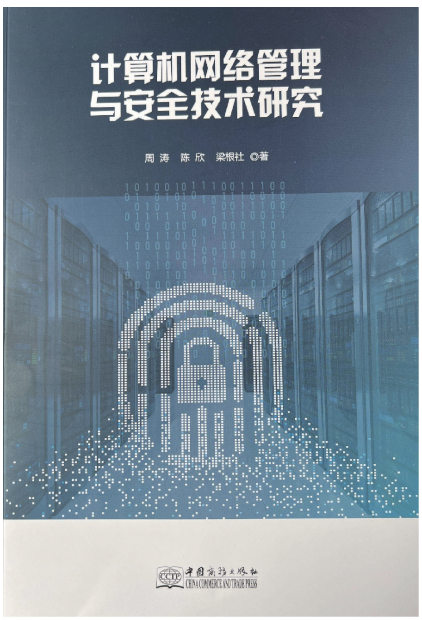
网络安全管理体系中的风险评估与防护策略
——评《计算机网络管理与安全技术研究》



书名:计算机网络管理与安全技术研究
作者:周涛,陈欣,梁根社
出版社:中国商务出版社
ISBN:9787510342042
出版时间:2023年7月
定价:50元

目前,网络已渗透到社会生产生活的各个方面,网络安全风险亦随之而来,这对网络产业可持续健康发展构成了威胁。网络风险评估能够全面识别和分析网络系统中的潜在威胁和脆弱性,防范和化解潜在的网络安全风险,确保网络系统的安全性与稳定性。

《计算机网络管理与安全技术研究》一书全面系统地介绍了计算机网络管理与安全技术的相关知识,结构严谨,叙述清晰。书中内容涵盖了网络管理基础、数据链路层、网络层、网络管理体系结构、远程网络监视、网段规划与管理、网络监控与故障管理、网络安全体系结构等多个方面。作者深入阐述了密码技术、信息隐藏技术、防火墙以及病毒防治等安全技术,并结合了最新的网络管理与安全技术成果和实际应用案例,因此,本书颇具借鉴价值。

作者指出,网络安全管理体系中,风险评估至关重要,其能够帮助组织识别、分析并量化其面临的网络安全威胁。机构单位可根据实际需要,灵活选择不同的风险评估方法。定性评估方法要求专家从经验出发,设定风险维度,再根据其性质进行风险剖析。在定性评估法中,常用工具包括风险矩阵、威胁建模等,通常不涉及复杂的数学模型或统计计算,而是通过专家访谈、问卷调查、小组讨论等方式收集信息,并基于这些信息对风险进行排序和分类。风险矩阵,即将所有风险因素整理出来,根据发生概率与影响大小进行排序,以此确定风险等级。威胁建模,是通过分析攻击者的动机、能力和资源,以及系统的脆弱性,预测可能的攻击路径和方式。与定性评估法不同,定量评估法以数据为基础,按照数学模型进行数据测算,因此,需要收集大量数据,包括历史安全事件记录、系统配置信息、漏洞扫描结果等,运用统计学和概率论的方法分析和处理这些数据,以得出风险发生的概率和影响程度。定量评估法采用客观数据为风险评估因素,更为精准,因此,可据此组织制定更为科学的安全策略和措施,然其需要大量的数据和计算资源,且评估过程可能较为复杂和耗时。在定量评估法中,常用的工具包括通用漏洞评分系统、风险评价模型等。混合评估法结合定性评估法和定量评估法的优点,既考虑专家的经验和判断,又运用数学模型和统计方法进行客观量化评估,更为全面。

笔者认为,用户识别和分析网络安全风险时需要制定相应的防护策略来降低风险并保护其网络资产。访问控制是网络安全防护的第一道防线,机构单位需要实施严格的访问控制措施,限制对网络系统和敏感信息的访问权限,具体包括采用身份认证、访问控制列表、安全策略等方法,确保只有授权人员才能访问网络系统和敏感信息。为强化访问控制,可采用多因素认证机制,如密码+指纹识别、密码+短信验证码等,提高账户的安全性,并定期审查和更新访问权限,确保员工只能访问与其工作相关的信息,防止因权限过大导致数据泄露和滥用。加密技术是保护网络通信和数据安全的重要手段,可采用套接字层/传输层协议等技术来保护网络通信的安全,确保数据的机密性和完整性。在保存传输敏感数据时,需要采用加密方式,防范来自网络非法机构或个人的拦截、窃取和篡改。为加强数据保护,机构单位还可采用数据脱敏技术,在数据共享或测试时脱敏处理敏感数据,以减少数据泄露的风险。此外,亦需定期更新软件补丁和安全补丁,以修复已知的漏洞和弱点,及时检测和排除潜在的安全隐患。网络安全防护需要采用多层次防御策略,结合不同的安全技术和管理措施形成一个坚固的防护体系,包括部署防火墙、入侵检测与防御系统(IDS/IPS)、反病毒和反恶意软件等安全设备和技术手段;制定和执行严格的安全管理制度和流程;采用数据加密、访问控制等技术手段来保护敏感信息和关键系统。多层次防御策略的实施,可有效降低网络安全风险,提高系统的安全性,并持续监控和评估其网络安全状况,及时发现并修复潜在的安全漏洞和弱点。

总之,网络安全事关国家安全与社会稳定,亦与民众日常生活密切相关,基于风险识别不断加强网络安全防护,才能确保网络系统的安全性与稳定性,为社会可持续发展保驾护航。

(王永恒/上海中侨职业技术大学)