计算机网络安全问题与对策分析

——评《计算机网络安全实验指导》

随着互联网的普及和发展,计算机网络已经成为人们生活和工作中不可或缺的一部分。在给人们带来极大便利的同时,计算机网络也面临着日益严重的网络安全威胁,如病毒、黑客侵袭、数据泄密等。网络安全问题不仅给个人和企业带来巨大损失,也给整个社会造成严重危害。如何消除网络安全隐患,确保信息安全,已成为一个重要的课题。

维护计算机网络安全,既需要大量的网络安全理论知识,也需要很强的实践动手能力。实践操作对于深入理解和掌握计算机网络安全知识有十分重要的意义。笔者在践行甘肃省教育厅2023年高校教师创新基金项目(2023A-225)过程中,认真学习了《计算机网络安全实验指导》一书,该书设计了大量的实验项目来帮助理解计算机网络安全原理和技术,共分为14个章节。分别介绍了计算机网络安全概论、密码学基础知识、认证与数字签名、PKI与数字证书、无线网络安全、IP及路由安全、传输层安全、DNS安全、Web应用安全、电子邮件安全、拒绝服务攻击及防御、网络防火墙、入侵检测与网络欺骗、恶意代码等计算机网络安全方面的知识,并通过相应的实验项目加深理解。

书名:计算机网络安全实验指导
编者:吴礼发
出版社:电子工业出版社
ISBN:9787121397790
出版时间:2020年10月
定价:59元

编者指出,网络安全对个人、企业和国家具有十分重要的意义。计算机网络安全是一个多层次、综合性的防护体系,需要结合多种安全技术进行合理配置和部署,包括密码学、防火墙技术、入侵检测系统等。实践是提高网络安全能力的关键,可以深入理解各种网络安全技术的原理和应用,提高解决实际问题的能力。网络安全不是一次性的工作,而需要持续的维护和管理,要时刻保持警惕,及时发现和处理安全威胁,定期进行安全审计和风险评估,不断完善和更新安全策略和防护体系。

笔者认为,计算机网络安全关乎国家的社会稳定和安全,需要引起高度重视。目前,计算机网络安全主要存在如下问题。首先是病毒和恶意软件的传播。计算机病毒和恶意软件是网络安全的主要威胁之一。它们通过电子邮件、下载文件、即时通信工具等途径传播,破坏计算机系统,窃取用户信息,甚至导致整个网络瘫痪。近年来,新型病毒和恶意软件层出不穷,传播速度越来越快,防范难度越来越大。其次是黑客攻击。黑客攻击是指通过技术手段非法侵入他人计算机系统,窃取、篡改或破坏数据的行为。黑客攻击手段多样,包括拒绝服务攻击、漏洞利用、社会工程学等。黑客攻击不仅使个人用户造成损失,还可能对企业和国家安全构成威胁。最后是信息泄露。信息泄露是指用户的个人信息、企业的商业机密等敏感信息在网络中被非法获取和使用。信息泄露的原因有很多,包括用户自身安全意识不足、企业安全防护措施不到位等。信息泄露不仅侵犯了用户的隐私权,还可能导致企业竞争力下降,甚至引发法律纠纷。针对以上安全问题,笔者建议采取以下策略应对。一是提高安全意识。提高个人和企业的安全意识是防范网络安全问题的第一步。用户还应定期更新操作系统和应用程序,安装并更新杀毒软件,不随意下载不明来源的文件。企业应加强员工的网络安全培训,制定并执行严格的信息安全政策。二是加强技术防护。技术防护是防范网络安全问题的重要手段。用户应使用复杂的密码,并定期更换密码,且避免使用相同的密码。企业建立完善的网络安全防护体系,包括防火墙、入侵检测系统、数据备份等。此外,企业还应加强对新兴技术的关注和研究,提高应对新型安全威胁的能力。三是加强法律法规建设。政府应加强对网络安全法律法规的建设和完善,为网络安全提供有力的法治保障。政府还应加大对网络犯罪的打击力度,严惩网络犯罪分子,维护网络安全秩序。同时,政府应推动国际合作,共同应对跨国网络犯罪。四是建立健全应急响应机制。建立健全应急响应机制是应对网络安全问题的关键。用户和企业应制定应急预案,明确应急响应流程和责任人。一旦发生网络安全事件,应立即启动应急预案,尽快控制损失,恢复正常运行。此外,用户和企业还应定期进行应急演练,提高应对网络安全事件的能力。

总之,计算机网络安全问题是一个长期、复杂的问题,需要全社会共同努力来应对。只有加强政府、企业和个人的合作,共同提高网络安全意识,加强技术防护,完善法律法规建设,建立健全应急响应机制,发挥社会力量作用,才能共同维护计算机网络的安全运行。

(张玮/兰州资源环境职业技术大学 信息工程学院/副教授)