新时代下通信网络技术的安全发展研究
——评《通信网络安全》

近年来,通信网络技术迅速发展,互联网、物联网、云计算、大数据等新兴技术的广泛应用,使得人们的生活和工作方式发生了深刻变化。然而,随着通信网络技术的普及,网络安全问题也日益突出。网络攻击、数据泄露、病毒传播等安全事件频发,给个人和企业带来了巨大的经济损失和隐私泄露风险。因此,加强通信网络技术安全发展已经成为当前的重要任务。

笔者在从事通信网络技术安全工作的过程中,认真阅读了《通信网络安全》一书。该书共5个模块,13个任务。模块1是通信网络基础知识,介绍了通信、通信网络、通信系统相关知识。模块2是TCP/IP基础,探讨了网络拓扑与TCP/IP的应用。模块3是网络安全,研究了安全传输与VPN构建。模块4是网络设备安全,介绍了交换机与路由器的配置。模块5是通信安全,阐述了日常生活中信息安全方面的相关知识。

书名:通信网络安全
编者:李可,黄博
出版社:北京理工大学出版社
ISBN:9787576318029
出版时间:2022年11月
定价:65元

编者指出,通信网络安全是保障国家安全、社会稳定和经济发展的重要基石,必须高度重视并加强防范。网络安全是实现通信网络安全的重要手段,是实现安全传输的载体。网络设备安全是保障通信网络安全的基础,了解交换器、安全路由器等设备配置可有效提高网络安全性。通信网络也面临着计算机病毒等各种安全威胁和攻击,需要采取相应的防范措施来保障通信网络的安全性。

笔者认为,当今通信网络技术安全发展主要面临以下挑战。一是网络攻击威胁不断增加。黑客组织、网络犯罪分子等恶意势力利用各种手段攻击通信网络,如病毒、蠕虫、勒索软件等恶意代码的传播,窃取用户数据、破坏系统设施等行为屡屡发生,给企业和个人造成损失。二是数据安全保护难度加大。随着大数据、云计算等技术的普及,大量敏感数据在通信网络中传输和存储,如何确保数据的机密性、完整性和可用性成为一个难题。数据泄露、滥用等风险日益严重,个人隐私和企业机密难以得到有效保护。三是基础设施安全面临考验。关键信息基础设施是经济社会运行的神经中枢,保障其安全是国家安全的重要组成部分。然而,随着基础设施规模的扩大和复杂度的增加,如何确保基础设施的安全稳定运行,面临着巨大考验。四是网络安全防御能力不足。尽管网络安全技术和产品不断发展,但网络安全防御能力仍然存在不足。一些企业和个人缺乏有效的安全防护措施,无法及时发现和应对网络攻击威胁,导致安全事件频发。尽管通信网络技术安全发展面临着诸多挑战,但也同样存在着许多机遇。首先,随着人们安全意识的提高和国家对网络安全法规的不断完善,网络安全市场需求将持续增长。这将为通信网络技术安全发展提供广阔的市场空间。同时,政府和企业也将加大网络安全投入,推动通信网络技术安全的发展。其次,新兴技术的快速发展将为通信网络技术安全发展带来新的机遇。例如:人工智能技术在网络安全领域的应用将有助于提高网络安全防御的效率和准确性。区块链技术也可以用于数据安全保护,确保数据的完整性和可信度。最后,国际合作将成为通信网络技术安全发展的重要推动力。各国在网络安全领域的合作将有助于共同应对网络安全威胁,推动全球通信网络技术安全的发展。

针对新时代下通信网络技术的安全发展,笔者建议:一是加强网络安全教育和培训。提高公众和企业对网络安全的认识和重视程度,增强网络安全意识和技能,培养专业的网络安全人才。二是加大科技研发投入。推动通信网络技术安全领域的科技创新,加强关键信息基础设施的保护,提高网络安全防御能力和应急响应能力。三是强化国际合作与交流。积极参与国际网络安全合作与交流活动,共同应对网络安全威胁,共享网络安全信息和经验,推动全球通信网络技术安全的发展。四是完善法律法规体系。制定和完善网络安全法律法规,明确网络安全责任和义务,加大对网络犯罪的打击力度,保护个人和企业合法权益。五是建立网络安全保障机制。建立完善的网络安全保障体系,明确各部门职责和协作机制,加强网络安全监测和预警,及时发现和应对安全威胁。

综上,在新时代下通信网络技术安全发展面临着前所未有的机遇和挑战。应加强国际合作与交流,共同推动全球通信网络技术安全的发展,确保个人和企业的信息安全,维护国家安全和社会稳定。

(杨泽辉/山西省财政税务专科学校 大数据学院/副教授,副院长;李琳/山西省财政税务专科学校/副教授)