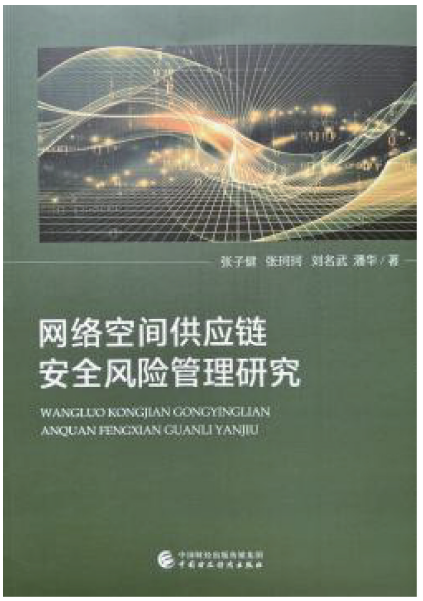
网络空间风险因素及安全管理对策
——评《网络空间供应链安全风险管理研究》

网络空间已非单纯的技术疆域,而是大国博弈的角斗场、经济运行的神经中枢与社会运行的数字底座。纵观当下,网络空间的风险因素与应对之策,实则是一场关于生存与发展的双重博弈,必须以雷霆手段斩断隐患,以系统思维构筑防线。

在数字化浪潮席卷全球的今天,供应链早已不仅是物流的血脉,更是网络战的"软肋"。《网络空间供应链安全风险管理研究》一书以国家关键信息基础设施为锚点,系统构建了一套从风险识别、评估到管控的全链路闭环理论。作者以演化博弈、系统动力学等硬核数学工具为手术刀,深度剖析了风险在网络供应链中的传导机制与脆弱性根源。书中不仅在理论上通过"熵"与复杂网络理论量化不确定性,更在实践层面针对仿冒治理、信任传递、弹性能力建设等棘手难题,给出基于 Shapley 值法、激励契约等具体的量化决策模型,为政府监管与企业防御提供极具价值的"中国方案",引导网络空间安全领域从被动防御迈向主动免疫。



书名:网络空间供应链安全风险管理研究
作者:张子健,张珂珂,刘名武,潘华
出版社:中国财政经济出版社
ISBN:9787522335704
出版时间:2024年12月
定价:78元

该书作者指出,当代数字大厦的基石是各项数字技术,从芯片制造到操作系统,从路由器到数据库,各种技术构建了数字网络时代的根基,因此,技术风险是显而易见的。这种底层技术的对外依赖,使得供应链污染成为一种极具隐蔽性和毁灭性的攻击方式。攻击者不再需要正面强攻坚固的城墙,而是选择在上游的开源组件、中间件甚至硬件固件中植入恶意代码,通过"上游注入-中游放大-下游激活"的链式反应,引发系统性的崩塌。在数字世界中,一些非法机构与黑客,利用技术设计制造病毒,攻击供应链,甚至进行网络勒索欺诈,这不仅是数字的跳动,更是国家安全防线的溃败。针对这一系统性风险,必须筑牢"自主可控"的钢铁长城,绝不能把命运交到别人手中。首先,必须实施关键信息基础设施的"国产化替代"攻坚战,集中力量突破核心电子元器件、高端芯片、操作系统操作条件基础软件等"卡脖子"技术,构建安全可控的信息技术体系,从根源上消除"后门"隐患。其次,要建立全生命周期的供应链安全审查机制,对供应商进行严格的安全画像与风险评估,将安全触角延伸至代码级和硬件级,确保采购的每一个产品、每一行代码都经得起最严苛的审视。

笔者认为,技术风险因素防控更多依赖于技术进步,而人的疏忽与安全意识缺乏等风险因素则需加强技术与安全意识培训、监管与引导。在网络安全事故中,有相当一部分与人为因素直接关联,具体包括弱口令设置随意、随意点击钓鱼邮件、不经甄别安装带有后门的 APP 等,尤其是一些企业的工作人员安全意识不足,在工作中滥用网络权限,甚至进行违规操作,使得人的因素成为安全管理中的最薄弱环节。甚至在一些企业内部员工在利益驱动下,沦为网络安全的"内鬼",给企业增加巨大网络风险。数据信息作为数智时代的高价值资产,亦面临着巨大的网络安全风险。在数字化转型的社会与产业发展中,如果缺乏底层约束,数据资产底数不清、分级不明,大量敏感数据甚至核心商业机密、个人隐私如同裸奔般暴露在公网上。错误的配置、未授权的访问、缺乏加密的传输,这些"低级错误"在海量暴露的资产面前被无限放大,一旦被黑产团伙利用,会直接给企业和个人带来巨大损失。若想根治这一顽疾,必须构建以人为本、以数据为核心的安全治理生态。在网络授权层面须全面推行"零信任"架构,打破"内网即安全"的幻想,对任何主体、任何设备、任何时间的访问请求都进行严格的身份认证与动态授权,并强制实施多因素认证,利用生物识别、行为分析等手段锁死非法入侵的通道。在内部管理层面则有必要开展全民网络安全素养的"扫盲行动",将安全培训常态化、实战化,通过钓鱼演练、红蓝对抗等方式,让每一位员工都成为一道"人形防火墙",与此同时要压实主体责任,建立严格的问责机制与操作审计体系,对违规行为"零容忍",从人的角度守护网络安全。

总之,网络空间安全是一场没有硝烟的持久战。唯有以坚定的政治意志为基础,以硬核的技术自主为武器,以严密的法治体系为保障,才能在数字化的浪潮中掌握安全主动权,让网络空间真正成为驱动国家发展的新引擎,这既是数字网络技术发展的方向,亦是数字科技产业可持续发展的根基。

(张艳丽/山西晋中理工学院/讲师)