数智背景下电子信息安全与管理应用策略

——评《电子信息与安全管理》

当下,数字智能技术已如水电般渗透至社会肌理,数据成为核心资产的同时,泄露与勒索风险亦如影随形。传统“防火墙”式防御在复杂攻击面前日渐吃力,安全不再仅是技术补丁,更是业务连续性的底线。在此语境下,探讨电子信息安全与管理应用,旨在打破技术与业务的壁垒,既关乎隐私保护,亦是医疗、金融等关键领域数字化转型的基石,唯有构建“人+制度+技术”的协同防线,数据应用才能在数智浪潮中行稳致远。

书名:电子信息与安全管理
作者:吴亚洁
出版社:吉林科学技术出版社
ISBN:9787574412361
出版时间:2024年3月
定价:70元

《电子信息与安全管理》一书基于技术演进与安全防护为主线,从微电子、光电子等基础技术切入,再从应用场景角度系统梳理了电子信息技术发展脉络,延伸至电子支付、金融科技等应用要求。以在线信息支付体系为例,既探讨了其底层安全机制,亦全面分析了其安全特征、防护技术及发展趋势。全书内容兼顾理论深度与实践价值,覆盖当下技术特点与未来技术发展趋势,突出“技术+安全”双维度特色,助力读者理解数字化时代的信息管理逻辑。

该书作者指出,堡垒容易从内部被攻破,电子信息系统亦是如此,因此,必须粉碎“内网即安全”的幻想,全面落地“零信任”架构。在万物互联的今天,企业的物理边界早已模糊。远程办公、移动终端、供应链协作让威胁无孔不入,内部威胁与外部攻击的界限不再分明。若还固守着“城堡式”防御,一旦防线被突破,攻击者便能长驱直入,如入无人之境。因此,技术视角必须从“网络位置”转向“身份与行为”。“零信任”不是一句口号,而是“永不信任,始终验证”的铁律。要实施最小权限原则,哪怕是首席执行官的账号,也不应默认拥有对核心数据库的访问权,每一次访问都必须经过多因素认证与环境感知的严苛校验。要利用微隔离技术,将庞大的网络切割成微小的“安全孤岛”,即使某个节点沦陷,也能将威胁锁死在方寸之间,防止威胁横向移动。更关键的是,需要引入人工智能(Artificial Intelligence,AI)驱动的行为分析,实时阻断异常流量、非常规时间的访问。这不仅是技术的升级,更是安全思维的革命——要做的不是“防住所有攻击”,而是让攻击者在每一步都付出惨重代价,使其知难而退。

笔者认为,信息技术安全工作要求将数据视为核心资产,构建全生命周期的“数据保险库”。在大数据时代,数据是新的石油,也是黑客眼中的金矿。勒索软件的肆虐、供应链的污染、内幕交易的窃取,无不指向数据安全的脆弱性。作为专业人员,不能仅满足于防火墙的拦截,必须深入数据的“肌理”。要建立数据分级分类制度,将绝密、机密、公开数据区分对待,把80%的防御资源集中在那20%最核心的资产上。在技术层面,加密不再是可选项,而是必选项。要推广同态加密、量子加密等前沿技术,确保数据在传输、存储甚至使用过程中始终以密文形态存在。针对日益严峻的隐私泄露风险,隐私计算(如联邦学习、差分隐私)将成为标配,实现“数据可用不可见”,在挖掘数据价值的同时严守隐私边界。此外,数据备份必须从“定期备份”升级为“瞬时恢复”,利用磁盘镜像与远程容灾技术,确保在灾难发生的毫秒级内恢复业务,因为在数字经济中,停机一分钟的损失可能就是天文数字。再坚固的盾牌也挡不住内部人员的无意泄露,再先进的AI也可能被更高级的AI欺骗。必须清醒地认识到,人是安全链条中最薄弱的一环,也是最坚固的一环。一方面,要通过持续的红蓝对抗、钓鱼演练,提升全员的“安全免疫力”,让每一位员工都成为威胁的“传感器”;另一方面,要主动拥抱AI,利用大模型进行威胁情报分析与漏洞挖掘,将防御能力从“人肉运维”提升至“智能自治”。数智时代的安全战场,不仅是技术的较量,更是意志与智慧的博弈。不能做被动挨打的“修墙工”,而要做主动出击的“数字守堤人”。

总之,数智时代的电子信息安全是一场没有硝烟的战争。作为专业技术人员,不能仅做修补漏洞的“消防员”,更要做业务发展的“护航员”。要用零信任架构重构信任基石,用数据治理激活要素价值,用智能技术对抗黑产攻击。唯有如此,才能在数字化的惊涛骇浪中,为企业筑起一道不仅能抵御风暴,更能将风暴转化为动力的钢铁长城。安全,不再是成本的累赘,而是数字经济时代最昂贵的信任资产。

(相智卓/石河子大学机械电气工程学院)