数智时代计算机信息安全管理策略

——评《计算机技术应用及信息安全管理研究》

数智时代,数据成为核心生产要素,信息安全已成为维护个人权益、企业运营及国家安全的关键基石。随着5G、物联网、人工智能的普及,网络攻击手段不断升级,数据泄露、系统瘫痪等风险日益凸显。数字化转型加速,构建动态防护、主动防御的信息安全体系,不仅是技术发展的必然要求,更是保障经济社会稳定运行的战略需求。

数智化背景下,可通过策略、技术及人员协同,保障信息系统、数据资产及网络空间,构建安全保障体系。《计算机技术应用及信息安全管理研究》全书共7章,架构严谨,从基础理论到前沿应用层层递进。第1章梳理了计算机发展脉络、类型划分及应用场景,奠定研究基石;第2章聚焦硬件系统,详述中央处理器、存储器、输入输出设备及总线技术的技术细节与维护实践;第3章转向软件系统,涵盖传统软件架构、网络软件系统及分层开发技术的应用逻辑;第4章创新探讨了网络技术前沿,融合人工智能、虚拟化、云计算等技术的实践路径;第5章—第7章深入信息安全领域,从密码学、身份认证、访问控制等核心技术,到防火墙、入侵检测、虚拟专用网等防护手段,再到病毒防范策略,形成"技术-防护-管理"的完整闭环。

书名:计算机技术应用及信息安全管理研究
作者:刘艳丽,曾光,杨倩
出版社:中国商务出版社
ISBN:787510344329
出版时间:2023年5月
定价:60元

作者指出,数智时代的数据价值挖掘与安全风险呈现螺旋式上升特征,需突破传统静态防护思维,建立覆盖数据全生命周期的动态防护机制。在数据采集阶段,应强化源头治理,通过数字水印、区块链存证等技术实现数据血缘追溯,确保采集设备、接口、日志的合规性审计可查。例如:工业物联网场景中,需对传感器数据采集频率、精度进行动态校准,防止恶意节点注入虚假数据导致决策偏差。数据存储环节需突破单一加密限制,实施分级分类存储策略。敏感数据应采用量子加密、同态加密等前沿技术实现"存储即加密",同时,结合零信任架构实现访问控制粒度细化至字段级。如在金融行业,客户交易数据作为需要高度保密的核心数据,需在分布式存储系统中实现多副本加密分割,结合访问行为基线分析,实时阻断异常访问请求。在数据传输阶段,为防止黑客破解,有必要构建抗量子计算攻击的传输通道,结合5G切片技术实现业务流与安全策略的动态绑定,确保数据在传输过程中实现完整性、机密性双重保障。在数据处理与共享环节,需根据相关法律引入隐私计算技术,对数据进行脱敏脱密处理,达到"数据可用不可见"的目的,如医疗科研机构在共享病例数据时,通过差分隐私技术添加统计噪声,在保护个体隐私的同时保障数据真实有效。

笔者认为,在数智时代背景下,计算机信息安全管理需构建多维协同的防护体系,以应对数据爆炸、智能算法滥用及网络攻击常态化等挑战。数据资产化管控是基础,需建立动态数据分类分级制度,对核心业务数据、用户隐私数据实施"最小必要"访问控制,采用量子加密、同态加密等技术强化传输与存储安全。网络防御需向智能化转型,传统防火墙、入侵检测系统需与人工智能(Artificial Intelligence,AI)驱动的威胁情报平台联动,通过机器学习分析异常流量模式,实现主动式防御。零信任架构的深化应用尤为关键,需打破"内网安全"幻觉,对用户、设备、应用实施持续身份验证与动态权限调整,尤其在混合云环境中确保"永不默认信任"。人员与制度层面需双管齐下:一方面,定期开展红蓝对抗演练,模拟钓鱼攻击、供应链渗透等场景,提升员工安全意识与应急响应能力;另一方面,完善安全合规体系,结合《数据安全法》《个人信息保护法》等法规,制定可量化的安全考核指标,将安全责任嵌入业务部门关键绩效指标。技术治理需兼顾创新与风险,对AI算法本身需开展安全评估,防止训练数据污染导致决策偏差,或模型被逆向攻击泄露敏感信息。基于上述策略,形成"监测-响应-进化"的闭环。通过安全运营中心实时汇总日志数据,结合AI分析预测潜在威胁,并定期复盘安全事件,动态调整防护策略,确保在数智时代的复杂环境中保持韧性。

总之,数智浪潮奔涌向前,信息安全已成时代命题。从数据采集的源头治理到销毁的彻底清除,从硬件维护的精益求精到算法治理的未雨绸缪,每一环节都需精密协同,因此,既要以技术创新筑牢动态防护之盾,更要以制度规范与人员信息安全意识提升编织韧性之网。

(刘大海/唐山幼儿师范高等专科学校/副教授)