网络信息化建设存在的安全问题和措施分析

苗 森
新疆维吾尔自治区战略和应急物资保障服务中心（乌鲁木齐中央级救灾物资储备库） 新疆 乌鲁木齐 830000

摘 要：在数字化浪潮席卷全球的今天，网络信息化建设已成为驱动社会经济发展、提升国家治理能力的核心引擎。然而，伴随着信息基础设施的日益普及和数据价值的空前凸显，网络安全威胁也呈现出前所未有的复杂性、隐蔽性和破坏性。本文系统性地剖析了当前网络信息化建设过程中面临的主要安全挑战，从物理层、网络层、系统层、应用层到数据层，全面梳理了由技术漏洞、管理缺陷、人为因素及外部攻击共同构成的多层次风险矩阵。在此基础上，论文提出了一套“技术、管理、法律、意识”四位一体的综合防护体系。该体系强调以纵深防御为技术核心，以全生命周期安全管理为制度保障，以健全的法律法规为准绳，并以全民网络安全素养的提升为根基。研究表明，唯有通过这种多维度、系统化、协同化的安全策略，才能有效应对日益严峻的网络安全形势，为国家关键信息基础设施、企业核心业务和公民个人信息构筑起一道坚不可摧的安全屏障。

关键词：网络信息化；安全问题；纵深防御；数据安全；安全管理体系

引言

二十一世纪是信息的时代，网络信息化建设的深度与广度，已成为衡量一个国家现代化水平和综合国力的关键指标。从智慧城市、数字政府到工业互联网、金融科技，信息化的触角已延伸至社会生产生活的每一个角落，极大地提升了效率、便利了生活、激发了创新。然而，“双刃剑”的效应同样显著。在享受信息化红利的同时，我们所依赖的网络空间正面临着来自四面八方的安全威胁。这些威胁不仅可能导致个人隐私泄露、企业商业秘密失窃，更可能引发关键基础设施瘫痪、金融秩序混乱乃至国家安全危机。斯诺登事件揭示了国家级网络监控的无孔不入，而层出不穷的勒索软件攻击则让无数企业和机构蒙受巨大经济损失。这深刻地警示我们：没有网络安全，就没有国家安全，就没有经济社会的稳定运行。因此，深入探究网络信息化建设中存在的安全问题根源，并构建一套科学、有效、可持续的防护措施体系，具有极其重要的现实意义和战略价值。本文旨在超越零散的现象描述，从系统工程的视角，对这一重大课题进行深入的理论分析。

1 网络信息化建设中的主要安全问题

1.1 物理与环境安全风险

网络信息化系统的根基在于其物理载体——服务器、交换机、存储设备以及承载它们的数据中心。这些设施本身极易受到物理环境和人为破坏的威胁。自然灾害如地震、洪水、火灾、雷击等，可能直接摧毁硬件设备，导致服务中断和数据永久丢失。电力供应的不稳定性，如电压波动、瞬间断电，也可能损坏精密的电子元件或造成数据写入错误。此外，物理访问控制的疏忽，如未授权人员进入机房、设备被盗或被恶意植入硬件后门（如“USB杀手”或微型窃听装置），都会给整个信息系统带来毁灭性的打击。这类风险往往被忽视，但却是所有上层安全防护的前提和基础。

1.2 网络通信层安全威胁

网络层是信息传输的高速公路，也是攻击者最常利用的通道。首先，协议自身的脆弱性是根本问题。例如，TCP/IP协议族在设计之初并未充分考虑安全性，其地址欺骗（IP Spoofing）、会话劫持（Session Hijacking）等漏洞至今仍是许多攻击的基础。其次，网络边界防御面临严峻挑战。防火墙、入侵检测/防御系统（IDS/IPS）等传统边界设备，在面对高级持续性威胁（APT）时往往显得力不从心[1]。APT攻击者通常采用0day漏洞、鱼叉式钓鱼邮件等手段，绕过边界防线，在内部网络中长期潜伏、横向移动，窃取核心数据。再者，无线网络的普及带来了新的安全隐患。开放的Wi-Fi热点、弱加密的WEP/WPA协议，使得中间人攻击（Man-in-the-Middle Attack）变得异常容易，攻击者可以轻松截获和篡改用户与服务器之间的通信内容。

1.3 操作系统与应用软件漏洞

操作系统和应用软件是用户与硬件资源交互的桥梁，其安全性直接决定了整个系统的安危。然而，任何复杂的软件系统都不可避免地存在漏洞。这些漏洞可能是编码错误、逻辑缺陷或配置不当所致。攻击者通过精心构造的恶意输入（如缓冲区溢出、SQL注入、跨站脚本XSS），可以利用这些漏洞执行任意代码、获取系统最

高权限（提权）、窃取敏感数据或使服务崩溃（拒绝服务DoS）。开源软件的广泛应用虽然促进了创新，但也因其代码公开，使得漏洞一旦被发现，便可能被大规模利用。供应链攻击更是将风险前置，攻击者通过污染软件开发工具链或在合法软件更新包中植入后门，从而实现对海量终端的精准打击。

1.4 数据安全与隐私泄露

在信息化时代，数据已成为最具价值的战略资产。因此，数据安全问题尤为突出。一方面，静态数据（存储在数据库、硬盘中的数据）面临未授权访问和窃取的风险。如果数据库缺乏严格的访问控制策略，或者加密密钥管理不善，一旦服务器被攻破，海量敏感数据将暴露无遗。另一方面，动态数据（在网络中传输的数据）若未采用强加密（如TLS 1.3），则极易被窃听和篡改[2]。此外，大数据和人工智能技术的应用，使得通过关联分析、数据挖掘等手段，从看似无害的匿名化数据中重新识别出个人身份成为可能，这构成了对个人隐私的深层次威胁。云服务的普及也带来了数据主权和跨境流动的新挑战，用户数据的物理位置和管辖权变得模糊不清。

1.5 管理与人为因素缺陷

技术并非万能，管理上的短板往往是安全链条中最薄弱的一环。许多安全事件的根源并非高深的技术攻击，而是简单的管理疏忽。例如，弱密码策略、长期不更新的默认口令、过度宽松的权限分配、缺乏定期的安全审计和日志分析等。员工的安全意识淡薄同样是巨大隐患。社会工程学攻击（如钓鱼邮件、电话诈骗）正是利用了人性的弱点，诱骗员工主动泄露凭证或执行恶意操作。内部人员的恶意行为，无论是出于经济利益还是报复心理，其造成的破坏往往比外部攻击更为严重，因为内部人员天然拥有更高的信任级别和更深入的系统知识。

2 构建综合性的网络安全防护体系

2.1 强化技术防护：构建纵深防御体系

面对多维度的威胁，单一的安全产品已无法胜任。必须构建一个覆盖“预测、防护、检测、响应”全链条的纵深防御（Defense in Depth）体系。（1）边界防护加固：部署下一代防火墙（NGFW），其不仅具备传统包过滤功能，还能深度识别应用层流量、集成IPS、防病毒和沙箱技术。同时，实施严格的网络分段（Network Segmentation），将关键业务系统置于独立的安全域，限制攻击者在网络内部的横向移动能力。（2）主机与应用安全：在服务器和终端上强制推行最小权限原则，及时安装安全补丁，部署主机入侵防御系统（HIPS）和端点检测与响应（EDR）解决方案。对Web应用，应实施Web应用防火墙（WAF），并遵循安全开发生命周期（SDL），在软件开发的每个阶段嵌入安全实践，从源头上减少漏洞。（3）数据安全为核心：实施数据分类分级保护策略，对不同级别的数据采取差异化的保护措施。全面推广数据加密，包括静态数据加密（At-Rest Encryption）和传输中数据加密（In-Transit Encryption）。采用令牌化（Tokenization）或格式保留加密（FPE）等技术处理敏感字段，即使数据被窃取也无法直接利用。建立完善的数据备份与灾难恢复（DR）机制，确保在遭受勒索软件攻击或物理灾难后能够快速恢复业务[3]。（4）主动威胁狩猎：超越被动的告警响应，建立专业的威胁狩猎（Threat Hunting）团队，利用SIEM（安全信息与事件管理）平台汇聚全网日志，结合威胁情报（Threat Intelligence），主动搜寻潜伏在内部的未知威胁。

2.2 完善安全管理体系：落实全生命周期管理

技术是骨架，管理是血肉。必须建立一套覆盖信息化项目全生命周期的安全管理体系。（1）安全组织与制度：设立专门的网络安全管理机构，明确各级人员的安全职责。制定并严格执行涵盖物理安全、网络安全、数据安全、人员安全等方面的规章制度和操作规程。（2）风险评估与合规：定期开展全面的信息安全风险评估，识别资产、威胁、脆弱性和风险，并据此制定风险处置计划。确保信息化建设符合国家及行业的相关法律法规和标准（如《网络安全法》、等级保护2.0、GDPR等）。（3）安全开发生命周期（SDL）：将安全要求嵌入到系统规划、设计、开发、测试、部署、运维直至废弃的每一个环节。在设计阶段进行威胁建模，在开发阶段进行代码审计，在上线前进行渗透测试。（4）应急响应与持续改进：制定详尽的网络安全事件应急预案，并定期进行演练。建立安全运营中心（SOC），实现7x24小时的安全监控、分析和响应。通过对安全事件的复盘和分析，不断优化安全策略和技术措施，形成PDCA（计划-执行-检查-改进）的闭环。

2.3 健全法律法规与标准规范

法律法规是网络安全的基石和准绳。国家层面需要不断完善网络安全法律体系，明确网络空间各方的权利、义务和责任，加大对网络犯罪的惩处力度，为网络安全工作提供强有力的法治保障。同时，大力推动和采纳国际国内先进的安全标准与最佳实践（如ISO/IEC 27001信息安全管理体系、NIST网络安全框架等），为各类组织提供可操作、可衡量、可审计的安全建设指南。通过法规和标准的双重驱动，营造一个公平、有序、安

全的网络环境。

2.4 提升全民网络安全意识与素养

人是安全体系中最活跃也是最不可控的因素。必须将网络安全教育常态化、普及化。（1）组织内部培训：对全体员工，特别是关键岗位人员，进行定期的、有针对性的网络安全意识培训。培训内容应包括识别钓鱼邮件、安全使用密码、保护移动设备、报告可疑活动等。通过模拟钓鱼演练等方式，检验和巩固培训效果。（1）社会公众教育：政府、媒体和教育机构应通力合作，通过多种渠道向公众普及基本的网络安全知识和防护技能，提升全民的网络素养和自我保护能力。让“网络安全为人民，网络安全靠人民”的理念深入人心。

3 面向未来的安全挑战与应对思路

3.1 新技术带来的新挑战

云计算、大数据、物联网（IoT）、人工智能（AI）等新技术的广泛应用，在赋能业务的同时，也引入了全新的安全范式。云安全的责任共担模型要求用户清晰理解自身与云服务商的安全边界。海量IoT设备的接入，因其普遍存在的弱口令、固件漏洞和缺乏安全更新机制，构成了巨大的攻击面，成为DDoS攻击的“僵尸”来源[4]。AI技术本身也可被用于发起更智能、更难以察觉的攻击，如生成逼真的深度伪造（Deepfake）内容进行欺诈，或利用机器学习算法自动化地寻找系统漏洞。应对这些挑战，需要发展与之匹配的安全技术，如零信任架构（Zero Trust Architecture）、基于AI的智能威胁检测、适用于IoT的轻量级安全协议等。

3.2 供应链安全的重要性日益凸显

现代信息系统高度依赖于复杂的软硬件供应链。任何一个环节的失守，都可能导致整个系统的沦陷。因此，必须将供应链安全纳入整体安全战略。这包括对供应商进行严格的安全资质审查，要求其提供软件物料清单（SBOM）以清晰掌握组件来源，建立供应链安全事件的应急响应机制，并积极推动自主可控核心技术的研发与应用，降低对外部供应链的过度依赖。

3.3 从被动防御到主动免疫

未来的安全防护将不再满足于被动地抵御已知威胁，而是要向主动免疫、内生安全的方向演进。这意味着安全能力应像生物免疫系统一样，内生于信息系统的设计和架构之中。通过可信计算、拟态防御等前沿技术，构建能够自我感知、自我诊断、自我修复和自我进化的能力，从根本上提升系统的抗攻击韧性和生存能力。

4 结语

网络信息化建设的安全问题是一个动态、复杂且永无止境的系统工程。它既涉及底层的物理设施和尖端的技术对抗，也关乎顶层的管理制度和全民的意识素养。本文通过对当前主要安全问题的系统梳理，提出并论证了“技术、管理、法律、意识”四位一体的综合防护策略。面对日新月异的网络威胁和不断涌现的新技术，任何单一的、静态的防御措施都将很快失效。唯有坚持系统思维，将安全理念贯穿于信息化建设的全过程、各方面，持续投入、不断创新、协同联动，才能在这场没有硝烟的战争中立于不败之地，真正筑牢国家、社会和个人在网络空间的安全基石，为数字经济的高质量发展保驾护航。

参考文献

[1]常志鹏,孙利宏.网络信息化建设存在的安全问题和措施分析[J].数字技术与应用,2024,42(11):52-54.

[2]潘彦宇.信息化建设中网络安全与维护策略[J].数字技术与应用,2026,44(01):73-75.

[3]陈洪波,赵稚萌.人工智能背景下网络安全信息化体系建设探究[J].办公自动化,2025,30(18):16-18.

[4]林雁军.信息化建设中网络安全与维护策略探究[J].中国新通信,2025,27(10):7-9.