计算机信息系统网络安全现状及分析

张在霞
山东省沂水县沂城街道办事处　山东　临沂　276400

摘　要：随着信息技术的飞速发展，计算机信息系统在各领域广泛应用，网络安全问题日益严峻。复杂多样的网络攻击手段、系统漏洞与配置风险以及人员安全意识薄弱等问题，严重威胁着系统安全稳定运行。为此，需强化漏洞管理与补丁更新，构建多层次防御体系，加强数据安全保护，并提升人员安全素养。通过系统性策略实施，可有效降低安全风险，保障计算机信息系统网络安全。

关键词：计算机信息系统；网络安全；现状

引言

随着信息技术深入发展，计算机信息系统网络安全重要性与日俱增。当下网络安全环境愈发复杂，新型攻击手段不断涌现，系统漏洞与配置风险因技术架构复杂性持续存在，而人员安全意识不足更放大了安全隐患。本文聚焦计算机信息系统网络安全现状，分析攻击手段、漏洞风险及人员因素等问题，进而探讨强化漏洞管理、构建防御体系等提升安全水平的策略，为保障信息系统安全提供参考。

1 计算机信息系统网络安全概述

计算机信息系统网络安全聚焦于保护系统内信息资源免受各类威胁，涵盖机密性、完整性与可用性三大核心目标，贯穿数据传输、存储及处理的全生命周期。随着信息技术的飞速发展，计算机系统深度融入社会生产生活各领域，从企业核心业务数据到个人隐私信息，海量数据的数字化流转使得网络安全风险与日俱增。网络安全威胁的形态呈现多元化与复杂化特征。恶意软件作为常见攻击手段，通过病毒、蠕虫、木马等形式入侵系统，篡改、窃取数据或控制设备。勒索软件更是凭借加密锁定数据的方式，迫使受害者支付赎金以换取解密。网络攻击利用系统漏洞展开，如操作系统、应用软件的安全缺陷，一旦被黑客发现并利用，便可能导致权限提升、数据泄露等严重后果。钓鱼攻击通过伪装成合法网站或邮件，诱使用户主动泄露敏感信息，社会工程学手段的运用进一步增强了攻击的隐蔽性与欺骗性。防御网络安全威胁依赖于技术手段与安全架构的协同构建。访问控制技术通过身份认证、授权机制限制非法用户对系统资源的访问，确保只有经过授权的主体能够获取对应数据。加密技术则通过数据的加密处理，即使信息在传输或存储过程中被截获，非授权者也无法解读其内容，保障数据机密性。入侵检测与防御系统实时监测网络流量与系统行为，及时发现异常活动并采取阻断措施。在安全架构层面，零信任模型打破传统网络边界防护理念，以“永不信任，始终验证”为原则，对所有访问请求进行严格身份验证与权限控制，构建更为严密的安全防护体系。网络安全并非静态的防御状态，随着新技术的不断涌现与攻击手段的持续演进，安全防护体系需持续迭代更新，以应对动态变化的安全挑战。

2 计算机信息系统网络安全现状分析

2.1 复杂多样的网络攻击手段

在数字化浪潮席卷全球的当下，计算机信息系统面临的网络攻击手段呈现出前所未有的复杂性与多样性。勒索软件作为极具破坏力的攻击形式，通过加密用户数据并索要赎金，给企业和个人带来严重的经济损失与业务中断风险。攻击者利用钓鱼邮件、恶意链接或漏洞植入勒索程序，一旦用户中招，整个系统的数据便会被加密锁定，如近期某制造企业因员工点击恶意邮件链接，导致核心生产数据被加密，生产线被迫停工数日，造成巨额经济损失。分布式拒绝服务（DDoS）攻击通过控制大量僵尸网络，向目标服务器发送海量请求，使其资源耗尽而无法正常响应合法用户访问。随着物联网设备的普及，攻击者能够利用大量存在安全漏洞的智能设备组建规模庞大的僵尸网络，发起超大规模的DDoS攻击，对在线服务、金融交易平台等关键信息系统构成严重威胁。高级持续性威胁（APT）攻击则以隐蔽性和持久性著称，攻击者通常经过长期的情报收集和精心策划，利用零日漏洞、社会工程学等手段渗透目标系统，在不被察觉的情况下窃取敏感数据或进行破坏活动。此类攻击往往针对政府机构、科研单位、金融企业等重要领域，因其攻击周期长、技术手段先进，难以被传统安全防护措施检测和拦截。供应链攻击也日益成为网络安全的新威胁。攻击者通过入侵软件开发商、硬件供应商等供应链

环节，在产品或服务中植入恶意代码，当用户使用受污染的产品或服务时，便会遭受攻击。这种攻击方式波及范围广，影响程度深，一旦得手，可能导致大量用户数据泄露或系统瘫痪[1]。

2.2 系统漏洞与配置风险

计算机信息系统的网络安全风险，很大程度上源于系统自身存在的漏洞以及不合理的配置。操作系统作为计算机系统的核心，其代码的复杂性和庞大性使得漏洞难以完全避免。从Windows系统到Linux系统，几乎每年都会被发现多个高危漏洞，这些漏洞若不及时修复，攻击者便可能借此入侵系统。例如，某些远程代码执行漏洞允许攻击者在未授权的情况下远程控制目标系统，获取敏感信息或进行恶意操作。应用软件同样面临严重的漏洞问题。无论是办公软件、数据库管理系统，还是各类Web应用程序，都存在被攻击的风险。跨站脚本（XSS）漏洞、SQL注入漏洞等常见的Web应用漏洞，能够让攻击者窃取用户会话信息、篡改数据库内容，甚至控制整个Web应用系统。数据库系统中的漏洞，如弱认证机制、权限配置不当等问题，可能导致数据泄露、被篡改或删除，给企业和用户造成不可估量的损失。除了系统和软件自身的漏洞，不合理的网络配置也是引发安全风险的重要因素。网络设备的默认配置往往存在安全隐患，如默认的用户名和密码、开放不必要的端口和服务等，这些都为攻击者提供了可乘之机。在企业网络环境中，若子网划分不合理、访问控制策略不严格，可能导致内部网络攻击的扩散，使得攻击者能够轻易地从一个受感染的设备横向渗透到整个企业网络，窃取更多敏感信息或破坏关键业务系统。网络设备的更新与维护不及时，也会导致其抵御新型攻击的能力下降，进一步加剧网络安全风险。

2.3 人员安全意识薄弱

人员安全意识薄弱是计算机信息系统网络安全防护体系中的关键薄弱环节。在日常工作中，用户往往对潜在的网络安全威胁缺乏足够的认知和警惕性。例如，使用简单易猜的密码是一种极为普遍的现象，部分用户甚至在多个系统和平台使用相同密码，一旦其中一个系统密码泄露，其他关联账户也将面临被盗取的风险。随意连接公共无线网络、在不可信的网站下载文件，以及不验证来源就打开邮件附件等行为，都为恶意软件的传播和网络攻击提供了便利条件。员工在操作计算机信息系统时，违反安全操作规范的情况屡见不鲜。为了图方便，一些员工会绕过安全验证流程，私自使用未经授权的移动存储设备接入工作计算机，这可能导致病毒、木马等恶意程序被引入企业内部网络，造成数据泄露或系统瘫痪。在企业远程办公场景中，员工若不采取有效的安全防护措施，如未使用安全的VPN连接，直接通过家庭网络访问企业内部系统，也会增加企业网络遭受攻击的风险。即使企业部署了先进的网络安全防护设备，人员的疏忽和不当操作仍可能使这些防护措施形同虚设。攻击者常常利用社会工程学手段，通过伪装成可信人员发送钓鱼邮件、拨打电话等方式，诱骗用户泄露敏感信息或执行恶意操作。由于员工缺乏对社会工程学攻击的识别能力，很容易上当受骗，成为网络攻击的帮凶。一旦攻击者获取到关键信息，如登录凭证、系统配置等，就能够突破企业的安全防线，对计算机信息系统造成严重破坏[2]。

3 提升计算机信息系统网络安全的策略

3.1 强化漏洞管理与补丁更新

（1）漏洞扫描作为漏洞管理的首要环节，需借助专业的自动化扫描工具，对操作系统、应用程序及网络设备进行深度检测。这些工具能够精准识别开放端口、错误配置以及已知漏洞，依据CVE（通用漏洞披露）标准生成详细报告，涵盖漏洞名称、等级、影响范围及修复建议。如扫描发现Web服务器存在SQL注入漏洞，可通过报告及时定位问题代码，为后续修复提供明确方向。（2）漏洞评估环节要结合业务系统的实际运行情况与数据敏感程度，对扫描出的漏洞进行优先级划分。对于影响核心业务、可能导致数据泄露或系统瘫痪的高危漏洞，必须立即处理；中低危漏洞则可在不影响业务连续性的前提下，安排合适时间修复。例如，在线支付系统中的漏洞应优先修复，而一些内部辅助系统的低危漏洞可稍后处理。（3）补丁更新工作要建立严格的测试机制，在将补丁部署到生产环境前，需在模拟环境中进行全面测试，验证补丁与现有系统的兼容性，避免因补丁冲突导致系统故障。制定详细的补丁更新计划，分批次、分阶段推进，监控更新过程中的系统状态，及时处理异常情况，确保漏洞修复工作安全、高效完成。

3.2 构建多层次防御体系

（1）网络边界防护是多层次防御体系的第一道防线，通过部署高性能防火墙，依据预设规则对进出网络的流量进行严格过滤，阻止非法访问与恶意流量。入侵检测与防御系统（IDS/IPS）实时监测网络流量，运用特征匹配、行为分析等技术，识别并阻断潜在的攻击行为，如DDoS攻击、端口扫描等，将威胁拦截在网络外部。（2）在内部网络层面，实施网络分段技术，依据业务功能、部门职能等因素，将网络划分为多个相对独立

的子网，限制不同子网间的非法访问，缩小攻击影响范围。例如，将财务部门网络与普通办公网络隔离，防止攻击者横向渗透。部署虚拟专用网络（VPN），为远程用户提供安全加密的访问通道，确保数据传输安全。（3）终端安全防护是网络安全防御体系的关键组成部分。在每台终端设备上部署专业的终端安全管理软件，可达成对设备的全方位实时监控与精细化管理，涵盖软件白名单精准管控、严格的终端准入控制、高强度数据加密等核心功能。定期开展安全基线检查，确保终端符合安全规范，杜绝其沦为攻击跳板，全方位保障网络安全[3]。

3.3 加强数据安全保护

（1）数据加密是保护数据安全的核心手段，针对静态数据，采用先进的加密算法，如AES（高级加密标准），对存储在硬盘、数据库中的敏感数据进行加密处理，即使数据存储介质丢失或被盗，攻击者也无法获取真实数据内容。对于传输中的数据，利用SSL/TLS协议建立安全连接，对数据进行加密传输，防止数据在网络传输过程中被窃取或篡改。（2）数据备份与恢复机制是数据安全的重要保障，制定合理的数据备份策略，根据数据重要程度与更新频率，选择全量备份、增量备份或差异备份方式，定期对数据进行备份，并将备份数据存储在异地安全位置，避免因自然灾害、火灾等物理因素导致数据丢失。定期进行数据恢复演练，验证备份数据的完整性与可用性，确保在数据遭受意外破坏时能够快速恢复业务运行。（3）访问控制机制严格限制用户对数据的访问权限，基于最小权限原则，根据用户的工作职责与业务需求，精确分配数据访问权限，只允许用户访问其工作所需的数据。采用多因素认证技术，结合用户名密码、生物特征、动态令牌等多种认证方式，增强用户身份验证的安全性，防止非法用户越权访问数据，有效保护数据资产安全。

3.4 提升人员安全素养

（1）通过持续开展多样化的安全培训活动，帮助人员深入了解网络安全威胁的形式与危害。培训内容涵盖常见的网络攻击手段，如钓鱼邮件、恶意软件、社会工程学攻击等的原理与防范方法，通过实际案例分析，让人员直观认识到安全风险。介绍数据泄露、系统瘫痪等安全事件带来的严重后果，增强人员的安全意识与责任感。（2）组织模拟实战演练，设置各类网络安全场景，如遭遇勒索软件攻击、数据泄露事件等，让人员在真实模拟环境中学习应急处理流程与方法。在演练过程中，指导人员如何快速响应、隔离受感染设备、启动备份恢复等操作，提升人员在面对突发安全事件时的应变能力与协作能力，确保能够迅速、有效地处理安全事件，降低损失。（3）建立安全意识文化氛围，在日常工作环境中通过内部宣传渠道，如公告栏、内部通讯软件等，定期推送网络安全知识与提示，潜移默化地强化人员的安全意识。鼓励人员之间分享安全经验与防范技巧，形成全员参与、共同维护网络安全的良好氛围，从人员层面筑牢网络安全防线[4]。

结语

综上所述，计算机信息系统网络安全现状受技术、管理及人员等多因素影响，面临严峻挑战。复杂攻击手段与系统固有漏洞威胁系统安全，人员安全意识薄弱加剧风险。提升网络安全需技术、管理与人员协同，强化漏洞管理、构建多层次防御体系、加强数据保护并提升人员素养，形成全方位安全防护体系，才能有效应对安全威胁，确保计算机信息系统安全、稳定、可靠运行。

参考文献

[1]孔建.计算机信息系统网络安全现状及分析[J].黑龙江科学,2022,13(10):100-102.

[2]苏艳.计算机信息系统网络安全与现状分析[J].信息技术时代,2022(9):63-65.

[3]陆培丰.探讨计算机信息系统网络安全现状及对策[J].大科技,2023(13):142-144.

[4]肖梦婷.浅谈计算机信息系统网络安全工程实施[J].建筑工程技术与设计,2020(13):2282.