计算机网络安全问题与防范策略探讨

张萧禹　刘明林
河北方维网络技术有限公司　河北　石家庄　050000

摘　要：随着数字化进程的深入推进，计算机网络安全已成为保障信息系统稳定运行与数据安全的核心议题。本文从网络安全的定义、核心目标及体系结构出发，系统剖析当前恶意代码攻击、网络攻击、数据泄露等主要安全威胁与风险隐患，深入探究技术、管理、人员及外部环境层面的根源问题。在此基础上，从技术防护、管理规范、人员培养三个维度提出针对性防范策略，构建多层次全方位的安全防护体系。研究成果可为提升网络安全防护能力、应对复杂网络安全态势提供理论参考与实践指导，助力筑牢数字化发展的安全屏障。

关键词：计算机网络；风险隐患；问题根源；防范策略

引言：在数字经济快速发展的当下，计算机网络已渗透到社会生产生活的各个领域，成为支撑经济社会运转的关键基础设施。但网络技术的普及与应用也伴随着各类安全风险，恶意攻击、数据泄露等安全事件频发，不仅威胁个人隐私与企业利益，更关乎公共安全与国家利益。网络安全的重要性日益凸显，如何有效应对网络安全问题、构建可靠的安全防护体系已成为亟待解决的重要课题。基于此，本文围绕计算机网络安全问题展开深入探讨，梳理安全威胁，剖析问题根源，提出科学有效的防范策略，为网络安全保障工作提供有益借鉴。

1 计算机网络安全概述

1.1 计算机网络安全的定义与内涵

计算机网络安全是通过技术与管理措施，保障网络系统及数据在运行、传输、存储全流程的安全可靠，防范潜在威胁与非法访问。其核心内涵涵盖技术防护、管理体系完善及人员意识提升，需兼顾软硬件稳定运行与数据安全可控，抵御外部攻击并防范内部操作风险，为数字化应用提供安全保障。

1.2 网络安全的核心目标

网络安全核心目标包括机密性、完整性与可用性，三者相互关联、缺一不可。机密性确保敏感信息仅授权主体可访问，保障个人隐私与各类数据安全；完整性保障数据在全流程不被篡改破坏，支撑决策有效性；可用性要求网络资源需时能正常服务，避免攻击或故障导致服务中断，保障企业经营与公共服务正常运转。

1.3 计算机网络安全体系结构概述

计算机网络安全体系结构是多层次全方位防护框架，涵盖多层面需求：物理层防护硬件设备与通信线路安全；网络层抵御攻击、过滤非法数据；传输层保障数据传输安全可靠；应用层防范应用程序漏洞风险。安全管理体系贯穿各层级，通过制度建设、流程规范与人员管理提供保障，形成技术与管理结合的全方位安全体系[1]。

2 当前计算机网络安全的主要威胁与风险隐患

2.1 恶意代码攻击

病毒需依附于其他程序才能传播，一旦激活便会破坏系统文件、占用系统资源，导致系统运行异常；蠕虫无需宿主程序，可通过网络自动复制传播，快速消耗网络带宽，造成网络拥堵甚至瘫痪；勒索软件则以加密用户数据为手段，向用户索要赎金，直接威胁数据完整性与可用性，尤其对企业、医疗机构等数据敏感单位影响极大，可能引发业务中断、经济损失等连锁反应。此类攻击的传播途径已覆盖邮件附件、恶意链接、移动存储设备等多个场景，防范难度持续提升。

2.2 网络攻击

黑客入侵通过利用系统漏洞、暴力破解等方式非法获取网络控制权，窃取敏感信息或篡改系统配置，对个人和企业的信息安全造成直接侵害；DDoS攻击通过控制大量僵尸主机向目标服务器发送海量请求，耗尽服务器资源，导致服务中断，常见于电商平台、游戏服务器等关键业务场景，直接影响商业运营与用户体验；SQL注入攻击则针对网站数据库漏洞，通过构造恶意SQL语句非法访问、篡改或删除数据库数据，可能导致用户信息泄露、网站被篡改等严重后果，是Web应用领域的主要安全威胁之一。

2.3 数据泄露与隐私侵犯风险

随着数字化进程加快，数据已成为核心生产要素，数据泄露与隐私侵犯风险愈发突出。此类风险既可能源于外部攻击，也可能因内部管理疏漏导致，如员工违规操作、数据备份不当等。个人信息、商业机密、政务数据等敏感数据一旦泄露，不仅会侵犯个人隐私权益，还

可能给企业带来商业损失与声誉损害，甚至威胁公共安全。当前，数据交易黑市的存在进一步放大了风险，泄露的数据被非法倒卖、滥用，形成完整的黑色产业链，对网络安全生态造成严重破坏，也给数据安全监管带来巨大挑战。

2.4 网络设备与系统漏洞引发的安全问题

网络设备如路由器、交换机等，若存在设计缺陷或未及时修复漏洞，可能被攻击者利用获取设备控制权，进而渗透整个网络；操作系统、应用软件等在开发过程中难免存在安全漏洞，若厂商补丁更新不及时，或用户未及时安装补丁，会给攻击者留下可乘之机。部分老旧设备与系统因技术淘汰无法获得安全更新，长期运行会持续放大网络安全风险，成为网络安全体系中的薄弱环节[2]。

3 计算机网络安全问题产生的根源分析

3.1 技术层面：网络架构缺陷与技术更新滞后

部分网络架构设计存在先天性缺陷，缺乏整体安全规划，各系统模块间兼容性与防护协同性不足，形成安全防护盲区。同时，网络技术迭代速度与安全防护技术更新不同步，部分网络系统仍依赖老旧技术架构，难以适配新型网络环境的安全需求。安全技术研发投入不足，核心防护技术与关键设备国产化程度有待提升，部分领域仍依赖外部技术支持，进一步加剧了网络安全的技术风险，为攻击者提供了可乘之机。

3.2 管理层面：安全管理制度缺失与执行不到位

部分单位缺乏系统完善的网络安全管理制度，未明确安全防护标准、操作规范及责任划分，导致网络安全工作无章可循。即便制定了相关制度，也常存在执行流于形式的问题，制度要求与实际操作脱节，安全检查、风险评估等关键环节落实不到位。网络安全管理缺乏动态调整机制，无法及时适配网络环境变化与新型安全威胁，导致管理措施滞后，难以有效防范各类安全风险。

3.3 人员层面：安全意识薄弱与操作不规范

多数用户与工作人员网络安全意识薄弱，对网络安全风险的认知不足，缺乏基本的安全防护常识。部分人员存在操作不规范行为，如使用弱密码、随意访问不明链接、违规传输敏感数据等，人为制造安全漏洞。网络安全专业人才匮乏，现有从业人员专业能力与技术水平不足，难以应对复杂多变的网络安全态势，无法及时发现并处置安全隐患，进一步削弱了网络安全防护能力。

3.4 外部环境层面：网络攻击手段迭代升级

当前网络攻击技术呈现专业化、智能化、产业化发展趋势，攻击手段不断迭代升级，隐蔽性与破坏性显著增强。攻击工具的普及降低了攻击门槛，各类网络攻击事件的发起成本大幅下降，攻击范围与影响面持续扩大。跨境网络攻击事件频发，国际网络安全形势日趋复杂，不同地区网络安全监管标准存在差异，导致跨境网络安全风险难以有效管控，进一步加剧了全球网络安全环境的不确定性[3]。

4 计算机网络安全防范策略

4.1 计算机网络安全防范的技术策略

4.1.1 基础防护技术

（1）防火墙技术的部署与优化应用。科学规划防火墙部署架构，根据网络拓扑结构与业务需求，合理设置边界防火墙、内部防火墙等多层防护节点，实现网络区域的有效隔离。优化防火墙规则配置，遵循“最小权限”原则，精准管控进出网络的数据流，屏蔽非法端口与危险协议，同时定期梳理并更新规则库，删除冗余规则，避免规则冲突导致的防护漏洞。强化防火墙的日志审计功能，实时监控网络访问行为，及时发现异常访问轨迹，为安全事件追溯提供数据支撑。选用支持深度包检测、应用识别等高级功能的下一代防火墙，提升对新型网络攻击的识别与拦截能力。（2）入侵检测与防御系统（IDS/IPS）的构建。构建分布式入侵检测与防御体系，结合网络型IDS/IPS与主机型IDS/IPS，实现对网络传输层与主机系统层的全面监测。优化IDS/IPS的检测规则，整合威胁情报数据，及时更新特征库，提升对未知攻击、变种攻击的检测灵敏度。建立IDS/IPS与防火墙等安全设备的联动机制，实现检测、告警、拦截的自动化闭环处理，当检测到恶意攻击行为时，自动触发防火墙阻断相关连接，降低攻击造成的损失。（3）数据加密技术的应用：对称加密与非对称加密。根据数据传输与存储的不同场景，合理选用加密技术，构建全生命周期的数据加密防护体系。在数据传输过程中，采用非对称加密技术实现密钥协商与身份认证，结合对称加密技术对海量数据进行加密处理，兼顾加密效率与安全性，保障数据在公网传输中的机密性与完整性。在数据存储环节，对敏感数据采用分区加密、文件加密等方式，选用高强度加密算法，避免数据存储介质丢失或被非法访问导致的信息泄露。建立完善的密钥管理体系，规范密钥的生成、分发、存储、更新与销毁流程，定期进行密钥轮换，防止密钥泄露引发的加密失效问题。

4.1.2 进阶防护技术

（1）身份认证与访问控制技术优化。构建多因素身份认证体系，整合密码认证、生物特征认证、硬件令牌认证等多种认证方式，提升身份认证的安全性与可靠性，避免单一密码认证被破解带来的风险。细化访问控

制策略，基于角色、职责与业务需求，明确不同用户的访问权限范围，实现“按需授权、最小权限”，严格限制非授权用户对敏感数据与核心系统的访问。引入零信任架构理念，秉持“永不信任、始终验证”的原则，对每一次访问请求都进行严格的身份认证与权限校验，无论访问者来自内部网络还是外部网络，均执行统一的安全管控标准。（2）终端安全防护技术：终端杀毒、补丁管理。构建全面的终端安全防护体系，为所有终端设备部署正版杀毒软件，定期更新病毒库，开启实时监控功能，及时查杀恶意代码与可疑程序。建立终端补丁管理规范，搭建统一的补丁分发与管理平台，实时监测终端系统与应用软件的漏洞情况，及时推送安全补丁并督促终端用户安装，对未及时安装补丁的终端进行提醒与管控，避免漏洞被攻击者利用。强化终端设备的安全配置，禁用不必要的服务与端口，关闭自动运行功能，设置复杂密码并定期更换，提升终端设备自身的安全防护能力。（3）云环境下的网络安全防护技术。针对云环境的分布式、虚拟化特性，构建适配云架构的安全防护体系。采用云防火墙、云入侵检测与防御系统等云原生安全产品，实现对云主机、云存储、云网络等云资源的精准防护。强化云平台的虚拟化安全防护，对虚拟主机、虚拟交换机等虚拟组件进行安全加固，防范虚拟机逃逸、虚拟网络攻击等新型风险。建立云数据安全防护机制，采用数据加密、数据脱敏等技术，保障云存储数据的安全[4]。

4.2 计算机网络安全防范的管理策略

（1）完善制度体系。结合法规与行业标准，制定覆盖网络建设、运维、数据安全、应急处置全流程的制度，明确各岗位职责，形成全员负责格局；配套操作规范、管理细则等文件，定期评审修订以适配环境与法规变化。（2）健全风险评估与应急机制。定期开展全面风险排查，制定整改方案；组建应急团队，明确流程与权限，制定多场景预案并定期演练；规范安全事件上报与处置流程，保障快速响应减损。（3）规范运维管理。建立设备全生命周期管理机制，规范采购、运维等流程；统一日志收集分析，定期巡检排查问题；明确运维人员权限与流程，全程记录审计。

4.3 计算机网络安全防范的人员培养与意识提升策略

（1）培养专业人才。结合岗位需求制定培养计划，通过内外部培训、校企合作提升专业能力；鼓励考取安全认证，建立激励机制吸引留存人才，加强行业交流学习先进经验。（2）提升全员意识。制定差异化培训计划，覆盖安全基础、威胁识别、操作规范等内容；采用多元培训形式提升参与度，定期考核确保全员掌握必备技能。（3）落实责任机制。明确各岗位安全责任并纳入绩效考核，建立责任清单细化标准；加强监督检查，对失职导致安全事件的依规追责，强化全员责任意识。

结束语：计算机网络安全是一项长期且复杂的系统工程，伴随着技术的发展与攻击手段的迭代，安全防护工作面临持续挑战。本文通过对网络安全问题的系统梳理与根源剖析，提出了技术、管理、人员协同发力的防范策略，为构建全方位安全防护体系提供了思路。未来，网络安全防护需紧跟技术发展步伐，持续优化防护策略，强化技术创新与管理升级，提升全员安全素养。

参考文献

[1]于小婷.浅析计算机应用中网络信息安全问题及应对策略[J].信息与电脑,2025,37(5):83-85.

[2]邱峻.计算机网络安全漏洞及防范策略探析[J].数字技术与应用,2025,43(6):71-73.

[3]季霖宇.大数据背景下计算机网络安全风险与防范策略[J].数字技术与应用,2025,43(10):55-57.

[4]张小燕.计算机应用中的网络安全防护策略[J].数字技术与应用,2025,43(3):80-82.