现代化计算机网络信息安全影响因素及防护策略研究

王正峰 汪泽宇

上海卫星工程研究所，上海，201109；

摘要：现代化计算机网络信息安全面临多重威胁，其影响因素涵盖操作系统漏洞、黑客攻击手段、病毒传播机制、用户行为模式及物理环境风险等层面。这些因素通过技术渗透、社会工程及环境破坏等路径，对信息系统的保密性、完整性与可用性构成复合型挑战。本文通过系统分析各影响因素的作用机理，提出加装杀毒软件、应用数据加密技术、部署防火墙系统、构建安全监控网络及强化用户安全素养等防护策略，旨在形成技术防御与管理优化协同的立体化安全体系。研究结果表明，综合运用主动防御与被动保护措施，可显著提升网络信息系统的安全韧性，为数字化社会的稳定运行提供基础支撑。

关键词：计算机网络；信息安全；黑客攻击；数据加密；防火墙；安全意识；安全监控；系统韧性

DOI：10.69979/3041-0673.26.02.033

引言

当前全球信息化进程正在加速演进，计算机网络已经深度嵌入国家治理、经济发展以及社会运行的各个层面，成为支撑数字时代的核心基础设施，然而网络空间在带来高效与便捷的也因为开放性、互联性与复杂性而面临日益严峻的安全挑战，攻击手段日趋智能化、组织化与武器化，从勒索软件到 APT 攻击，从供应链污染到零日漏洞利用，安全威胁已从单一技术问题演变为系统性风险，传统“边界防护 + 补丁修复”的被动模式难以应对动态、多维、跨域的现代攻击，因此本文立足于当前网络安全攻防对抗的实际态势，深入剖析影响信息安全的内在机理与外在动因，突破孤立技术视角，构建“技术防御，智能监控，人本管理”三位一体的主动防护架构。研究旨在为组织提供可落地、可演进、可协同的安全策略体系，强化网络空间的韧性与可控性，切实保障信息资产的机密性、完整性与可用性，筑牢数字中国建设的安全基石。

1 计算机网络信息安全的定义与特征

计算机网络信息安全，是指在信息的采集、传输、存储、处理与应用全生命周期中，通过技术、管理与法律等综合手段，保障信息的机密性、完整性、可用性、可控性与不可否认性，防止信息被非法访问、篡改、破坏、泄露或滥用的系统性工程。其本质是构建一个动态平衡的安全边界，在保障业务连续性的同时，有效抵御内外部威胁。

现代计算机网络信息安全呈现出四大核心特征：其一，系统性。安全不再局限于单一设备或孤立应用，而是覆盖网络架构、协议栈、终端设备、数据中心与云平台的全局体系，任何环节的脆弱性都可能引发系统性风险。其二，动态性。攻击手段持续迭代，防御策略必须随之演进，静态防护已无法应对 APT（高级持续性威胁）、零日漏洞等新型攻击模式。其三，对抗性。安全防护本质上是攻防双方的博弈过程，攻击者不断寻找防御盲区，防御者则需构建纵深防御体系并预判攻击路径。其四，人本性。无论技术如何先进，最终的操作者与决策者仍是人类，用户行为、管理制度与组织文化对安全态势具有决定性影响。理解这些特征，是制定有效防护策略的前提。

2 计算机网络信息安全的影响因素

2.1 操作系统与软件因素

操作系统作为计算机运行的基础平台，它的架构设计缺陷以及更新机制漏洞是安全威胁的重要源头，内存管理模块的缓冲区溢出漏洞长期处于安全漏洞榜首位置，攻击者能够通过构造异常输入触发系统崩溃或者代码执行，权限管理机制的不完善造成普通用户可访问系统核心文件，比如 Windows 系统曾因注册表权限配置错误，让攻击者可以篡改系统启动项，软件供应链的复杂性进一步加剧了风险。第三方库的引入扩大了攻击面，在 2021 年 Log4j2 漏洞事件中，攻击者借助日志记录功能远程执行代码，影响到全球数十万应用系统，软件更新机制的不健全也带来了隐患，部分用户关闭自动更新功能，导致已知漏洞长期存在，给攻击者提供了可乘之机。

2.2 黑客因素

黑客攻击手段正呈现出技术专业化和目标精准化

的趋势，其中 APT 攻击会通过多阶段渗透以及长期潜伏的方式，来突破传统的防御体系，就像在 2020 年 SolarWinds 供应链攻击事件里，黑客通过篡改软件更新包的手段，成功入侵美国多个政府部门的核心网络，并且持续监控长达 9 个月的时间，社会工程学攻击则是利用人性弱点，通过伪装身份的办法来获取敏感信息，而钓鱼邮件目前仍是主要的攻击载体，其成功率和邮件内容的逼真程度密切相关，自动化攻击工具的普及使得技术门槛有所降低。

2.3 网络病毒入侵

病毒传播机制一直在不断演变，最开始是通过存储介质进行传播，之后逐渐发展为利用网络协议漏洞来进行扩散，蠕虫病毒会通过扫描网络里的脆弱设备来实现自我复制，就像 2017 年的 WannaCry 勒索病毒利用 SMB 协议漏洞，在 24 小时内就感染了全球 150 个国家的 20 余万台设备。木马程序会伪装成正常软件，通过捆绑下载或者欺骗安装的方式进入系统，进而远程控制受感染设备进行数据窃取或者挖矿操作，病毒变种的更新速度也在加快，攻击者采用多态编码技术生成特征不同的病毒样本，导致传统特征码检测方法难以应对这种情况，零日漏洞利用成为了新型攻击方式，攻击者会在漏洞披露前就开发出攻击代码。例如，2023 年 Chrome 浏览器零日漏洞被用于攻击政府机构，从漏洞发现到攻击发生仅仅间隔了 72 小时。

2.4 用户缺乏安全意识

人为因素是安全事件的重要诱因，密码管理不当是典型表现。用户倾向于使用简单密码或重复使用同一密码，导致单个账户泄露引发连锁反应。钓鱼攻击成功率与用户认知水平密切相关，攻击者通过伪造官方网站或客服电话，诱导用户输入账号密码。物理安全意识薄弱同样引发风险，部分员工将含敏感信息的纸张随意丢弃，或未锁定计算机屏幕即离开工位。内部威胁不容忽视，离职员工利用残留权限访问系统，或在职员工出于利益泄露数据，某金融机构数据泄露事件中，内部人员通过数据库备份功能窃取客户信息，导致直接经济损失超 2000 万元。

2.5 自然灾害因素

自然灾害对网络基础设施的破坏具有不可预测性与广泛影响性。洪水导致数据中心断电或设备浸水，2021 年郑州暴雨造成某数据中心业务中断 12 小时，影响金融、交通等多个领域。地震破坏通信光缆与基站，2008 年汶川地震使四川境内 80%基站瘫痪，通信恢复耗时 72 小时。极端温度影响设备稳定性，数据中心机房温度每升高 10℃，电子元件故障率提升 50%，需通过精密空调系统维持恒温环境。电磁干扰导致数据传输错误，高压输电线路附近的通信基站误码率可达正常环境的 3 倍，需采用屏蔽电缆与滤波技术降低影响。

3 计算机网络信息系统安全问题解决策略

3.1 加装杀毒软件

杀毒软件是通过特征码匹配、行为监测以及启发式分析等技术来实现病毒防御的。特征码匹配技术依赖于病毒样本库，它是通过比对文件特征码的方式来识别已知病毒的，不过需要定期更新病毒库才能应对新的病毒变种。行为监测技术则是分析程序运行时的系统调用和网络行为，以此来识别像文件加密、注册表修改等异常操作，这种技术可以拦截 80%的未知病毒。启发式分析是通过模拟程序执行环境的方法，来检测潜在的恶意行为，它适用于零日漏洞攻击的防御。云查杀技术能够提升检测效率，终端设备会将可疑文件的哈希值上传至云端服务器，服务器再通过大数据分析返回检测结果，这样可以减少本地计算资源的占用。企业级杀毒软件需要集成终端管理功能，以此来实现全网设备的策略下发和漏洞修复。

3.2 采用数据加密技术

3.2.1 链路数据加密技术

链路加密在物理层对数据进行加密，确保传输介质上的数据不可读。IPSec 协议通过 AH（认证头）与 ESP（封装安全载荷）头实现端到端加密，AH 提供数据完整性验证，ESP 提供加密与认证功能。在 VPN 场景中，IPSec 通过预共享密钥或数字证书建立安全隧道，保护数据在公网传输过程中的安全性。某跨国企业采用 IPSec VPN 连接分支机构，数据传输加密强度达 AES-256，有效抵御中间人攻击。链路加密需与密钥管理结合，量子密钥分发技术利用量子力学原理生成无条件安全的密钥，中国“墨子号”卫星已实现 1200 公里量子密钥分发，为未来超长距离安全通信提供可能。

3.2.2 节点加密

节点加密在数据经过网络设备时进行动态解密与重新加密，确保中间节点无法获取明文。SDN（软件定义网络）架构下，加密策略可集中编排，通过控制器下发至各网络设备，实现全网流量加密。某云服务商通过 SDN 控制器定义加密规则，支持按应用类型、用户组等维度实施差异化加密策略，策略下发延迟低于 50ms。硬件加密卡提升处理性能，Intel SGX 技术可在 CPU 内

部创建安全飞地（Enclave），密钥生成与存储均在受保护环境中完成，防止密钥泄露导致的数据破解。节点加密适用于对数据保密性要求极高的场景，如金融交易、医疗数据传输等。

3.2.3 端到端加密

端到端加密能够确保数据在发送端进行加密、在接收端实现解密，并且中间节点仅仅处理密文而不涉及明文，Signal 协议采用双重 Ratchet 算法来实现前向安全，就算长期密钥出现泄露，历史消息依然无法被解密，该算法通过定期更新会话密钥的方式，让攻击者无法凭借截获的密文去推导后续密钥。某即时通讯工具引入端到端加密之后，用户数据泄露事件下降了 92%，从而有效保护了用户隐私，区块链技术借助非对称加密与哈希链来实现数据不可篡改，比特币网络运行 12 年都未发生核心数据修改事件，其共识机制能够确保所有节点对交易记录达成一致，端到端加密适用于对数据隐私与完整性要求极高的场景，例如政务通信、企业机密文件传输情况。

3.3 安装防火墙

防火墙会借助访问控制列表（ACL）以及状态检测技术来过滤非法流量，其中传统包过滤防火墙是基于源/目的 IP 地址、端口号等五元组信息进行规则匹配，其处理速度较快但安全性存在一定的局限性，状态检测防火墙会跟踪 TCP 连接状态，只允许已建立连接的合法流量通过，能够拦截 70%的端口扫描与 SYN 洪水攻击，下一代防火墙（NGFW）集成了入侵防御（IPS）与应用识别功能，通过深度包检测（DPI）技术分析应用层协议，进而识别 P2P 下载、即时通讯等非业务流量，某电商平台部署 NGFW 后，SQL 注入攻击拦截率从 65%提升到 92%，有效地保护了数据库安全，软件定义防火墙（SDFW）可以实现策略动态调整，通过集中控制器根据网络状态实时更新规则，某金融机构通过 SDFW 将新业务上线安全配置时间从 2 天缩短到 2 小时。

3.4 应用计算机安全监控信息网络技术

安全信息与事件管理（SIEM）系统整合日志分析、威胁检测与响应功能，通过关联分析识别复杂攻击。Splunk Enterprise Security 可处理每秒 10 万条日志，支持200余种安全事件的关联规则，自动生成攻击链图谱。用户实体行为分析（UEBA）通过机器学习模型识别异常行为，某银行利用 UEBA 检测到内部员工异常数据导出行为，该员工在非工作时间频繁访问客户数据库，系统提前 14 天预警并阻止数据泄露。网络流量分析（NTA）技术检测隐蔽攻击，Darktrace AI 系统通过无监督学习建立正常流量基线，识别异常通信模式，成功拦截多起 APT 攻击中的横向移动行为。

3.5 增强用户安全防护意识和防护技能

安全培训需要全面覆盖密码管理、钓鱼识别以及物理安全多方面内容，其中密码管理培训着重强调使用强密码，也就是包含大小写字母、数字与特殊符号的密码，并且推荐使用密码管理器工具，比如某制造企业在开展季度安全演练之后，员工弱密码的使用率从 35%显著降至 8%，钓鱼攻击模拟测试是通过发送伪造邮件来评估员工的防范能力，像某金融机构通过红蓝对抗发现有32%的部门存在点击钓鱼链接的行为，在进行针对性整改之后系统入侵尝试减少了 76%，物理安全培训涵盖设备锁定、文件销毁等操作规范，例如某企业要求员工离开工位时必须锁定计算机屏幕，并且通过监控摄像头抽查执行情况，使得违规率从 25%大幅降至 5%，安全意识评估工具能够量化培训成效，例如 KnowBe4 平台通过模拟攻击测试生成用户安全指数，从而帮助企业定位薄弱环节并制定相应的改进计划。

4 结束语

计算机网络信息安全防护是技术与管理深度融合的系统工程。操作系统与软件的漏洞修复、黑客攻击的动态防御、病毒传播的立体阻断、用户意识的结构化提升及自然灾害的冗余设计，共同构成安全防护的核心要素。实践表明，单一技术手段难以应对多元化威胁，需通过杀毒软件、数据加密、防火墙、安全监控等技术的协同应用，形成覆盖数据全生命周期的防护体系。用户安全意识培养与技术工具部署同等重要，二者缺一不可。唯有将安全理念融入系统设计、开发、运维全流程，构建“技术防御+管理优化+人员素养”的三维防护框架，方能实现计算机网络信息安全的可持续保障，为数字化社会的稳定运行提供坚实基础。

参考文献

[1]杜伟.大数据时代计算机网络信息安全及防护策略[J].中阿科技论坛(中英文),2024,(10):34-38.

[2]于光许.信息化背景下计算机通信网络信息安全防护策略[J].信息与电脑(理论版),2023,35(04):239-241.

[3]王中亚.大数据时代计算机网络信息安全及防护策略[J].数字通信世界,2021,(02):165-166+169.

[4]安玲.大数据时代计算机网络信息安全及防护策略分析[J].产业创新研究,2024,(10):61-63.