计算机数据通信网络维护与网络安全问题探索

叶勇辰
武昌职业学院　湖北武汉　438600

摘　要：在当今信息时代，计算机数据通信网络已经无处不在，对个人、企业和社会的运作至关重要。然而，网络安全威胁和数据通信网络维护问题也日益突出。本文强调了加强计算机数据通信网络维护和网络安全的必要性，当前网络面临的安全隐患进行分析，并提出了切实可行的应对措施，旨在为计算机数据通信网络维护与网络安全问题提供有效借鉴。

关键词：数据通信网络、网络安全、网络维护、安全防护、防范意识

随着时代发展，计算机数据通信网络已成为现代社会有效运转的重要基础设施。无论是企业的内部办公系统，还是跨国公司的全球业务协作，抑或个人在家中上网、在线支付、远程工作等，都离不开数据通信网络的支撑。它使信息能够高效率、实时地在不同节点间传递，为人类的工作和生活带来了巨大便利。但同时，病毒、木马、黑客入侵等攻击手段层出不穷，给企业和个人造成了重大财产损失和隐私泄露风险。一旦关键网络系统受到破坏，整个社会的正常运转都将遭受冲击。因此，加强对计算机数据通信网络的维护和安全防护，已经成为当务之急。

1. 加强计算机数据通信网络维护与网络安全的必要性

在当今信息时代，人们日常生活和工作越来越依赖于互联网和数据通信。从支付账单到远程办公，从社交媒体到在线娱乐，网络已经无处不在。然而，网络安全威胁也与日俱增。病毒攻击、数据泄露等事件时有发生，给个人和企业乃至社会带来重大财产损失和隐私风险。加强网络安全意味着保护关键基础设施的正常运转，维护社会稳定 [1]。同时，现代社会对高效可靠的数据传输和通信有着迫切需求。无论是企业内部系统之间的数据交换，还是远程办公、视频会议等跨地域沟通，数据通信网络都扮演着关键角色。数据通信技术的不断进步，使信息能够快速传递。从以太网到无线局域网，再到 5G 移动通信，这些技术极大提高了工作效率和生活质量。然而，只有对数据通信网络进行良好的建设和维护，才能最大限度发挥其优势。

2. 计算机数据通信网络面临的安全隐患

2.1 计算机病毒的入侵

计算机病毒是当今网络环境中最常见也最危险的安全威胁之一。只需轻轻一个疏忽，病毒就可能悄无声息地潜入系统，给数据通信网络带来灾难性后果。病毒具有自我复制和传播的能力，可通过多种途径感染计算机系统，如木马程序、电子邮件附件、U 盘拷贝等。一旦入侵成功，病毒会破坏系统文件、删除重要数据、窃取机密信息、控制系统资源等，导致网络瘫痪、数据泄露等严重问题。

2.2 系统环境安全性低

计算机数据通信网络所处的系统环境，包括硬件、操作系统、防火墙、网络拓扑结构等方方面面，如果存在配置不当或管理疏忽，极易导致整体安全性降低。硬件缺陷可能使系统面临物理层面的攻击风险 [2]。老旧的操作系统版本和防火墙规则如果没有及时更新，会留下可被利用的漏洞。网络拓扑结构不合理，就无法有效隔离危险区域和关键区域。内外网边界管控不当，也可能使内部网络暴露在外部威胁之下。

2.3 用户行为习惯的影响

在很多情况下，最危险的网络安全威胁并非来自病毒或黑客，而是源于用户本身的不当行为习惯。有些用户对于网络安全的重要性缺乏足够认识，在上网浏览、发送邮件、使用 U 盘等环节疏于防范。他们可能随意打开不明来源的附件、访问不安全网站、传播计算机病毒等，给网络带来极大隐患。更有甚者，一些内部人员可能会蓄意实施破坏性行为，从内部渗透并攻击网络系统。

3. 加强计算机数据通信网络维护与网络安全的有效举措

3.1 加强对计算机数据通信网络的维护

3.1.1 定期巡检网络设备。保持网络设备的正常运行是计算机数据通信网络维护的基础。定期对网络硬件设备如路

由器、交换机、服务器等进行全面巡检，是发现并解决潜在故障的有效途径。巡检的内容包括检查设备的工作状态参数、更新固件版本、清理积灰和故障备件的更换等[3]。同时要查看设备的配置是否正确、线路连接是否牢固、供电和散热是否良好等。对于发现的故障隐患，要及时记录并采取应对措施，确保网络畅通。例如大型企业内部，IT 运维人员每月会对机房内数百台网络设备进行彻底检查，包括做数据性能测试、更新 IOS 系统、清洁风扇滤尘网等。这种工作的持续开展，就能极大降低网络中断风险。

3.1.2 检查应用程序。计算机数据通信网络上运行着大量应用程序，用于办公、管理、通信等目的。这些程序若有缺陷或被恶意代码感染，将直接影响网络的正常运作。因此，对应用程序的严格检查和监控至关重要。必须密切关注应用程序的使用情况和运行状态，确保它们始终处于最佳状态。这包括对应用程序的版本更新情况进行定期检查，确保程序始终处于最新版本，避免因为版本过旧而带来的安全风险。同时，还要关注应用程序的内存和 CPU 占用率，防止因为资源过度消耗而导致的网络拥堵或崩溃。除此之外，对应用程序的行为分析也是必不可少的。需要通过专业的工具和技术手段，对应用程序进行深入的行为分析，判断其是否存在恶意行为。

3.1.3 优化网络拓扑结构。网络拓扑结构设计，作为数据通信网络构建的核心环节，其合理与否直接关系到整个网络的性能与安全性。一个优秀的拓扑结构能够确保网络的稳定传输、高效扩展以及严密的安全防护[4]。相反，不合理的拓扑结构不仅可能导致数据传输效率低下，还可能增加安全风险，给企业的运营带来严重困扰。因此，必须高度重视网络拓扑结构的设计与优化工作。在实际操作中，应根据企业的实际需求，对网络拓扑进行持续的评估和调整。这包括根据功能需求，合理划分不同的安全域，如七层 DMZ 区、服务器区、办公区等，并通过防火墙、VPN 等先进技术实现各区域之间的有效隔离和访问控制。同时，在核心和广域网区域，还应采用备份冗余链路的设计，以提高网络的容错能力，确保在突发情况下网络的稳定运行。

3.2 保障网络系统安全

3.2.1 建立网络安全保护体系。网络安全不应是一蹴而就的工作，而需要一个持续完善的保护体系作为支撑，明确责任主体、管理流程和技术措施。首先要建立完备的网络安全管理制度和流程，包括风险评估机制、事件响应预案、责任追究等内容。同时确立统一的网络安全管理部门，对各项措施的实施进行规划、协调和监督。其次要落实严格的人员准入和授权管理。对所有人员身份进行核实、访问权限控制，关键系统更要采取双人值守等措施。再者要建设各类安全技术防护设施，如入侵检测、防火墙、网闸等。此外，成熟的网络安全保护体系还应包括紧急情况处理预案、安全知识培训、定期审计、资源投入保障等诸多方面的内容。只有全方位构建和落实好这一体系，才能从根本上为网络安全保驾护航。

3.2.2 强化安全防护策略。制定并持续优化网络安全防护策略，是确保数据通信网络安全的关键一环。防护策略需要根据实际网络环境、面临的威胁种类等因素制订，全面覆盖安全防护目标[5]。例如，针对外部入侵威胁，要部署防火墙、IPS/IDS、VPN 等设备，限制非法访问；针对内部威胁，要采取最小权限原则，控制关键系统的访问权限；针对计算机病毒，要安装防病毒软件，并及时更新病毒码库等。同时，在具体防护策略上，须遵循分级分域、确保完整性、适应性强等原则。企业还可参考 ISO27001 等安全标准，对策略进行规范化管理。此外，要针对新出现的攻击手段，及时修订和完善防护策略。

3.2.3 开展网络漏洞检测和修复。无论是操作系统、应用软件、网络设备、Web 应用等，只要参与到数据通信网络中，它们都可能存在编程缺陷或配置疏忽导致的安全漏洞。这些漏洞为黑客入侵提供了机会，必须及时检测并修复。漏洞检测的方式包括人工代码审计、自动化漏洞扫描工具、模糊测试、渗透测试等。重点需检测的漏洞种类有溢出、注入、跨站脚本、认证绕过等，而且漏洞数量增长迅速。对于发现的高危漏洞，要根据厂商提供的补丁尽快修复，降低被利用风险。同时要采取临时的缓解措施，如限制访问、增加监控、采用虚拟补丁等。如果漏洞有被利用迹象，还应对事件开展调查，追查源头并消除影响。

3.2.4 规范网络应用软件的开发和使用。应用软件在数据通信网络的运作中扮演着重要角色。如果软件开发和使用过程缺乏规范，不仅会引入安全漏洞，也可能导致系统效率低下、数据错乱等问题。因此，必须建立完善的软件开发生命周期管理制度，从需求分析、设计、编码、测试到发布上线，均须严格遵守相关标准和规范。譬如 OWASP 对 Web 应用

安全编码规范有明确要求，SDLC 阶段要引入安全评审等。开发过程中，要优先选用成熟可信的编程语言框架，严格执行输入验证和数据过滤，防止注入漏洞。同时要遵守最小权限原则，避免授予不必要的系统权限。代码要经过彻底审计和渗透测试，确保无高危漏洞。此外，对于网络中运行的所有应用软件，要及时安装补丁更新，制定并执行严格的使用政策和权限控制措施。

3.2.5 加强信息技术保密管理。保护关键数据和系统免受泄露是网络安全的重中之重。为此，必须建立完善的信息技术保密管理制度，规范数据分类分级、授权使用、存储销毁等全生命周期管理 [6]。首先要识别机密信息和关键业务系统，对其进行分级保护。如敏感个人信息、商业秘密、关键基础设施控制系统等都需要最高级别的保密防护。其次要落实严格的访问控制措施，如身份认证、权限管控、监控审计等。对于重要系统和数据，可采取须知和最小权限原则，并引入双人值守等机制，确保关键节点无法被单人攻破。存储介质的保密防护也不容忽视。要加密存储机密数据，使用可信赖的加密算法和密钥管理措施。对报废介质要做好磁盘清除和物理销毁处理。此外，网络上传输的重要数据也须进行加密保护。

4. 结束语

总之，加强计算机数据通信网络维护与网络安全，是一项系统工程，需要持续的投入和努力。未来，随着信息技术的不断发展，新的挑战和威胁将源源不断出现。比如，5G/6G、物联网、云计算等新型网络架构和应用模式，给网络安全防护带来了新的复杂性；量子计算的兴起，也可能使传统加密算法失去保护能力。因此，网络维护和安全防护工作也须与时俱进，紧跟技术发展步伐。只有坚持不懈地完善各项保障措施，从技术、制度、人才、国际合作等多方面入手，才能为数据通信网络的健康可持续发展保驾护航。

参考文献

[1] 严寿福 . 计算机数据通信网络维护与网络安全问题探索 [J]. 数字通信世界 ,2023,(11):175–177.

[2] 冷海涛 . 计算机数据通信网络维护与网络安全问题研究 [J]. 中国管理信息化 ,2023,26(03):155–158.

[3] 张文娟 , 常秀颖 , 夏瑞雪 . 计算机通信网络的数据安全维护策略分析 [J]. 电子技术 ,2022,51(06):186–187.

[4] 莫晓楠 . 计算机数据通信网络安全维护要点研究 [J]. 网络安全技术与应用 ,2021,(11):16–17.

[5] 郑翔 . 计算机数据通信网络安全维护要点探索 [J]. 中国新通信 ,2020,22(20):34–35.

[6] 孙艺峰 . 计算机通信网络安全维护问题探索 [J]. 产业与科技论坛 ,2017,16(19):250–251.

作者简介：

叶勇辰（1992.1.20 – ），男，汉族，湖北黄冈，本科，研究方向：计算机网络。