

# 计算机网络维护中的安全防护策略

赵越

天津市滨海新区新河街社区卫生服务中心

DOI:10.12238/acair.v2i4.10339

**[摘要]** 随着信息技术的快速发展,计算机网络已成为社会运行的重要支撑。然而,伴随着计算机网络的普及,各种安全问题也日益凸显,网络安全事件频发,影响人们的工作、生活。本文通过分析计算机网络安全的影响因素,探讨当前计算机网络维护中的安全防护策略,旨在提升网络的安全性,为各类网络用户提供更加可靠的保障。

**[关键词]** 计算机; 网络维护; 安全防护

**中图分类号:** G623.58 **文献标识码:** A

## Security protection strategy in the computer network maintenance

Yue Zhao

Tianjin Xinhe Street Community Health Service Center

**[Abstract]** With the rapid development of information technology, computer networks have become an essential support for social operations. However, alongside the widespread adoption of computer networks, various security issues have become increasingly prominent, leading to frequent cybersecurity incidents that affect people's work and daily life. This paper analyzes the factors influencing computer network security and explores current security protection strategies in computer network maintenance, aiming to enhance network security and provide more reliable protection for various network users.

**[Key words]** computer; network maintenance; security protection

### 引言

计算机网络的广泛应用使得信息的传递、获取更加快捷与高效,然而,网络安全问题也随之而来。网络攻击、病毒传播、数据泄露等问题给个人、企业安全都带来威胁。因此,计算机网络维护中的安全防护策略变得至关重要。本文将从网络安全的影响因素入手,分析各种潜在威胁,并提出相应的防护措施,以保障网络环境的安全性。

#### 1 计算机网络安全的影响因素

##### 1.1 人为因素

在计算机网络安全问题中,人为因素占据了极其重要的地位,甚至是导致许多网络安全事故的主要原因。无论是用户的安全意识不足,还是操作不当,都可能成为网络安全隐患的根源。首先,用户对网络安全知识的匮乏是造成安全漏洞的重要原因。很多人用户、企业员工缺乏对网络威胁的基本认知,不了解如何妥善处理安全风险。例如,一些用户在使用网络时,容易点击陌生的链接、访问可疑的网站,甚至随意下载未经验证的软件,从而给恶意程序的入侵打开了大门。此外,密码管理不当也是人为因素中常见的问题。用户习惯设置简单、易于破解的密码,或者在多个账户中重复使用相同的密码,这使得黑客能够轻松获取

访问权限,进行非法操作。即便有些企业规定定期更换密码,但若员工对密码的重要性缺乏足够重视,往往会采用简单的替换方式,如在旧密码的基础上加数字,这依然无法有效抵御潜在的攻击。内部人员的失误或故意破坏行为也是计算机网络安全中的重要风险点。许多网络攻击事件不仅来源于外部黑客,也有部分是由内部员工无意中或故意引发的。例如,员工可能因为不当操作,导致网络设备的故障,甚至有些员工出于个人利益,故意泄露公司机密。内部威胁往往比外部威胁更难以防范,因为员工通常拥有系统的合法访问权限,因此他们的不当行为可能会导致更加严重的后果。

##### 1.2 计算机病毒

计算机病毒是网络安全中最为常见且破坏力极强的威胁,它不仅影响网络的正常运行,还可能导致数据丢失、系统崩溃。计算机病毒是恶意程序的一种,设计者通过特定手段将病毒植入目标系统或网络中,借助感染、复制、传播等方式,扰乱计算机系统的正常功能。近年来,随着网络技术的快速发展,病毒的种类变得更加复杂,防范计算机病毒成为网络安全工作中不可或缺的一部分。计算机病毒可以通过多种途径进行传播,最常见的传播方式包括电子邮件、可疑链接、文件共享。一些病毒伪

装成正常的附件,当用户无意间点击时,病毒便会侵入系统并开始复制。例如,通过钓鱼邮件发送的恶意附件,用户一旦打开附件,病毒便会迅速感染用户设备,并有可能蔓延至整个网络。此外,网络浏览时访问不安全的网站,也有可能遭遇病毒入侵,甚至通过浏览器漏洞自动下载恶意程序。近年来,病毒的类型不断多样化,其中勒索病毒和蠕虫病毒引发了广泛关注。勒索病毒是一种通过加密用户数据来达到勒索目的的恶意软件,攻击者通过加密受害者的文件,并要求支付赎金才能恢复数据,这种病毒对企业、个人用户都造成了极大的经济损失。而蠕虫病毒则能够在网络中自动传播,不需要用户的任何操作便可迅速扩散至整个网络,导致网络带宽的消耗。

### 1.3 计算机操作系统存在漏洞

计算机操作系统漏洞是网络安全中的一个重大隐患,直接影响着网络的安全性。操作系统作为计算机的核心软件,负责管理硬件资源、提供应用程序运行环境,因此,一旦操作系统存在漏洞,网络攻击者便可利用这些漏洞实施攻击,导致数据泄露、系统崩溃,甚至完全控制整个网络。随着操作系统的复杂性不断增加,漏洞问题也愈发频繁,这给网络安全管理带来了挑战。操作系统漏洞的产生原因多种多样,主要包括程序代码设计缺陷、功能更新不完善以及开发过程中的疏漏等<sup>[1]</sup>。例如,在操作系统开发过程中,由于程序员疏忽,可能会留下安全隐患,黑客可以通过这些漏洞执行恶意代码,获取系统的管理权限。即便是经过广泛测试的操作系统版本,也难以避免存在潜在的漏洞,尤其是随着新功能的不断添加,这些漏洞会不断暴露在攻击者面前。

### 1.4 当前计算机网络安全缺乏评估和监管手段

当前,计算机和网络安全的评估与监管手段相对薄弱,导致许多潜在的安全隐患无法及时发现处理。这种不足主要体现在企业对网络安全的重视程度不够,缺乏系统化的安全评估机制。随着网络威胁的形式日益复杂化,传统的安全管理手段显得力不从心,无法应对复杂多样的攻击手段和潜在风险。首先,现有的网络安全评估手段较为滞后,难以全面应对新型威胁。在许多企业和机构中,网络安全评估通常依赖定期的系统检查。然而,这种评估方式具有局限性,无法应对快速变化的攻击手段。例如,针对性较强的高级持续性威胁(APT)和零日攻击往往具有高度隐蔽性,传统的评估工具很难发现这些威胁的迹象<sup>[2]</sup>。此外,现有的评估多集中在网络设备的表层安全性上,忽视了数据层面的潜在风险。其次,网络安全监管制度的缺失也是造成安全防护薄弱的一个重要因素。许多企业在实际运营中,缺乏有效的安全监控与应急响应机制,对潜在的网络攻击无法进行实时监控和快速反应。尤其是中小型企业,由于资源有限,通常没有专门的网络安全团队,网络安全更多依赖于被动防御,缺乏主动性。

## 2 计算机网络安全的安全防护措施

### 2.1 个人要树立网络安全意识

在计算机网络安全防护中,个人的网络安全意识起着至关重要的作用。无论是个人用户还是企业员工,如果没有良好的安全意识,将很容易成为网络攻击的目标。随着网络攻击手段的多

样化,个人作为网络系统中最薄弱的环节,常常是黑客入侵网络的突破口。因此,提升个人的网络安全意识是保障整体网络安全的关键一步。首先,个人必须意识到网络安全不仅仅是技术人员的责任,而是每一个网络用户的共同责任。网络安全事件的发生往往与个人操作习惯直接相关,许多病毒、木马或网络攻击都是通过用户的不当操作进入系统的。例如,一些用户喜欢随意点击不明链接、访问可疑网站,这些行为很容易为恶意程序的传播提供途径。此外,许多人习惯使用简单密码或在多个平台重复使用同一密码,这种做法极大增加了账户被盗取的风险。因此,个人应时刻保持警惕,避免这些低级错误,确保自己在使用网络时采取必要的防护措施。同时,个人应养成定期更换密码、使用复杂密码组合等良好习惯,降低账户被攻破的风险。此外,用户可以借助密码管理工具来帮助安全地管理,以避免因记忆困难而使用简单密码。防范网络攻击的一个重要方面是定期更新软件。操作系统和应用程序经常会发布安全更新,修复潜在的漏洞。如果用户忽视这些更新,攻击者就可能利用未修补的漏洞入侵系统。因此,个人用户应确保自己的设备始终处于最新版本,以最大程度地降低安全风险。此外,安装并定期更新防病毒软件也是提高网络安全的重要手段,可以帮助用户识别潜在的恶意程序。

### 2.2 加强建设计算机网络安全管理体系

建立和完善计算机网络安全管理体系是确保网络安全的关键。首先,网络安全管理体系的建设应从顶层设计入手,制定清晰的安全策略。每个企业或组织应根据自身的业务需求和网络架构,建立一套完善的网络安全政策,明确各部门在网络安全中的职责,确保责任到位。例如,企业需要制定严格的访问控制策略,确保只有具备授权的人员能够访问关键系统。其次,安全管理体系的实施需要依赖全面的技术支持<sup>[3]</sup>。企业应部署多层次的安全防护工具,如防火墙、入侵检测系统等,形成多道防线,防止外部入侵。防火墙可以有效过滤不明数据包,防止恶意访问;入侵检测系统能够实时监控网络流量,发现潜在的安全威胁;防病毒软件则可以检测中的恶意程序。此外,数据加密技术也是安全管理的重要组成部分,特别是对敏感数据的传输和存储,应该采取加密措施,以防止数据泄露。网络安全管理体系还应包括严格的权限管理和审计机制。企业在设置网络系统时,应根据用户的职责和权限对其进行分类,确保各类人员只能访问与其工作相关的数据和系统功能,从而降低内部人员误操作或恶意行为带来的安全风险。同时,建立完善的日志记录和审计系统,定期对网络活动进行检查,确保所有操作可追溯。一旦发生安全事件,可以通过审计日志迅速定位问题来源,及时采取补救措施。

### 2.3 加强对访问权限的控制

加强对访问权限的控制是计算机网络安全管理中至关重要的一环。通过合理配置、管理用户的访问权限,企业能够有效防止未经授权的人员访问敏感信息,减少数据泄露和内部威胁的风险。随着网络攻击手段的日益复杂化,内部人员的不当操作已成为企业网络安全的主要威胁,因此对访问权限的精细化管理

是确保信息安全的重要手段。首先,访问权限的控制应遵循“最小权限原则”。这一原则要求用户仅能访问其工作所需的最少权限,而不应拥有超出工作需求的任何额外权限。通过这种方式,可以最大程度地减少恶意行为带来的风险。例如,在企业中,财务人员应只被授予财务系统的访问权限,而不应接触到研发部门的技术数据。同样,普通员工不应拥有管理服务器或修改系统设置的权限,这样可以防止因权限过大而引发的潜在风险。其次,企业应根据用户的职责角色,采取分级权限管理的方式。不同部门、不同职位的员工应被授予不同级别的权限,以确保各类数据、系统操作被合理隔离<sup>[4]</sup>。例如,管理员拥有最高级别的权限,可以管理整个系统和所有用户;而普通用户只应拥有访问特定资源的权限。这种基于角色的权限分配方法可以有效减少权限滥用的可能性,同时提高权限管理的效率。管理员应定期审查权限设置,确保权限配置始终与实际业务需求相符。

#### 2.4 加强对计算机病毒的防范

计算机病毒是网络安全中的重大威胁,能够通过多种方式传播,并对个人、企业和机构的系统造成严重损害。因此,加强对计算机病毒的防范是确保计算机网络安全的重要措施。随着病毒技术的不断演进,传统的防御手段已难以完全阻挡新型病毒攻击,因此必须采取综合性、系统化的防范措施。首先,安装和定期更新防病毒软件是防范计算机病毒的基础步骤。防病毒软件能够自动检测、清除已知的病毒、木马和其他恶意程序,保护计算机系统免受病毒入侵。然而,病毒的变种和新型病毒不断涌现,防病毒软件的病毒库需要保持最新状态,才能有效对抗这些新威胁。因此,企业应确保其防病毒软件保持自动更新功能,及时获取病毒库的最新信息,防止系统被新的病毒感染。此外,用户应定期扫描系统,确保任何潜在的威胁能够被及时发现并清除。其次,定期更新操作系统和软件补丁是另一项重要的防范

措施。许多计算机病毒是通过利用系统中的漏洞进行传播的,因此及时修补这些漏洞可以有效防止病毒利用这些安全缺口进行入侵。例如,操作系统和应用程序开发商会定期发布安全补丁来修复已发现的漏洞,用户应确保这些更新被及时安装,以防止病毒通过未修补的漏洞侵入系统。同时,使用正版软件也非常重要,因为盗版软件通常缺乏更新支持,更容易受到病毒攻击<sup>[5]</sup>。

### 3 结束语

随着信息技术的迅猛发展和网络环境的日益复杂,计算机网络安全面临着前所未有的挑战。只有在技术与管理、意识与行为相结合的前提下,才能有效构建起一个全面、多层次的网络安全防护体系。面对不断变化的网络威胁,唯有不断学习与适应,才能确保在信息化时代中,网络安全得到有效保障,信息资产不受侵犯。

#### [参考文献]

- [1]朱昱林.计算机通信网络中的安全防护策略分析[J].集成电路应用,2023,40(4):340-341.
- [2]吴瑞祥,李祥,隋远.计算机网络信息安全及防护策略研究[J].中国新通信,2016,18(23):67.
- [3]程谢琚.计算机软硬件维护和网络安全防护问题及策略[J].卫星电视与宽带多媒体,2023(5):50-52.
- [4]韩琚,杨莉莉.计算机通信网络的安全防护策略分析[J].集成电路应用,2023,40(8):186-187.
- [5]李豪杰.计算机网络信息安全防护策略及评估算法分析[J].电脑编程技巧与维护,2023,(12):168-170.

#### 作者简介:

赵越(1991—),女,汉族,天津市滨海新区人,本科,助理工程师,研究方向:计算机。