

# 计算机网络安全技术的影响因素与防范措施

陈梓钰<sup>1</sup> 艾玲<sup>2</sup>

1. 66389部队 陕西 西安 710000

2. 78156部队 青海 西宁 816000

**摘要:** 在当今信息化社会, 计算机网络已经深度融入人们的日常生活与工作之中, 成为信息交流、业务开展、社交互动的重要平台。然而, 随着网络技术的迅猛发展, 网络安全问题也日益凸显, 对个人隐私、企业数据和国家安全造成了严重威胁。计算机网络安全技术作为维护网络安全的关键手段, 受到了广泛关注和研究。本文将深入探讨影响计算机网络安全技术的因素, 并提出相应的防范措施, 以期为保障网络安全提供有益的参考和借鉴。

**关键词:** 计算机网络; 安全技术; 影响因素; 防范措施

引言: 随着信息技术的快速发展, 计算机网络安全问题日益突出。本文重点探讨了影响计算机网络安全技术的因素, 并提出了相应的防范措施。通过分析, 我们发现网络设备、用户行为、恶意攻击和安全管理制度等方面都对网络安全产生了影响。为了应对这些威胁, 我们需要采取一系列有效的对策, 如建立安全管理制度、访问控制、数据加密、防火墙技术、入侵检测和防御以及病毒防范等。这些对策将有助于提高网络安全防护能力, 降低安全风险。

## 1 计算机网络安全技术的概述

计算机网络安全技术是保护计算机网络系统免受未经授权的访问、攻击、数据泄露、篡改或破坏的一系列技术和方法。随着信息技术的快速发展和互联网的广泛应用, 计算机网络安全问题日益突出, 网络安全技术的重要性也愈发凸显。首先, 计算机网络安全技术的主要目标是确保网络系统的机密性、完整性和可用性。机密性指的是保护信息不被未经授权的个人或实体获取; 完整性指的是保护信息在传输和存储过程中不被篡改或损坏; 可用性则是指保证授权用户能够正常访问和使用网络资源。为了实现这些目标, 计算机网络安全技术涵盖了多个方面, 包括防火墙技术、加密技术、入侵检测与防御系统、安全审计与日志分析、系统备份与恢复等。这些技术相互补充, 共同构建起一个多层次、全方位的网络安全防护体系。其次, 网络安全技术的发展始终伴随着网络攻击和威胁的演变<sup>[1]</sup>。因此, 网络安全技术需要不断更新和完善, 以应对日益复杂和多样化的网络安全挑战。这要求网络安全从业人员具备高度的专业素养和敏锐的安全意识, 能够及时发现和应对各种网络安全威胁。

## 2 计算机网络安全技术的影响因素

### 2.1 自然灾害和物理环境

自然影响因素是计算机网络安全技术中不可忽视的一环。这些因素通常包括自然灾害、恶劣的物理环境等不可抗力因素, 它们对计算机网络的安全造成严重的影响。首先, 自然灾害如地震、洪水、火灾等, 可能对计算机网络的基础设施造成严重破坏。这些灾害可能导致网络设备和通信线路损坏、数据中心瘫痪等后果, 进而影响网络的正常运行和服务。因此, 对于自然灾害的防范措施是必不可少的。此外, 各种威胁计算机安全硬件的恶劣环境也是需要关注的问题。例如, 过高的温度、过低的湿度、过多的灰尘等环境因素可能对计算机硬件设备造成损害, 影响其正常运行。因此, 保持计算机硬件设备所处环境的稳定和适宜条件是至关重要的。

### 2.2 协议安全的脆弱性

网络协议是计算机网络通信的基础, 其安全性对于整个网络的安全至关重要。然而, 由于设计和实现上的复杂性, 网络协议可能存在各种安全隐患和漏洞, 这些漏洞可能被黑客利用, 对网络进行攻击和破坏。首先, 网络协议的缺陷可能导致数据泄露。攻击者可以利用协议的漏洞, 窃取敏感信息, 如用户密码、私密数据等。例如, 一些协议在传输过程中未对数据进行加密, 或者加密算法存在缺陷, 导致数据被轻易截获和破解。其次, 网络协议的漏洞也可能导致数据被篡改。攻击者可以利用协议的漏洞, 对传输的数据进行篡改, 如插入恶意代码、篡改控制指令等。这可能导致系统被恶意攻击者控制、应用程序崩溃或数据损坏等严重后果。

### 2.3 人为因素

人为因素是计算机网络安全技术中另一个不可忽视的影响因素。人为因素可以分为内部人员威胁和外部人员威胁, 都可能对计算机网络的安全造成重大影响。首先, 内部人员威胁是一个重要的人为因素。由于内部人

员通常具有对网络的访问权限,因此他们可能出于各种目的对网络进行破坏或窃取数据。一些内部人员可能由于缺乏安全意识,无意中泄露敏感信息或破坏系统。而另一些人则可能出于个人利益或恶意目的,窃取数据、篡改系统或进行其他非法活动。其次,外部人员威胁也是不可忽视的人为因素<sup>[2]</sup>。外部人员通常是指网络攻击者、黑客等,他们可能利用网络漏洞进行攻击,窃取数据或破坏网络正常运行。

#### 2.4 病毒和黑客攻击

病毒和黑客攻击是计算机网络安全面临的严重威胁。随着网络的普及和技术的不断发展,病毒和黑客攻击的形式和手段也日益多样化,给网络安全带来了极大的挑战。首先,病毒是一种常见的网络安全威胁。病毒是一种恶意程序,可以通过网络、邮件、文件等方式进行传播。病毒可以在计算机系统中进行自我复制,并对系统进行破坏或窃取数据。一些病毒甚至可以远程控制被感染的计算机,使其成为僵尸网络的一部分,用于发起更大规模的攻击。其次,黑客攻击也是计算机网络安全面临的一种严重威胁。黑客利用网络漏洞和弱点,对计算机系统进行非法访问和攻击。黑客可能会窃取敏感数据、篡改系统、破坏应用程序等,甚至控制整个系统进行非法操作。黑客攻击通常具有隐蔽性和针对性,难以被发现和防范。

#### 2.5 数据安全风险

数据安全风险是计算机网络安全领域中的一个核心问题。在数据传输和存储的过程中,若没有采取适当的安全措施,数据可能会面临被窃取、篡改甚至丢失的风险。首先,在数据传输过程中,如果未使用加密技术或加密强度不足,攻击者可能截获数据并轻易解密,从而获取敏感信息。此外,在公共网络上传输数据时,若不使用安全的传输协议,也可能遭受中间人攻击,导致数据泄露。其次,在数据存储环节,如果未采取充分的访问控制和数据保护措施,内部或外部人员可能非法访问、篡改或删除数据。这不仅可能导致数据完整性受损,还可能引发一系列安全问题,如身份盗用、欺诈等。

### 3 计算机网络安全技术的防范措施

#### 3.1 建立安全管理制度

建立安全管理制度是保障计算机网络安全的基础。一个健全的安全管理制度可以提供清晰的指导,让所有员工明白自己在网络安全方面的责任。首先,必须制定详细的规章制度,明确指出哪些行为是允许的,哪些是禁止的,以及违反规定会受到的惩罚。这不仅包括对网络设备的使用,还涉及到数据的存储、传输和处理。其

次,这个制度应该明确每个人的网络安全责任。无论是管理层还是普通员工,每个人都应该对自己的网络行为负责,意识到自己的行为可能对整个网络的安全产生影响。此外,安全管理制度中还应包括安全控制要求。这包括对网络设备的安全配置、对系统的定期安全审查、对员工的安全培训等。这些控制要求能够确保网络设备和系统的安全,预防潜在的安全风险。最后,这个制度应该是动态的,能够随着网络环境和安全威胁的变化而变化。定期审查和更新安全管理制度,以确保其始终能反映当前的安全最佳实践。

#### 3.2 访问控制

访问控制是计算机网络安全的重要环节,其目的是确保只有经过授权的用户才能访问特定的网络资源。首先,制定并实施严格的访问控制策略是必要的。这些策略应明确规定不同用户或用户组对不同资源或操作的访问权限。这包括数据的读取、修改、删除等操作,以及某些特定的系统功能或应用的使用。其次,实施多层次的身份认证机制是保障访问控制有效性的关键。除了密码认证外,还可以引入动态口令、生物识别等技术,提高身份认证的安全性。同时,定期更换密码和实施强密码策略也是防止未经授权访问的有效手段。另外,审计和监控也是访问控制中不可或缺的部分<sup>[3]</sup>。通过记录用户的网络活动,可以及时发现异常行为或潜在的安全威胁,并采取相应的措施进行处置。此外,强化对远程访问的管理也至关重要。对于远程访问网络的用户,应采取VPN、加密通道等技术手段来确保数据传输的安全性。同时,对远程访问的设备进行安全检查,防止潜在的威胁通过远程访问进入网络。

#### 3.3 数据加密

数据加密是保护敏感数据免受未经授权访问的一种重要手段。通过数据加密,可以确保数据在传输和存储过程中的机密性和完整性。首先,数据加密技术可以应用于数据的存储和传输。在存储数据时,使用加密算法对敏感数据进行加密,将密文存储在数据库或硬盘上。这样,即使数据被非法获取,攻击者也无法解密和阅读原始数据。其次,数据加密在数据的传输中也起着重要作用。当数据在传输过程中,使用加密算法对数据进行加密,确保数据在传输过程中不被截获或篡改。通过使用安全的传输协议,如SSL/TLS,可以提供端到端的数据加密,确保数据在传输过程中的机密性和完整性。此外,对于特定的应用场景,还可以采用更高级的加密技术。例如,对于大数据应用,可以采用同态加密技术,允许对加密数据进行计算并得到加密结果,而不需要解

密原始数据。这样可以在保证数据隐私的同时进行数据处理和分析。为了确保数据加密的有效性,需要选择合适加密算法和密钥管理策略。

### 3.4 防火墙技术

防火墙技术是计算机网络中用于安全防护的重要措施。它利用一系列规则和策略,对进出网络的数据包进行检测和过滤,从而防止恶意流量和攻击对网络设备和系统造成损害。首先,防火墙可以阻止未授权的访问和数据传输。通过配置访问控制规则,防火墙能够识别并过滤掉来自外部网络的非法访问请求,如未授权的IP地址、恶意端口扫描等。这有助于防止恶意用户对内部网络的入侵和数据窃取。其次,防火墙具有流量监控和过滤功能。它可以实时监测网络流量,并根据设定的安全策略对可疑流量进行拦截。例如,防火墙可以阻止病毒传播、阻止DDoS攻击等。这有助于减轻网络设备和系统的负担,降低潜在的安全风险。此外,防火墙还具有日志记录和报警功能。它可以记录网络流量和安全事件,提供有价值的信息用于安全审计和事件调查。同时,当检测到可疑活动或攻击时,防火墙能够触发报警机制,及时通知管理员采取相应措施。

### 3.5 入侵检测和防御

入侵检测和防御是计算机网络安全的重要组成部分,用于实时监测和识别网络中的异常行为和恶意攻击,并及时采取措施进行响应和防御。首先,入侵检测系统(IDS)能够实时监控网络流量和系统状态,通过分析流量和日志数据,检测出异常行为和潜在的攻击行为。IDS可以识别出各种恶意活动,如未经授权的访问、恶意代码注入、拒绝服务攻击等。一旦检测到异常行为或攻击,IDS可以立即发出警报,并提供详细的信息帮助管理员进行事件处理。其次,入侵防御系统(IPS)则是一种主动的安全防护措施。IPS在网络中部署,能够实时检测并阻止恶意流量和攻击行为。与IDS相比,IPS不仅能够检测出攻击,还能自动采取措施,如丢弃恶意数据包、关闭恶意端口等,从而阻止攻击的进一步扩散。为了提高入侵检测和防御的效果,需要采取多种手段和技术。例如,可以结合使用基于签名的检测和基于异常行为的检测,以提高检测的准确性和适应性。同时,可以

结合防火墙、安全审计等其他安全措施,共同构建一个多层次的安全防护体系。

### 3.6 病毒防范

病毒防范是计算机网络安全的重要一环,可以有效防止病毒的传播和破坏。为了实现有效的病毒防范,需要采取一系列措施。首先,安装可靠的杀毒软件是必要的。市场上有许多知名的杀毒软件,它们能够实时监控系统运行状况,检测和清除病毒、木马等恶意程序。杀毒软件能够自动更新病毒库,及时识别和防御新型病毒,提供全面的防护<sup>[4]</sup>。其次,定期更新病毒库也是至关重要的。病毒库是杀毒软件的“数据库”,包含了已知病毒的特征和防御方法。定期更新病毒库能够使杀毒软件随时掌握新型病毒动态,从而有效防御病毒的攻击。此外,对系统和数据进行全面检测和清除也是关键环节。杀毒软件应该定期对系统和数据文件进行全面扫描,检测和清除潜在的病毒。同时,在发现病毒后,杀毒软件应该能够彻底清除病毒,避免病毒的残留和再次感染。为了提高病毒防范的效果,用户也需要养成良好的安全习惯。例如,不随意打开未知来源的邮件和链接、定期备份重要数据、不下载和运行未知来源的程序等。这些习惯有助于降低感染病毒的风险。

结语:综上所述,计算机网络安全是一个复杂且不断变化的领域,需要我们时刻保持警惕和采取有效的防范措施。通过综合运用多种安全技术和策略,我们能够提高网络的安全防护能力,降低安全风险,保护用户信息和系统的安全。在未来的发展中,我们需要不断加强计算机网络安全技术的研究和应用,以应对不断出现新的安全威胁和挑战。

### 参考文献

- [1] 於肇鹏.计算机网络安全技术的影响因素与防范策略分析[J].无线互联科技,2021,18(20):21-22.
- [2] 吴晖.计算机网络安全技术的影响因素探索[J].无线互联科技,2021,18(20):78-79.
- [3] 林旭凤.计算机网络安全技术的影响因素与防范策略[J].软件,2021,42(10):99-101.
- [4] 曾伟渊.计算机网络安全技术的影响因素与防范措施[J].河南科技,2021,40(19):24-26.