计算机网络信息安全及防护策略研究

薛荣胜　聂　伟　郭　易
中国酒泉卫星发射中心　甘肃　酒泉　732750

摘　要：随着互联网的不断发展，计算机网络信息安全问题成为一个热门话题。当前，网络安全攻击手段和技术越来越复杂，给用户、公司以及政府带来了很大的风险和挑战。因此，对计算机网络信息安全问题进行研究，制定防护策略也十分重要。本文将就计算机网络信息安全问题及防护策略进行深入的探讨。

关键词：计算机网络；信息安全；防护策略

引言：计算机网络具有高度的开放性和互联性，但其自身的结构特征也使其十分脆弱，易受攻击。随着计算机网络的普及，其安全隐患也越来越大。因此，必须充分认识到计算机网络的信息安全问题，并对其存在的问题进行了分析，提出了相应的对策，以增强其防范能力，防止其受到恶意的网络攻击，从而减少因网络信息泄漏而带来的巨大损失，从而有效地保证了网络的安全与稳定。

1 计算机网络信息安全重要性

计算机网络信息安全是指在计算机网络通信过程中，对计算机系统与网络进行保护，防止非法入侵、信息泄露、病毒攻击等信息安全威胁的一种保障措施。它主要涉及计算机软件、硬件、网络通信、数据存储等方面的安全问题，是维护企业的机密性、完整性、可用性和可靠性所必须的措施。计算机网络信息安全的重要性不言而喻。首先，安全的计算机网络能够保证企业机密信息不被非法获取、篡改或破坏，从而保证企业的商业利益。其次，信息安全还能保证企业的品牌形象和信誉不受损害，使企业在市场竞争中占有优势。另外，随着互联网和信息化的快速发展，越来越多的数据和信息在网络中传输和存储，信息安全问题也日益突出。安全的计算机网络不仅关乎企业自身的利益，也关乎整个社会的稳定和安全。为了保障计算机网络信息安全，需要采取一系列措施来进行管理和维护[1]。首先，企业需要对内部计算机网络进行全面评估，分析网络可能存在的安全隐患，制定相应的安全管理策略，确保网络安全。其次，企业需要开展内部的安全培训和宣传工作，加强员工的安全意识，降低安全隐患发生的概率。此外，企业还需要加强对网络设备的管理和维护，及时更新安全补丁，加强对敏感数据的访问控制，增强系统鉴别能力，防止恶意攻击和黑客入侵。

2 计算机网络信息安全问题分析

2.1 计算机病毒

（1）计算机病毒是一种恶意软件，其目的是为了破坏或控制计算机系统，或传播自身到其他系统。它们可以复制自身并在计算机系统中传播，对计算机产生破坏或潜在的危害。计算机病毒通常是非法软件，其目的是进行恶意活动，例如窃取个人信息、破坏系统、传播广告等等。（2）计算机病毒的出现可以追溯到上世纪80年代初，当时它们只是简单的程序，但随着计算机技术的迅速发展和网络的大规模普及，计算机病毒逐渐成为了网络攻击的主要手段之一。如今，计算机病毒已经成为了一种全球性的安全威胁，能够对计算机系统、信息和数据造成极大的破坏和损失。（3）常见的计算机病毒包括木马病毒、蠕虫病毒、文件型病毒等。木马病毒通常会伪装成合法软件来诱骗用户安装，然后对其进行远程控制和操纵。蠕虫病毒是一种自我复制的程序，可以通过网络传播并感染其他系统。文件型病毒是一种感染文件类型的病毒，可以修改文件代码并破坏文件内容。（4）计算机病毒的侵袭可能会对系统造成数据、信息、应用程序被破坏的风险，产生很大的财物损失或重要数据丢失的后果。因此，防范和清除计算机病毒是非常重要的。一般来说，防范计算机病毒需要采取多种措施，包括安装杀毒软件、更新系统补丁、不随意安装未知来源的软件、加强安全意识等。同时，如果计算机系统受到了病毒的侵袭，需要及时采取措施进行清除和修复，避免造成更大的损失。

2.2 网络钓鱼

网络钓鱼是一种常见的网络攻击手段，其利用了社交工程学的原理，通过伪装成可信的来源，诱骗用户提供机密信息或进行未经授权的数据收集。网络钓鱼的攻击手段有多种，其中最常见的是通过电子邮件附件或URL链接进行欺骗。攻击者会伪装成银行、网站、机构等可信的来源，向用户发送电子邮件或短信，要求用户

点击链接或下载附件。一旦用户点击了链接或下载了附件，攻击者就可以通过恶意代码或病毒来获取用户的敏感信息，或者进行未经授权的数据收集。除了电子邮件和URL链接，网络钓鱼还可以通过其他方式进行，比如在社交媒体上伪装成真实的人士，与用户建立联系，并利用社交工程学原理骗取用户的敏感信息[2]。

2.3 网络蠕虫

网络蠕虫是一种常见的恶意软件，它能够在网络中自我复制，利用漏洞进入系统，并破坏网络的安全性。网络蠕虫具有快速传播、危害性强等特点，在短时间内可能会感染大量的计算机系统，危害非常严重。网络蠕虫的传播方式有多种，其中最常见的是通过电子邮件附件或URL链接进行传播。攻击者会将蠕虫代码伪装成电子邮件或网页，诱使用户点击链接或下载附件。一旦用户点击了链接或下载了附件，蠕虫就可以在系统中繁殖，并利用漏洞攻击其他系统。除了电子邮件和URL链接，网络蠕虫还可以通过其他方式进行传播，比如网络共享、漏洞利用等。网络蠕虫在传播过程中，会不断扫描网络中的其他计算机系统，寻找漏洞并进行攻击。网络蠕虫的危害非常严重，它能够破坏计算机系统的正常运行，导致数据丢失、系统瘫痪、网络中断等问题。此外，网络蠕虫还能够窃取用户的敏感信息，如密码、银行卡号等，对用户的隐私和财产造成威胁。

2.4 黑客攻击

黑客攻击是一种常见的网络攻击行为，其目的是侵犯计算机系统，并获取或破坏系统内的数据。黑客攻击的形式多种多样，包括密码破解、拒绝服务攻击、非法入侵等。其中，密码破解是黑客攻击最常见的形式之一。黑客会利用各种手段，如暴力破解、社交工程学等方法，尝试破解系统的登录密码或其他敏感信息。如果黑客成功破解了密码，他们就可以非法进入系统，获取或篡改数据。拒绝服务攻击也是黑客攻击的常见形式。这种攻击方式是通过向系统发送大量的无用的请求，使得系统无法正常处理合法用户的请求，从而实现攻击目的。这种攻击方式可能会导致系统瘫痪或服务中断，对系统的稳定性和可用性造成严重影响。非法入侵是另一种常见的黑客攻击形式。这种攻击方式是通过利用系统漏洞或用户弱密码等手段，非法进入系统，获取或破坏系统内的数据。非法入侵可能会对系统的安全性和稳定性造成严重威胁。

3 信息安全防护策略研究

3.1 设备安全保护

设备安全保护是确保计算机系统稳定运行和数据安全的重要措施。以下是一些设备安全保护的措施：（1）设置防火墙：防火墙是保护计算机系统安全的第一道防线，它可以阻止未经授权的网络流量和攻击。防火墙可以通过过滤网络流量、阻止非法访问等方式来保护计算机系统不受攻击。（2）及时升级和修补操作系统、应用软件：操作系统的漏洞和应用程序的漏洞可能会被攻击者利用，因此及时升级和修补操作系统和应用软件是非常重要的[3]。这样可以确保计算机系统的安全性和稳定性。（3）定期检查系统中的病毒：计算机病毒是对计算机系统安全的一种重大威胁。为了防止病毒的感染和传播，应该定期检查系统中的病毒，并安装杀毒软件来清除病毒。（4）加强对计算机的维护和管理：计算机的维护和管理是保护计算机系统安全的基础。应该定期清理计算机系统中的垃圾文件和临时文件，保持良好的系统状态。同时，应该避免在计算机上安装不必要的软件，避免下载不明来源的软件和文件。

3.2 网络安全加密

网络安全加密是保护敏感数据的一种重要措施。在信息传输和存储过程中，应该采用数据加密技术来保护数据的机密性、完整性和可用性。数据加密技术是通过将原始数据转换为密文，从而防止未经授权的人员获取和利用数据。数据加密技术可以使用不同的算法，如对称加密和非对称加密。对称加密使用相同的密钥对数据进行加密和解密，而非对称加密使用公钥和私钥两个密钥来进行加密和解密。在信息传输过程中，可以使用传输层加密技术，如SSL/TLS协议来保护数据的机密性和完整性。传输层加密技术可以确保数据在传输过程中的机密性，通过使用加密算法和密钥来对数据进行加密。同时，传输层加密技术也可以保护数据的完整性，通过添加消息认证码来确保数据在传输过程中没有被篡改。在信息存储过程中，可以使用存储加密技术来保护数据的机密性和完整性。存储加密技术可以通过对数据进行加密和对访问进行控制来保护数据的机密性。同时，存储加密技术也可以通过备份和恢复机制来保护数据的完整性[4]。

3.3 密码安全保护

密码安全保护是保护个人信息和数据安全的重要措施。在使用敏感信息应用程序时，应该采取完善的密码保护措施，以降低信息泄露的风险。首先，应该禁止使用简单的密码。简单密码容易被猜测或破解，从而容易被攻击者获取敏感信息。应该采用多种复杂性强的密码组合，包括数字、字母和特殊字符的组合，以增加密码的强度。其次，应该定期修改密码。定期修改密码可以避免密码被攻击者破解或泄露后长时间内无法发现。同

时，也应该限制访问权限，避免不需要的人员获取敏感信息。此外，应该采用多因素身份验证机制，如同时使用密码和手机验证码或指纹识别等方式进行身份验证。多因素身份验证可以增加身份验证的强度，降低身份冒充的风险。最后，应该注意保护密码信息的安全。不要将密码记录在明文或简单的加密方式中，以避免密码被泄露。同时，也应该避免在公共场合或非安全网络环境下输入密码，以减少密码被窃取的风险。

3.4 信息员工培训和管理

企业应该定期对员工进行网络安全培训，使员工具备基本网络安全知识和技能，以避免由于员工操作不当导致的安全问题。首先，企业应该制定网络安全培训计划，包括网络安全基础知识、网络安全风险和应对措施等方面的培训内容。通过培训，使员工了解网络安全的重要性，掌握网络安全的基本知识和技能，能够正确地处理网络安全事件。其次，企业应该持续地进行监管控制，确保员工行为合规、规范运营。企业应该建立完善的网络安全管理制度，明确员工的网络安全职责和操作规范。同时，企业应该对员工的网络行为进行监控和管理，及时发现和纠正员工的违规行为。此外，企业在员工离职之前应该注销所有密码和独立访问权限，以避免离职员工非法访问企业网络和数据。企业应该建立员工离职处理流程，明确注销密码和访问权限的操作步骤，确保员工离职后企业网络和数据的安全。

3.5 保障网络重要信息的备份和恢复

保障网络重要信息的备份和恢复是确保企业网络连续性和数据安全的重要措施。以下是一些建议：（1）建立备份计划：企业应该建立完善的备份计划，明确备份时间和备份周期。备份计划应该考虑到企业的业务需求和数据重要性，确保备份数据的完整性和准确性。（2）选择合适的备份设备：企业应该选择安全的备份设备，如离线存储设备、云存储等。备份设备应该具备高度的可靠性和稳定性，能够保证备份数据的完整性和安全性。（3）及时更新备份数据：企业应该及时更新备份数据，确保备份数据的最新性和完整性[5]。同时，企业应该定期测试备份数据的可恢复性，确保在需要恢复数据时能够快速、准确地恢复数据。（4）建立数据恢复计划：企业应该建立完善的数据恢复计划，明确数据恢复流程和操作步骤。数据恢复计划应该考虑到各种数据丢失情况，包括备份设备损坏、数据逻辑错误等。（5）测试数据恢复计划：企业应该定期测试数据恢复计划，确保数据恢复计划的可行性和有效性。在测试过程中，企业应该模拟各种数据丢失情况，测试数据恢复计划的恢复能力和稳定性。

结语

计算机网络安全问题涉及的范围非常广泛，防护策略也非常复杂。针对这些网络安全问题，如病毒、黑客、网络钓鱼、网络蠕虫等，不同的防范措施应该被制定。而企业或用户在正式使用计算机网络之前，应该对网络安全风险进行全面的评估和分析,包括系统弱点,用户信息安全等。然后建立网络安全管理体系，制定科学的网络安全防护策略和管理措施。只有慎之又慎地对计算机网络信息解决方案、安全技术、应急预案等方面进行充分的研究，才能有效地保护计算机网络安全，进一步落实和加强网络安全。

参考文献

[1]史伟民.计算机网络信息安全及防护策略研究[J].通信电源技术,2021,38(5):186-188.

[2]孟东雪.计算机网络信息安全及防护策略研究[J].数码世界,2019(4):229.

[3]辛培成.大数据时代计算机网络信息安全及防护策略研究[J].中国新通信,2021,23(3):131-132.

[4]蔡彬彬，孙忠辉.计算机网络信息安全问题及防护策略研究[J].长春理工大学学报（自然科学版），2019，42（3）：128-132；137.

[5]顾云,史正林.新时期计算机网络信息安全技术分析[J].电脑编程技巧与维护,2021(06):164-165.