

计算机网络安全存在的问题及对策研究

白 茹

西安电子工程研究所 陕西 西安 710100

摘 要: 现在计算机网络已经遍布了我们周围的生活,它无处不在,通过计算机网络就可以进行比较快捷地传递信息,而且它简单、快速,是在现代网络化发展的大趋势中应运而生的。计算机网络能够在快捷、方便地传递信息的同时,还可以做到数据共享。人类也能够利用计算机网络这种平台分享交换各自的资料,大家可以共同交换信息、共享。所以,计算机网络也可以说是一种传递信息、共享的网络系统。

关键词: 计算机网络安全; 问题; 对策研究

引言: 随着互联网技术的飞速发展,计算机网络已经成为人们生活、工作、学习等方面不可或缺的一部分。然而,网络安全问题也随之而来,给个人和企业带来了巨大的损失。本文将对计算机网络安全存在的问题进行分析,并提出相应的对策建议。

1 计算机网络安全基本概述

计算机网络安全是指保护计算机网络系统及其数据不受未经授权的访问、使用、披露、破坏、修改或者破坏的措施。随着互联网的普及和信息技术的飞速发展,网络安全问题日益严重,对个人、企业乃至国家安全造成了极大的威胁。为实现这些目标,计算机网络安全需要采取多种措施,包括加密技术、访问控制、防火墙、入侵检测系统等。加密技术是计算机网络安全的核心手段之一,通过对信息进行加密处理,可以有效地防止未经授权的用户获取或篡改信息。常见的加密技术有对称加密算法和非对称加密算法。对称加密算法是指加密和解密使用相同的密钥,如DES、AES等;非对称加密算法是指加密和解密使用不同的密钥,如RSA、ECC等。加密技术在保护通信过程中的数据安全方面发挥着重要作用。访问控制是计算机网络安全另一个重要组成部分,它通过对用户的权限进行限制,确保用户只能访问其被授权的资源。访问控制可以分为身份认证和授权两个层次。身份认证是指确认用户的身份,通常通过用户名和密码来实现;授权是指确定用户可以访问哪些资源以及执行哪些操作,通常通过访问控制列表(ACL)来实现。访问控制技术在防止未经授权的用户访问敏感资源方面具有重要意义。防火墙是计算机网络安全的第一道防线,它通过对网络流量进行监控和过滤,阻止恶意用户进入内部网络。防火墙可以分为硬件防火墙和软件防火墙。硬件防火墙是指具有专门硬件设备的安全设备,如ASA、Fortinet等;软件防火墙是指基于操作系统

的软件程序,如Windows防火墙、Linux防火墙等^[1]。防火墙在保护内部网络免受外部攻击方面发挥着关键作用。入侵检测系统(IDS)是一种实时监控系统,用于检测网络中的异常行为和攻击事件。IDS通常部署在网络的边缘,对网络流量进行实时监控和分析,一旦发现异常行为或攻击事件,就会立即报警并采取相应的措施。IDS可以帮助网络管理员及时发现和应对网络安全威胁,提高网络的安全性能。计算机网络安全还需要关注其他一些方面的问题,如物理安全、人员管理、安全意识培训等。只有综合运用各种技术手段和管理措施,才能有效地保障计算机网络安全。

2 计算机网络安全存在的问题

2.1 网络攻击手段日益翻新

随着互联网技术的快速发展,网络攻击手段也在不断地翻新和升级。网络安全问题已经成为了全球关注的焦点,尤其是在个人信息安全、企业数据安全以及国家网络安全等方面。网络攻击手段的多样化使得网络安全防护面临巨大的挑战。传统的防火墙、入侵检测系统等安全设备很难应对新型的网络攻击手段,如DDoS攻击、APT攻击等。这些新型攻击手段往往具有高度隐蔽性、针对性强、难以防范等特点,给网络安全带来了极大的隐患。网络攻击手段的不断翻新导致了网络犯罪活动的日益猖獗。黑客利用各种攻击手段,窃取个人信息、企业数据,甚至进行勒索、诈骗等犯罪活动,给个人和企业带来了严重的损失。随着网络攻击手段的不断升级,网络安全专业人才需要具备更高的技能和素质,以应对日益严峻的网络安全形势。然而,目前我国网络安全人才的培养还存在很大的问题,如教育体系不完善、人才流失严重等,这些问题都制约了我国网络安全人才的发展。

2.2 网络安全意识薄弱

随着信息技术的飞速发展,计算机网络已经渗透到

社会生活的各个方面。然而，网络安全问题也日益突出，给个人、企业和国家造成了巨大的经济损失和信息安全风险。其中一个重要的问题就是网络安全意识薄弱。许多人在使用计算机网络时，缺乏必要的安全意识和防范意识。他们往往随意泄露个人信息，如银行卡号、密码、身份证号等，或者在社交媒体上公开发布私人照片、旅行计划等敏感信息，这些都为不法分子提供了可乘之机。一些人在使用公共Wi-Fi时，不注意保护个人信息，容易被黑客窃取敏感数据。除了个人用户外，一些企业和组织也存在网络安全意识薄弱的问题。他们往往只关注业务发展和技术创新，忽视了网络安全的重要性。一些企业甚至为了节省成本，不愿意在网络安全方面进行投入，导致系统漏洞百出，容易遭受攻击和入侵。此外，一些组织在采购设备和软件时，过于追求功能和性能，忽视了安全因素，也给计算机网络安全带来了隐患。网络安全意识薄弱还表现在对新技术的盲目追求上。随着物联网、云计算、大数据等新技术的不断涌现和应用，新的安全问题也不断出现。一些人盲目追求新技术的新奇和便利，忽视了其带来的安全风险和挑战。例如，智能家居设备可能会被黑客攻击和控制，造成家庭隐私泄露或者财产损失；云计算服务可能会因为安全漏洞而导致用户数据泄露或者被篡改。

2.3 内部安全管理不善

计算机网络安全问题是当前全球面临的重大挑战之一，尤其是对于内部安全管理不善的情况，内部网络中的数据和资源可能被未经授权的人员访问，这可能导致数据泄露，系统损坏，甚至更严重的安全问题。许多组织仍然使用过于简单或重复的密码，这使得黑客能够轻易地破解这些密码并获取对系统或数据的访问权限。软件和系统的漏洞通常通过定期更新来修复，但许多组织由于缺乏足够的资源或人员，无法及时进行更新，从而使这些漏洞长期存在。例如，开放的端口、不安全的协议和服务等都可能安全威胁^[2]。许多员工可能不了解基本的网络安全知识，例如如何识别和避免钓鱼攻击，或者如何安全地处理电子邮件等。当网络安全事件发生时，没有明确的应急响应计划可能会导致反应不及时，错失处理问题的最佳时机。即使有再强大的网络安全措施，如果硬件设备被盗或丢失，也可能导致数据泄露。在发生数据丢失或系统崩溃的情况下，如果没有足够的备份和恢复机制，可能会导致重要数据永久丢失。

2.4 木马病毒程序

木马病毒是一种非常常见的网络安全威胁，它通过伪装成有用或无害的程序来欺骗用户下载和安装。然

而，尽管木马病毒在技术上可能非常复杂和难以检测，但它们仍然存在许多问题和挑战。木马病毒的隐藏性是其最大的问题。由于木马病毒通常会伪装成正常的系统文件或应用程序，因此它们很难被用户或防病毒软件发现。这使得木马病毒能够长时间潜伏在用户的计算机上，窃取敏感信息，或者对系统造成破坏。木马病毒的传播方式也非常多样。除了通过电子邮件附件、下载链接或恶意网站下载外，一些高级的木马病毒甚至可以自我传播，通过感染其他计算机来扩大其影响范围。这种自我复制的能力使得木马病毒的威胁更加严重。木马病毒的防御也面临着巨大的挑战。由于木马病毒的种类繁多，且不断出现新的变种，因此防病毒软件需要不断更新以识别和阻止新的木马病毒。然而，即使是最好的防病毒软件也不能完全避免所有的威胁。

3 计算机网络安全对策研究

3.1 加强网络安全防护体系建设

计算机网络安全对策是保障网络信息安全的重要手段，加强网络安全防护体系建设是实现网络安全的关键。为了有效应对日益严峻的网络安全形势，每个网络用户都应该认识到网络安全的重要性，增强自我保护意识，遵守网络道德规范，不参与非法网络活动，不传播有害信息，共同维护网络空间的安全和稳定。我们应该加大对网络安全技术的投入，鼓励企业和科研机构开展网络安全技术研究，不断提高网络安全防护能力。同时，要加强国际合作，引进国外先进的网络安全技术和管理经验，提升我国网络安全水平。加强对网络安全的立法工作，制定完善的网络安全法律法规，为网络安全防护提供法律依据。要加大对网络犯罪的打击力度，严厉打击网络黑客、病毒传播等违法犯罪行为，维护网络空间的法治秩序。将网络安全教育纳入国民教育体系，培养更多的网络安全专业人才。同时，要加强对在职人员的网络安全培训，提高他们的网络安全防护意识和技能，确保网络安全工作的落实。企业应建立健全网络安全应急响应机制，及时发现和处置网络安全事件，减少网络安全风险。同时，要加强与其他国家和地区的网络合作，共同应对跨国网络安全威胁。我们要从多方面入手，共同努力，为构建安全、和谐的网络空间贡献力量。

3.2 提高网络安全意识

为了提高计算机网络安全意识，可以通过宣传教育活动、在线安全课程、安全提示等方式，向用户普及网络安全知识，提高用户对网络安全的认知和理解能力，引导用户养成良好的上网习惯和安全意识。组织应该建

立健全的安全管理制度和操作规程,规范员工的日常行为和工作流程,明确安全责任和要求,加强安全意识的培养和教育,提高员工的安全意识和技能水平。应该加强对计算机网络安全的管理,制定和完善相关法律法规和标准规范,为计算机网络安全提供保障和支持。同时加强执法力度,严厉打击网络犯罪活动,维护网络秩序和安全。全社会应该共同努力,营造一种关注网络安全、重视网络安全的文化氛围,使每个人都认识到计算机网络安全的重要性,树立正确的安全观念和价值观,增强自我保护意识,防范安全风险的发生。通过加强教育和培训、建立管理制度、加强法律法规建设和执法力度、建立网络安全文化等措施,我们可以提高个人和组织的安全意识和防范意识,共同维护计算机网络安全。

3.3 完善内部网络安全管理制度

计算机网络安全对策是保护计算机网络免受未经授权的访问、破坏或更改的一系列措施。为了确保网络安全,我们需要完善内部网络安全管理制度。企业应制定详细的网络安全政策和规程,明确网络安全的目标、责任和要求,确保员工了解并遵守相关规定。定期对员工进行网络安全培训,提高员工的网络安全意识和技能,使他们能够识别潜在的网络安全威胁并采取相应的预防措施。定期对企业的网络系统进行安全检查,发现并及时修复潜在的安全隐患。制定网络安全应急预案,确保在发生网络安全事件时能够迅速、有效地应对,降低损失。采用强密码策略,实施多因素身份认证,限制用户权限,防止未经授权的访问和操作。对存储和传输的敏感数据进行加密处理,确保数据安全^[3]。加强员工对网络钓鱼和恶意软件的防范意识,提供安全防护工具,定期更新防病毒软件。通过网络流量监控工具,实时了解网络运行状况,发现异常流量并及时处理。定期对企业的重要数据进行备份,以防数据丢失或损坏。企业还应密切关注网络安全领域的最新动态和技术发展,不断优化和完善网络安全管理制度,以应对不断变化的网络安全威胁。

3.4 安装杀毒软件

计算机网络安全对策是保护计算机系统免受未经授权的访问、破坏或泄露信息的措施。杀毒软件可以检测和清除计算机中的病毒、恶意软件和其他威胁。确保选择一款可靠的杀毒软件,并定期更新其病毒库以保持最新的防护能力。防火墙是一种网络安全设备,用于监控和控制进出网络的流量。它可以阻止未经授权的访问,并提供额外的安全层。确保在网络中设置适当的防火墙规则,以限制对敏感信息的访问。通过使用加密协议(如SSL/TLS)对数据进行加密,可以防止敏感信息在传输过程中被窃取或篡改。确保在使用互联网时使用安全的连接方式,并避免在不安全的网络上进行敏感信息的传输。使用强密码是保护个人和组织信息安全的重要措施。确保为每个账户设置独特且复杂的密码,并定期更改密码以增加安全性。此外,禁止共享密码和重复使用相同的密码。及时安装操作系统和应用程序的安全补丁和更新,以修复已知的漏洞和安全问题。这有助于提高系统的安全性,并减少潜在的风险。根据员工的角色和职责,限制对敏感信息的访问权限。确保只有经过授权的人员才能访问关键数据和系统。通过采取这些计算机网络安全对策,可以有效地保护计算机系统免受各种网络威胁和攻击。然而,网络安全是一个不断演变的领域,因此需要持续关注最新的安全技术和威胁情报,以及定期评估和更新安全措施。

结语

计算机网络安全问题是一个复杂的系统工程,需要政府、企业和个人共同努力。只有建立健全的网络安全防护体系,提高网络安全意识,完善内部管理制度,加强国际合作与交流,才能有效应对网络安全挑战,保障网络空间的安全与稳定。

参考文献

- [1]蔡海珍.计算机网络安全性维护研究思路构建[J].网络安全技术与应用,2020(11):5-6.
- [2]赵任飞.计算机网络信息安全威胁及数据加密技术探究[J].网络安全技术与应用,2020(11):40-41.
- [3]蒋回生.大数据时代计算机网络安全及防范措施研究[J].网络安全技术与应用,2020(11):71-72.