

浅析计算机网络安全防范措施

奚永强

苏州江南航天机电工业有限公司 江苏 苏州 215100

摘要：计算机网络安全是信息技术领域的重要议题，涉及技术、用户行为及系统多个层面。随着技术的不断更新，网络安全面临新的挑战，如新型攻击手段的出现。用户行为与安全意识的不足也加剧了安全风险，同时系统与软件自身存在的缺陷成为攻击的突破口。为了应对这些威胁，需采取一系列防范措施，包括提升用户安全意识、加强隐私加密、完善防火墙设置以及强化网络环境管理，确保计算机系统的稳定运行和数据安全。

关键词：计算机；网络安全；防范措施

引言

计算机网络安全是确保信息系统稳定运行和数据保护的关键。随着信息技术的飞速发展，网络安全问题日益凸显，成为制约信息技术应用的重要因素。技术的不断更新虽然带来了便利，但也催生了新的安全挑战。用户行为的不规范和安全意识的淡薄，以及系统与软件自身存在的安全漏洞，都为黑客攻击提供了可乘之机。因此，深入探讨计算机网络安全防范措施，对于保障信息安全具有重要意义。

1 计算机网络安全概述

计算机网络安全是一个复杂而关键的领域，它专注于保护计算机网络系统中的硬件、软件和数据免受恶意攻击、破坏或非法访问。这一领域涵盖了一系列技术和策略，旨在确保信息的机密性、完整性和可用性。在计算机网络安全范畴内，防火墙扮演着至关重要的角色，防火墙通过监控和控制进出网络的数据流，有效阻止未经授权的访问和潜在威胁。它们能够基于预设的安全规则，对数据包进行过滤和检查，从而构建起网络安全的第一道防线。除了防火墙，加密技术也是保障计算机网络安全的重要手段，通过对敏感数据进行加密处理，即使数据在传输过程中被截获，攻击者也无法轻易解读其内容。这极大地增强了数据的保密性和安全性，保护了用户隐私和业务机密。入侵检测系统（IDS）和入侵防御系统（IPS）是另外两种关键的网络安全组件，IDS能够实时监控网络活动，检测并报告可疑行为，而IPS则更进一步，能够主动采取措施阻止检测到的攻击。这些系统共同协作，为网络提供了实时的威胁感知和响应能力。随着云计算、大数据和物联网等新兴技术的快速发展，计算机网络安全面临着更加复杂和多样化的挑战。为了应对这些挑战，网络安全专业人员需要不断更新知识和技能，采用先进的安全技术和策略，以确保网

络系统的持续安全和稳定。计算机网络安全是一个不断发展和演变的领域，需要综合运用多种技术和策略来应对不断出现的威胁和挑战。

2 计算机网络安全现状分析

2.1 技术更新带来的新挑战

在信息技术日新月异的今天，计算机网络的安全环境正经历着前所未有的变革。云计算技术的广泛应用，无疑为数据存储与处理提供了前所未有的便捷性，但这也对数据隐私保护提出了新的挑战。在云计算服务中，数据往往被存储在远程服务器上，这就要求服务提供商必须构建出足够强大的安全防护体系，以防止数据被非法访问或篡改。然而，现实情况却是，随着云计算的普及，数据泄露事件频发，如何确保数据在云端的安全存储与传输，已成为当前网络安全领域亟待解决的关键问题。大数据技术的崛起，为数据分析与挖掘提供了强大的支持，但这也使得数据泄露的风险进一步加剧。在大数据环境下，数据规模庞大且类型多样，一旦安全防护措施不到位，就可能导致敏感信息被泄露，进而引发严重的后果。因此，如何在大数据环境下构建出有效的安全防护机制，以确保数据的机密性、完整性和可用性，是当前网络安全领域面临的重要课题。物联网技术的快速发展，使得越来越多的智能设备接入网络，但这也为网络安全带来了新的隐患。物联网设备往往存在安全漏洞，一旦被黑客利用，就可能造成严重的后果。高级持续性威胁（APT）等隐蔽性强、持续时间长的攻击手段，也对传统的安全防护体系构成了严峻挑战。这些攻击手段往往难以被传统的安全防护工具所检测，这就要求我们必须不断更新安全防护策略，以应对日益复杂的网络安全威胁^[1]。

2.2 用户行为与安全意识的不足

在网络安全防护体系中，用户行为与安全意识的不足

足构成了不容忽视的潜在威胁。尽管网络安全技术日新月异,防火墙、入侵检测、数据加密等防护措施日益完善,但用户作为网络安全防护体系中的首要环节,其行为模式和安全意识水平的高低,直接决定了整个安全链条的稳固性。遗憾的是,众多用户在网络安全知识方面存在明显短板,这不仅体现在对复杂密码策略的忽视上,如频繁使用生日、电话号码等简单信息作为密码,为黑客提供了轻易破解的机会;还表现在对网络信息的盲目信任上,用户往往未经核实便随意点击来自不明来源的链接,这种行为极易触发钓鱼攻击,导致个人信息被窃取。软件补丁的更新也是用户容易忽视的一环,许多用户出于习惯或懒惰,未能及时安装系统或应用程序的安全更新,这些更新往往包含了修复已知漏洞的重要补丁,一旦缺失,将使得系统暴露在已知的攻击风险之下。随着移动办公和远程工作模式的兴起,用户在不同网络环境下使用个人设备进行工作的现象愈发普遍,这无疑进一步增加了网络安全管理的难度。在非安全环境下,个人设备往往缺乏足够的安全防护,加之用户自身安全意识的淡薄,使得数据泄露、恶意软件感染等风险事件频发,对组织的网络安全构成了严重威胁。因此,加强用户安全教育和培训,提升用户的安全意识和防护能力,已成为当前网络安全工作的重要任务。

2.3 系统与软件的固有缺陷

计算机系统和应用软件在设计和开发阶段,由于技术限制、开发周期紧张或需求理解偏差等因素,难以完全避免漏洞和缺陷的存在,这些漏洞可能潜藏于代码的深处,表现为逻辑错误、内存泄漏、未授权访问等多种形式。一旦这些漏洞被黑客识别并利用,就可能成为他们渗透系统、窃取数据或破坏服务的突破口,对系统的完整性和安全性构成严重威胁。软件更新滞后也是导致系统安全漏洞频发的重要原因,随着技术的不断进步和黑客攻击手段的不断演变,旧版本的软件往往难以抵御新型的攻击方式。由于更新流程繁琐、测试不充分或用户抵触更新等原因,许多系统仍然运行着存在已知漏洞的旧版本软件,从而大大增加了被攻击的风险。补丁管理不善和系统配置不当也是导致系统安全漏洞的重要因素,补丁是修复软件漏洞的重要手段,但如果补丁的部署不及时、不完整或未经充分测试,就可能引入新的安全问题。同样,系统配置不当也可能导致安全策略失效,使系统暴露在潜在的安全威胁之下。因此,加强补丁管理和系统配置审核,确保系统的安全性和稳定性,是保障网络安全不可或缺的一环,及时发现并修复系统与软件的漏洞,是维护网络安全的重要基石^[2]。

3 计算机网络安全防范措施

3.1 提升计算机用户安全防范意识

(1) 随着时代的不断进步和科学技术的迅猛发展,计算机用户的安全防范意识却显得相对薄弱,这一现象已成为众多计算机网络安全事件的重要诱因之一。为了构建一个和谐且安全的互联网环境,计算机用户的作用不容忽视,他们亟需增强自身的网络安全意识。在使用电脑的过程中,用户应当主动注册个人账号,并设置包含大小写字母、数字及特殊符号的复杂密码,确保账号的安全性。IP地址应与个人设备绑定,以避免被他人非法占用或攻击,用户还应根据实际需求,合理设置个人访问计算机的权限,限制未经授权的访问行为。(2) 针对重要文件和数据的安全保护,计算机用户应树立正确的备份意识。通过定期将重要文件备份至外部存储设备或云端服务器,用户可以有效避免因系统故障或数据丢失而导致的损失。对于包含敏感信息的重要文件,用户还应采取先进的加密保护措施,确保这些信息在传输和存储过程中的安全性。通过加强数据加密和访问控制,用户可以进一步提升重要信息和数据的安全等级。(3) 为了应对不断变化的网络安全威胁,计算机用户还应及时升级系统、软件和硬件。通过定期更新补丁和修复漏洞,用户可以显著降低被黑客攻击的风险。用户还应学会科学使用计算机,避免访问不明网站或下载未知来源的软件,以减少潜在的安全隐患。通过这些措施的实施,计算机用户将能够在享受互联网便利的同时,更好地保障自身的信息安全。

3.2 加强隐私加密设置

(1) 病毒入侵作为网络安全领域的一大威胁,给计算机使用者带来了极大的困扰,尤其是对数据的破坏和盗取,更是让使用者深感忧虑。为了应对这一挑战,数据加密技术应运而生,成为确保重要数据安全、防止数据被盗取的重要手段。数据加密在计算机使用中的普及程度日益提高,其高安全性也得到了大量事实的验证。(2) 数据加密技术,简而言之,就是对重要信息进行密码设置,使得只有设置者及知道密码的人才能打开并访问这些文件。这种技术手段在保护数据安全方面发挥了重要作用。数据加密并非万无一失,其在使用过程中也存在一些潜在的弊端。例如,在认证过程中,信息仍然需要通过网络进行传输,这就给了侵入者窃取登录信息的机会。尽管数据加密技术具有较高的安全性,但仍需警惕其可能存在的隐患。(3) 为了进一步提升网络安全性,目前隐私加密控制已经发展出了多种技术手段。其中,密钥加密和公开密钥加密是两种常见的加密方式,

它们通过不同的算法和密钥管理机制,为数据提供了更为严密的保护。对IP进行接入控制也是一种有效的安全措施,它可以通过限制访问权限,防止未经授权的用户访问网络资源。这些技术手段的应用,为网络安全性提供了有力的保障,使得计算机用户在使用网络时能够更加安心^[3]。

3.3 加强防火墙设置

(1) 防火墙作为网络安全的核心组件,通过精心设计的规则集,对所有进出网络的数据包实施严格的监控与过滤流程,确保仅允许符合安全策略且经过授权的数据流通。这种基于明确规则的访问控制机制,构筑起一道坚不可摧的防线,有效抵御了未经授权的访问请求及潜在的恶意攻击。防火墙还具备强大的网络流量记录与分析能力,能够实时监测网络活动,及时发现并报告异常行为,为管理员提供宝贵的洞察信息,助力其迅速响应并处置安全威胁,从而全方位提升了系统的安全防护水平。(2) 随着网络技术的日新月异,防火墙的功能亦随之不断演进与增强。现代防火墙在坚守基本的包过滤职责之余,更融入了状态检测、应用层代理等多元安全策略。这些进阶功能赋予防火墙更高的灵活性与智能性,使其能在错综复杂的网络环境中游刃有余,有效抵御层出不穷的新型网络攻击。特别是状态检测防火墙,凭借其对网络连接状态信息的实时追踪能力,实现了对数据包的深度识别与精准管控,进一步巩固了网络安全防线。(3) 为了提升防火墙的防护能力,管理员需要定期对防火墙进行配置审查和更新。这包括检查防火墙规则的有效性、调整访问控制策略以适应新的业务需求,以及及时更新防火墙的软件和硬件。管理员还应密切关注网络安全领域的最新动态,及时将新的安全威胁纳入防火墙的防护范围。通过这些措施的实施,可以确保防火墙始终保持在最佳的工作状态,为计算机网络提供坚实的安全保障。

3.4 加强网络环境管理

(1) 黑客活动的猖獗一直是计算机网络安全问题难以彻底解决的关键因素。鉴于此,相关网络安全管理人

员必须加大对网络环境的治理力度,并着力提升对黑客攻击的防范能力。在计算机系统内部安装先进的保密程序,是有效防止黑客入侵、减少潜在损失的重要措施。这不仅要求技术层面的不断革新,还需管理人员具备高度的安全意识和责任感。(2) 计算机用户在设置个人账号和密码时,也应采取更为谨慎的态度。选择复杂度高、关联性不强的信息作为密码,可以大大增加黑客破解的难度,从而降低账号被盗用的风险。黑客在发动攻击前往往会先确定目标用户的IP地址。用户在网络活动中隐藏自己的IP地址,成为了一种有效的自我保护手段,可以有效避免黑客的追踪和恶意入侵。(3) 为了构建更加安全的计算机网络环境,网络安全管理部门还需制定和完善相关管理制度与法规。对于黑客违法入侵他人计算机的行为,必须依法严惩,绝不姑息。通过严厉的法律制裁,以“重典”震慑潜在的不法分子,形成强大的法律威慑力。这不仅能够维护计算机用户的合法权益,还能为整个计算机网络提供一个更加安全、稳定的运行和使用环境,推动网络空间的健康有序发展^[4]。

结语

综上所述,计算机网络安全防范是一个复杂而系统的工程,需要综合考虑技术、用户行为及系统等多个方面。通过提升用户安全防范意识、加强隐私加密设置、完善防火墙功能以及强化网络环境管理,可以有效降低网络安全风险。未来,随着技术的不断进步和威胁的不断演变,我们还需要持续关注和更新网络安全防范措施,确保信息系统在复杂多变的环境中稳定运行。

参考文献

- [1]袁康乐.计算机网络安全防范措施探析[J].信息记录材料,2021,22(11):59-60.
- [2]黄婉夏.计算机网络安全防范措施[J].中国宽带,2021(5):22.
- [3]周雷干.计算机网络安全问题及其防范措施[J].网络安全技术与应用,2021(05):162-164.
- [4]陈思思,潘娟,李凯航,等.计算机网络安全防范措施研究[J].电子技术与软件工程,2021(10):247-248.