Research on the Threat and Prevention Strategy of Computer Network Security

Shaoze Jiang

Quanzhou Nan'an City Public Security Bureau, Quanzhou, Fujian, 362000, China

Abstract

Computer network security is an important part of the development of information technology, which directly affects the security of data and the stability of the network. With the rapid progress of the Internet, the threat to network security has become more and more serious, forcing us to take strong protective measures to deal with it. This paper discusses the necessity of computer network security, common threats and challenges, and specific preventive measures to improve network security, focusing on the central role of computer network security in protecting user information, ensuring the stability of network services, and supporting economic and social development. Combined with the current situation, it analyzes the main threats, which not only endanger personal data, but also may damage the smooth operation of the entire network system. The paper further proposes practical preventive strategies, hoping to enhance the level of network protection through systematic programs. Thus ensuring the security of the network environment, the implementation of these protective strategies is expected to effectively reduce security threats and prevent illegal infringement of network data.

Keywords

computer; network security; threat; strategy

计算机网络安全的威胁与防范策略研究

江少泽

泉州南安市公安局, 中国·福建 泉州 362000

摘要

计算机网络安全是信息技术发展的重要一环,直接影响到数据的安全和网络的稳定性,随着互联网的快速进步,网络安全受到的威胁愈加严峻,迫使我们必须采取有力的防护措施应对,论文深入讨论了计算机网络安全的必要性,常见威胁与挑战,以及提升网络安全的具体防范措施,重点说明了计算机网络安全在保护用户信息、保障网络服务稳定性以及支持经济社会发展方面的核心作用,结合现状分析了主要威胁,这些威胁不仅危及个人数据,还可能破坏整个网络系统的平稳运行,进一步提出了实用的防范策略,希望通过系统化方案提升网络防护水平,从而保障网络环境的安全,通过这些防护策略的落实,有望有效减少安全威胁,防止网络数据遭受非法侵害。

关键词

计算机; 网络安全; 威胁; 策略

1 引言

数字化时代下,计算机网络逐步渗透到社会生活的各个方面,个人信息的存储和国家重要基础设施的运转都依赖于网络技术,网络安全也因此直接影响着社会的稳定与发展,计算机网络环境日益复杂,安全威胁不断演变,深入研究并实施有效的防范策略已经变得格外关键,论文详细分析了计算机网络所面临的各种安全挑战,并提出了系统性的解决方案,旨在增强网络的防御能力和应对突发事件的处理能力。

【作者简介】江少泽(1989-),男,中国福建泉州人,硕士,助理工程师,从事计算机网络安全研究。

2 维护计算机网络安全的必要性

2.1 保护敏感数据

计算机网络安全对保护敏感数据至关重要,当前信息化时代下,个人信息、商业机密、金融记录和政府数据等大量数据在计算机网络中存储和传输,这些数据因其敏感性和高价值,吸引了黑客和网络犯罪分子的注意,而一旦这些数据被未经授权访问或泄露,便可能引发隐私侵犯、经济损失和信誉危机。网络安全措施包括防火墙、加密技术、访问控制以及实时的安全监控,这些手段组成了一个防御系统,专门用于防范非法入侵和数据泄露,且随着技术发展和新型攻击方式的不断涌现,网络安全工具也在更新,以应对新的威胁与挑战^[1]。比如数据加密技术能确保即使数据传输中被截获,没有对应的解密密钥也无法获取内容。网络安全不仅是

技术层面的问题，还牵涉法律与道德层面，组织有责任保护用户和客户的数据免遭滥用或非法获取，因此，落实网络安全措施不仅可以防范外部威胁保护敏感数据，同时也增强用户信任，维护企业品牌声誉和市场地位。

2.2 防止网络攻击

维护计算机网络安全至关重要，能够有效防止网络攻击带来的潜在破坏，这些攻击往往以病毒、木马和勒索软件等形式存在，每一种形式都通过不同方式对网络系统造成威胁，病毒可以借助电子邮件附件传播感染系统文件，直接干扰系统的核心功能，木马会伪装成合法软件，一旦用户下载便可能窃取用户不知情的敏感信息，勒索软件则直接锁定系统中的重要数据，以要求支付赎金作为解锁条件，因此，通过强化网络安全措施来保障系统安全尤为重要。例如，对系统进行定期更新并执行补丁管理以修补漏洞，能够显著降低攻击风险，此外，部署高效的防病毒软件和入侵检测系统有助于在攻击初期将其遏制，确保网络不受损害，员工的网络安全教育和培训也十分关键，能大幅增强员工的安全意识并降低因人因素引发的安全事件。

2.3 维持业务连续性

维护计算机网络安全直接关系到业务的连续性和服务的稳定性，尤其是在数字化高度依赖的今天，各类企业和组织的日常运营越来越离不开计算机网络，面对 DDoS 攻击、恶意软件或数据泄露等网络风险，关键业务系统极易受到冲击，从而导致服务中断甚至瘫痪，像一次成功的攻击足以关闭在线交易、切断供应链或使客户服务系统停摆，建立稳固的网络安全体系可以成为应对这一类风险的基础^[2]。通过采用先进的安全技术和协议、定期更新系统、修补漏洞、实施全面的入侵检测和防御体系对潜在威胁进行实时监控和响应，同时制定有效的灾难恢复计划也至关重要，有了这一体系，企业在面对数据丢失或系统故障时才能迅速恢复业务运行，从而降低因网络攻击带来的经济损失，并维持客户信任和企业信誉，以此为企业的持续发展与稳定奠定基础，维护计算机网络安全也因此成为所有依赖现代技术的企业必须执行的核心策略。

3 计算机网络安全中常见的威胁挑战分析

3.1 恶意软件攻击

计算机网络安全的维护是防止数据泄露、保护用户隐私和确保设备正常运行的关键工作，而在这过程中，恶意软件攻击已成为普遍而棘手的威胁。恶意软件攻击形式多样，主要包括病毒、蠕虫、特洛伊木马和勒索软件，它们通过不同手段侵入用户设备，带来一系列破坏。病毒一般依附在宿主文件中，通过自我复制扩散来损坏系统，蠕虫则无需宿主文件即可自我传播至其他计算机，且不需要用户参与；特洛伊木马常伪装成合法程序，欺骗用户下载并运行，一旦执行，它便会为攻击者打开远程访问的后门，进而实现对设备的控

制或数据窃取。勒索软件通过加密用户重要文件后索要赎金来获取经济利益。恶意软件的传播方式广泛，常见路径包括电子邮件附件、软件下载以及操作系统和应用漏洞的利用，尤其是钓鱼邮件中的恶意附件会诱使用户点击，导致恶意程序安装在设备上开始破坏；下载不安全来源的应用程序也让用户更容易受到恶意代码的威胁。此外，未修补的系统和应用漏洞为攻击者提供了便利，让他们借机植入恶意软件，从而破坏设备或窃取登录信息、金融数据等敏感信息。

3.2 网络钓鱼攻击

计算机网络安全维护非常重要，其中常见威胁挑战包括网络钓鱼攻击。网络钓鱼攻击作为一种具有破坏力的安全威胁，通常运用社会工程学技巧欺骗用户，攻击者常假扮可信的个人或机构，通过发送电子邮件、短信或社交媒体消息，诱使用户执行特定操作，这些信息往往伪装成银行、社交平台、电子支付服务等合法来源，容易让用户产生信任，从而按照指示点击链接或打开附件。钓鱼邮件或消息的内容通常带有紧急或诱导性的语言，目的是促使用户快速响应，而其中的链接通常指向外观上高度仿真的恶意网站，意图诱导用户输入用户名、密码、信用卡信息等敏感数据。用户在这些虚假网站上输入的信息，往往会被攻击者截获，用于非法访问、身份盗窃或其他欺诈活动^[3]。网络钓鱼的成功率高，一方面由于攻击者设计手法精细，策略持续变化以应对最新的安全防护，另一方面由于用户在不同平台上往往使用相似或相同的账号信息，这意味着一旦一个账户遭到入侵，其他账户也可能面临风险。

3.3 分布式拒绝服务攻击

计算机网络安全中，分布式拒绝服务（DDoS）攻击是一种常见且严重的威胁，这类攻击意在使目标的网络服务或资源过载到无法正常使用的程度。攻击者通过控制大量被恶意软件感染的计算机组成的僵尸网络，同时向目标发送海量请求或数据包，使目标服务器或网络超出其负载。DDoS 攻击通常有多种形式，比如通过大量合法请求消耗服务器资源的 HTTP 洪水攻击，即以大量 HTTP 请求耗尽网站服务能力，或者通过发送大量 UDP 数据包使网络带宽被填满的 UDP 洪水攻击，阻断合法流量。DDoS 攻击影响力大且成本低，不仅迅速瘫痪网络服务，且其技术门槛不高，攻击者甚至能直接租用僵尸网络发动攻击而无需自行搭建复杂设施。此类攻击通过协调产生压倒性请求流来突破网络服务的处理极限，且因来源分散，单一安全措施难以有效拦截，对依赖网络服务的组织而言，DDoS 攻击始终是重大安全威胁。

4 促进计算机网络安全防范策略分析

4.1 安全教育与培训

计算机网络安全多种防范策略中，安全教育与培训是一个至关重要的基础环节，其核心在于通过定期的培训和教育课程让员工深刻意识到网络安全的潜在威胁，同时掌握

识别网络钓鱼等常见网络攻击的方法,尤其网络钓鱼针对的是组织中易受攻击的人员,通过培训课程向员工详细讲解如何辨别可疑的电子邮件、链接和附件等常见钓鱼手段,同时该教育培训还应涵盖安全的互联网使用习惯,如设定安全密码并定期更换、避免在不安全网络中执行敏感操作等,此外,员工需学习数据保护的实际操作,如在传输重要文件前加密文件,以及使用安全的数据传输与存储解决方案^[4]。类培训不仅局限于新员工的入职学习,而是一个持续的过程,因为网络安全威胁不断演变,只有通过不断更新培训内容,才能确保员工的安全知识始终处于最新状态,通过模拟攻击演练、安全意识活动、网络安全研讨会和定期安全通信等形式,可以使员工保持高度警觉,并有效应对新兴的网络安全挑战。这种系统化的教育方式不仅强化了员工个人的安全意识,还为整个组织筑起一道稳固的防线,极大降低了由于疏忽导致的安全风险。

4.2 使用防火墙和入侵检测系统

计算机网络安全防范措施中,部署防火墙和入侵检测系统(IDS)是关键手段,防火墙作为保护网络的第一道防线,负责监控和管理进出网络的数据流,依靠预设的规则来阻止未经授权的访问并防范潜在攻击,这些规则通常基于源地址、目标地址、传输协议或端口号,使防火墙在筛选入站和出站流量时更具针对性。与此同时,入侵检测系统专注于监测网络内部活动和数据传输,能够识别和响应内部的异常行为和威胁,IDS通过分析网络数据包,与已知攻击模式进行比对已发现恶意活动,一旦检测到可疑行为便发出警报,并可能根据配置自动采取措施防止进一步的损害和数据泄露,现代网络环境通常结合防火墙、IDS以及入侵预防系统(IPS),后者在识别威胁的同时能够主动阻止攻击,通过这种集成的安全系统,组织得以全面掌控网络安全,实时防护来自各方的潜在威胁。

4.3 数据加密

计算机网络安全中的数据加密技术通过算法将信息转化为特定格式,仅拥有正确密钥的人可以读取,成为提升网络安全的重要方式。个人身份信息、财务记录及公司内部数据等敏感信息,在服务器存储或网络传输时都应进行加密,这样即使数据被截获或非法访问,没有解密密钥的第三方也无法读取真实内容。加密技术包含对称加密和非对称加密两种方式,其中对称加密使用相同密钥来加解密数据,适合大量数据加密,速度较快,而非对称加密则采用公钥加密、私钥解密,尽管处理速度较慢但能提供更高的安全性,适合传

输过程中的密钥加密和少量数据加密。此外,现代加密技术还包含数字签名和数字证书等手段,数字签名用于确保数据完整性和发送方身份,数字证书则用于验证公钥真实性,通过这些方式有效提升数据传输的安全性和数据来源的可信性,从多方面保障了网络中传输和存储的数据免受未经授权访问和篡改。

4.4 应用程序和系统的及时更新

应用程序和操作系统的及时更新是维护网络安全的关键,软件开发商会持续发布新版本以修复发现的安全漏洞,如果企业或个人没有及时应用这些更新,他们的系统就会持续暴露在这些已知漏洞下,给攻击者带来攻击机会,除了操作系统本身,所有安装的应用程序和依赖库也都需要保持最新状态,更新过程自动化则能有效减少人为忽视或延迟的风险,很多系统和应用程序都带有自动检测和安装更新的功能^[5]。大幅简化了管理流程,对于大型企业,集中管理更新效果更显著,专门工具如补丁管理系统能够更高效地保障整体网络的安全,零信任架构的应用则能进一步增加保护,即便部分系统未及时更新,也可以限制威胁的扩散,在更新前进行测试也非常重要,可以确保这些更新不会影响现有系统的兼容性,避免更新可能引发的功能问题或新的安全隐患。因此企业在推送更新至生产环境之前,会在测试环境中进行充分的测试。

5 结语

计算机网络安全涉及技术、防护管理、法律规范和安全教育等多领域问题,网络安全威胁正日益复杂,仅凭一方努力难以应对,需要多方共同作用,通过技术防护升级、法律法规健全、公众安全意识提升和国际合作等手段,共同构建全面的网络安全防御体系,网络技术在未来将持续发展并深入应用,网络安全的挑战也将不断多元化,这要求在安全策略上不断创新调整,以适应不断变化的安全需求。

参考文献

- [1] 彭珺,高琨.计算机网络信息安全及防护策略研究[J].计算机与数字工程,2011,39(1):1672-9722.
- [2] 彭南兵.计算机网络信息安全及防护策略研究[J].电子技术与软件工程,2013(22):64.
- [3] 刘华清.计算机网络信息安全及防护策略研究[J].信息与电脑,2017(21):2.
- [4] 刘宗敏.浅析计算机网络应用安全问题与策略研究[J].商情,2011(5).
- [5] 吴丙午.大数据背景下计算机网络安全防范策略研究[J].新潮电子,2023(5):1-3.