计算机网络安全管理与维护

李 可 陈 鹏 郭珂琦 唐懋钧 王 力
北京计算机技术及应用研究所 北京 100854

摘 要：在当今信息化时代，计算机网络安全如同稳固的基石，守护着数据的海洋不被侵犯。本文深入剖析了网络安全的重要性，揭示了当前网络威胁的错综复杂性，并针对性地提出了一系列高效的安全管理与维护策略。通过本文的探讨，旨在为企业筑起一道坚不可摧的网络安全屏障，同时也为个人用户提供切实可行的防范指南，确保网络数据的完整性、机密性和可用性得到坚实保障。

关键词：计算机；网络安全；管理；维护

引言

在数字化时代的今天，计算机网络如同神奇的结晶般将我们的世界紧密地编织在一起，推动着社会生活的每一个细胞进行变革与创新。但在这光芒背后，网络世界的阴影也悄然滋生。安全威胁，如同潜伏在暗处的猎手，时刻窥视着每一个漏洞，企图给企业和个人的信息安全带来致命的打击。正是在这样的背景下，加强计算机网络安全管理与维护显得尤为重要。本文旨在深入探讨这一关键议题，为我们的网络环境筑起一道坚固的屏障，为构建一个更加安全、稳定的数字世界贡献我们的力量与智慧。

1 计算机网络安全概述

计算机网络安全是一个多层次、多维度的概念，它不仅仅关注单一的技术层面，更是一个融合了技术、管理和法律的综合性领域。从广义上讲，计算机网络安全是指利用网络技术和各种管理措施，确保网络系统中的硬件、软件以及存储、传输的数据资源不受未经授权的访问、破坏、篡改或泄露的威胁。这种保护旨在维持网络系统的持续、稳定和正常运行，确保网络服务能够不间断地为用户提供。网络安全涉及的层面极为广泛，首先是物理安全，它关注网络设备所处的物理环境是否安全，例如服务器机房是否有防火、防水、防雷击等措施。其次是网络安全，这一层面主要关注网络传输过程中的数据安全和网络通信的可靠性，防止数据在传输过程中被截获或篡改。系统安全则聚焦于操作系统、数据库等基础设施的安全，确保这些系统不被恶意软件或黑客攻击所利用。应用安全则是指各种应用软件在运行过程中的安全性，包括防止应用被注入恶意代码、防止数据泄露等。最后是数据安全，它关注的是数据的保密性、完整性和可用性，确保数据在存储、处理、传输过程中不被非法访问或篡改。这些安全层面相互关联、相互影响，共同构成了一个复杂的网络安全体系。任何一个层面的漏洞都可能成为攻击者入侵的突破口，因此，在网络安全管理和维护中，需要综合考虑各个层面的安全需求，采取综合性的安全措施来确保整个网络系统的安全[1]。

2 网络安全威胁分析

当然，我们可以更深入地分析这些网络安全威胁的细节，以更好地理解它们如何运作以及为何它们如此危险。计算机病毒：计算机病毒是一种能够自我复制并在计算机网络中传播的恶意代码。它们通常隐藏在看似无害的文件或程序中，当用户打开这些文件或程序时，病毒就会被激活并开始感染用户的系统。一些病毒还会通过网络连接传播到其他计算机，形成大规模的感染。病毒的破坏性可以从简单的数据破坏到复杂的系统瘫痪，甚至有一些病毒被设计为专门破坏特定的硬件设备。黑客攻击：黑客攻击是一种利用系统漏洞、弱密码或社交工程等手段非法侵入计算机系统或网络的行为。黑客通常会使用各种工具和技术来探测目标系统的漏洞，并利用这些漏洞来获取系统的访问权限。一旦成功入侵，黑客就可以窃取敏感信息、篡改数据或破坏系统。黑客攻击的危害不仅限于直接的经济损失，还可能包括声誉损害、客户流失以及法律责任等。网络钓鱼：网络钓鱼是一种欺骗性的攻击手段，攻击者通常会发送看似来自正规机构（如银行、政府机构等）的电子邮件或消息，诱导用户点击恶意链接或下载恶意附件。这些链接或附件通常会要求用户提供个人信息（如用户名、密码等），或者安装恶意软件来窃取用户的敏感信息。网络钓鱼攻击的成功率之所以较高，是因为它们往往能够准确地模仿正规机构的外观和语气，使得用户很难分辨真伪。恶意软件（Malware）：恶意软件是一种被设计为在用户不知情或未经授权的情况下安装在计算机系统中的有害

程序。这些程序可以执行各种恶意行为，如窃取个人信息、破坏系统文件、干扰系统操作等。恶意软件的传播方式多种多样，包括通过恶意网站、感染的软件下载链接、垃圾邮件附件等。一旦恶意软件被安装到用户的计算机上，它们就可以隐藏起来并悄悄地执行恶意行为，使得用户很难察觉和清除。拒绝服务攻击（DoS/DDoS）：拒绝服务攻击是一种通过大量合法的或伪造的请求来耗尽目标系统资源的攻击方式[2]。这些请求可以是来自单个攻击源的（DoS攻击），也可以是来自多个攻击源的（DDoS攻击）。攻击者通常会利用大量的计算机或设备来同时发送请求，使得目标系统无法处理这些请求并导致服务中断。拒绝服务攻击的危害不仅限于目标系统本身，还可能影响到与该系统相关的其他系统和用户。例如，一个被攻击的网站可能会无法访问，导致用户无法获取重要的信息或服务。

3 网络安全管理与维护策略

3.1 建立完善的网络安全管理体系

建立完善的网络安全管理体系是企业保障网络安全的首要任务。这一体系应该是一个多层次的、综合性的安全框架，旨在确保网络系统的机密性、完整性和可用性。首先，企业需要制定明确的网络安全政策，这些政策应该基于企业的业务需求、风险评估和法律法规要求。政策内容应包括对网络访问的控制、数据保护的原则、安全事件的报告和响应流程等。通过制定这些政策，企业可以为员工提供一个清晰的行为指南，确保他们在日常工作中能够遵循安全规定。其次，明确安全管理职责是至关重要的。企业应设立专门的安全管理团队或指定专人负责网络安全工作。这些人员应具备专业的安全知识和技能，能够负责安全策略的制定、安全措施的实施以及安全事件的响应。此外，企业还应定期对安全管理人员进行培训，提升他们的专业技能和应对能力。实施安全审计和监控是保障网络安全的重要手段。企业应定期对网络系统进行安全审计，检查系统中是否存在漏洞、配置是否正确以及安全措施是否有效。同时，通过部署安全监控设备和软件，企业可以实时监控网络流量、异常行为和安全事件，及时发现并处置潜在的安全威胁。最后，建立应急响应机制是应对安全事件的关键。企业应制定详细的应急响应计划，明确在发生安全事件时的处置流程、责任人和沟通渠道。此外，企业还应定期进行应急演练，检验应急响应计划的有效性和员工的应对能力。通过建立这样的应急响应机制，企业可以在安全事件发生时迅速做出反应，最大程度地减少损失和影响。

3.2 强化网络安全技术防范

在网络安全管理与维护的策略中，强化网络安全技术防范占据着举足轻重的地位。随着网络攻击手段的不断演变和升级，单一的防护措施已难以满足现代网络安全的需求。因此，企业需要采用一系列先进的网络安全技术，构建多层次的安全防护体系[3]。首先，防火墙技术是网络安全的基础设施之一。通过在内外网之间建立一道安全的屏障，防火墙能够有效地过滤和控制进出网络的数据流，阻止未经授权的访问和恶意攻击。企业应根据自身的业务需求和安全风险，合理配置防火墙规则，确保其能够有效地发挥作用。其次，入侵检测系统（IDS）是实时监测网络流量的重要工具。通过对网络数据的深度分析和模式识别，IDS能够及时发现并报警针对网络的异常行为和潜在威胁。企业应将IDS与防火墙等其他安全设备相集成，形成联动的安全防御体系。此外，数据加密技术是保护数据机密性的关键手段。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，攻击者也无法轻易获取其中的内容。企业应采用国际标准的加密算法和密钥管理机制，确保数据加密的有效性和安全性。除了上述技术外，定期更新系统和软件补丁也是至关重要的。系统和软件中存在的漏洞是攻击者入侵的主要途径之一。因此，企业应定期关注厂商发布的安全公告和补丁信息，及时对系统和软件进行更新和修复，降低被攻击的风险。

3.3 提高网络安全意识与培训

在网络安全管理与维护的策略中，提高网络安全意识与培训是不可或缺的一环。随着网络技术的飞速发展和网络攻击的日益猖獗，单纯的技术防护已经不足以应对复杂的网络安全威胁。因此，加强网络安全宣传教育，提高员工和用户的网络安全意识，成为企业保障网络安全的重要手段。首先，企业需要定期开展网络安全宣传教育活动。通过张贴安全标语、发放安全手册、举办安全知识竞赛等形式，向员工普及网络安全基础知识，让他们了解常见的网络攻击手段和防范措施。同时，企业还可以利用内部网站、电子邮件等渠道，定期向员工推送网络安全动态和预警信息，提醒他们时刻保持警惕。其次，网络安全培训是提升员工安全防范技能和应急处理能力的有效途径。企业应定期组织员工参加网络安全培训课程，学习如何识别和应对网络威胁、如何配置和使用安全设备、如何处置安全事件等实用技能。培训过程中，可以采用案例分析、模拟演练等教学方法，让员工在实际操作中掌握技能，提高培训效果。此外，企业还应建立网络安全意识培养的长效机制。通

过制定网络安全行为规范、将网络安全纳入员工绩效考核体系等措施，引导员工养成良好的安全习惯。同时，鼓励员工积极参与网络安全管理和维护工作，发现潜在的安全隐患并及时报告，共同维护企业的网络安全。

3.4 实施访问控制和身份认证

在网络安全管理与维护的策略体系中，实施访问控制和身份认证是确保网络资源安全的关键措施。随着企业数字化转型的加速和远程办公的普及，网络资源和数据的访问需求愈发复杂，未经授权的访问和数据泄露风险也随之增加。因此，建立严格的访问控制和身份认证机制至关重要。访问控制是网络安全的第一道防线，它通过对网络资源和数据设置访问权限，确保只有经过授权的用户才能访问特定的网络资源。企业应建立完善的访问控制策略，明确不同用户角色和权限的划分，并严格限制对敏感数据和关键系统的访问[4]。同时，实施最小权限原则，即仅授予用户完成任务所需的最小权限，减少潜在的安全风险。身份认证是访问控制的前提和基础，它通过验证用户的身份和权限，确保只有合法用户才能访问网络资源。企业应采用多种身份认证技术，如用户名密码、动态口令、数字证书等，提高身份认证的安全性和可靠性。同时，实施多因素身份认证，结合生物特征、手机短信等多种认证因素，进一步增强身份认证的安全性。在实施访问控制和身份认证的过程中，企业还应注意保护用户的隐私和数据安全。应采取加密技术对敏感数据进行加密存储和传输，确保数据在传输和存储过程中不被泄露和篡改。同时，建立完善的审计和监控机制，对用户的访问行为进行实时监控和记录，及时发现和处置异常访问行为。

3.5 定期进行网络安全评估和演练

在网络安全管理与维护的全方位策略中，定期进行网络安全评估和演练占据了重要的地位。随着网络技术的不断发展和网络攻击手段的持续演变，企业面临的网络安全威胁也日益严峻。为了确保网络系统的持续安全稳定运行，企业必须定期对自身的网络安全状况进行深入的评估，并通过演练来检验安全管理和应急响应措施的有效性。网络安全评估是对企业网络系统的安全性进行全面检查的过程。通过定期的评估，企业能够及时发现网络系统中存在的潜在安全隐患，如系统配置不当、漏洞未修复、恶意软件感染等。评估过程中，企业应借助专业的安全评估工具和团队，对网络系统的各个方面进行深入的分析和检测，确保不留下任何安全死角。一旦发现安全隐患，企业应立即采取整改措施，及时消除安全风险。网络安全演练则是对企业安全管理和应急响应措施的一次实战检验。通过组织定期的演练，企业可以模拟真实的网络攻击场景，检验自身的安全防护和应急响应能力。演练过程中，企业应注重实战化、场景化，确保演练的真实性和有效性。同时，企业还应邀请专业的安全团队参与演练，提供指导和建议，帮助企业不断完善安全管理和应急响应机制。

结语

立足于信息化时代的高峰，计算机网络安全管理与维护的重要性愈发凸显，它如同一座坚不可摧的堡垒，时刻守护着珍贵的数据海洋和信息脉络。这一任务的艰巨性不言而喻，唯有企业、政府和个人三方齐心协力，共同构筑起坚固的防线，方能应对日益严峻的挑战。通过不断完善管理体系、运用先进的安全技术、培养深入骨髓的安全意识，我们必将打造一道无懈可击的网络安全屏障，为数字时代的繁荣与发展提供坚实保障。

参考文献

[1]唐高阳.计算机网络安全管理与维护[J].数字通信世界,2023(8):194-196.

[2]许开杰,赵彦敏,朱实强.计算机网络安全隐患管理及维护探讨[J].网络安全技术与应用,2018,11(4):223-224.

[3]王子标.浅谈计算机网络技术与安全管理维护[J].广东蚕业,2018,29(7):127-128.

[4]朱庆荣.对计算机网络安全管理工作的维护措施研究[J].网络安全技术与应用,2019,33(5):211-212.