

计算机网络安全管理与维护策略探讨

王嘉

绥化市公安局科技信息支队，黑龙江绥化，152061；

摘要：计算机网络技术已经遍布人们日常生活的方方面面，尤其是计算机网络技术凭借其高效快捷的优点，已成为人们日常工作必不可少的辅助工具，但计算机网络安全的挑战也随之而来。因此，探讨计算机网络安全管理与维护策略具有重要的现实意义。基于此，本文根据常见的计算机网络安全管理与维护问题，浅析加强计算机网络管理中的安全管理及维护工作的相应策略，切实做好相关网络维护，确保日常工作的顺利进行。

关键词：计算机；网络安全；管理与维护

Discussion on computer network security management and maintenance strategy

Zhang San, Li Si, Wang Wu

School of Electronic Information Engineering Chengdu University, Sichuan Chengdu, 610106;

Abstract: Computer network technology has been all over the aspects of People's Daily life, especially computer network technology with its efficient and fast advantages, has become an indispensable auxiliary tool for People's Daily work, but the challenge of computer network security also comes. Therefore, it is of great practical significance to discuss the security management and maintenance strategy of computer network. Based on this, according to the common computer network security management and maintenance problems, this paper analyzes the corresponding strategies to strengthen the security management and maintenance of computer network management, and effectively do the relevant network maintenance to ensure the smooth progress of daily work.

Keywords: computer; network security; management and maintenance

DOI: 10.69979/3041-0673.24.6.011

随着社会经济的迅猛发展和高新技术的日新月异，计算机已成为日常办公的重要工具。在日常工作中，无论哪个单位，其计算机网络都是高频使用，以处理繁杂的工作内容，这需要由专业技术人员进行安全管理和及时维护，确保计算机网络畅通，以满足日常工作的实际需要。所以，单位和专业技术人员只有认真对待安全管理工作，定期对计算机网络进行维护，做好日常检查工作，及时处理发现的安全威胁问题，才能给工作人员提供一个绿色、健康、安全的网络使用环境，让网络、信息系统在安全稳定运行的基础上，更好发挥计算机网络带来的价值。

1 强化网络权限管理与控制

网络权限管理与控制是计算机网络安全管理中的重要环节。科学合理进行网络权限管理与控制，可以有效降低非授权访问和恶意攻击的网络安全风险，保护单位的资料信息安全。因此，在网络权限管理与控制方面，首先需要制定明确的权限管理策略。通过对不同用户和角色的权限进行分类和划分，可以确保每个用户在网络

系统中只能获得其所需的权限，从而避免了因非授权访问导致的信息泄露和系统崩溃风险。其次，权限管理策略还需要考虑到单位不同部门之间的权限划分，确保各个部门之间的权限不会互相冲突，同时又能够保证信息的流通和共享。为了实施有效的网络权限管理与控制，还需要采用适当的技术手段。一种常见的做法是通过访问控制列表（ACL）来限制网络访问。ACL 可以基于用户或 IP 地址来设定访问规则，只有符合相应规则的用户才能够访问系统资源。此外，还可以运用身份认证和授权技术，确保用户身份的真实性和授权合法性。另外，网络权限管理与控制还需要与网络安全策略相结合。网络安全策略的制定应该包括了对网络权限的管理要求，明确规定了不同用户在网络中所能够进行的操作和访问范围。同时，网络权限管理与控制也需要与事业单位的安全培训和教育相结合，加强对用户的权限管理意识和操作规范的培养，提高员工对于网络权限管理的重视程度。

2 优化网络设备安全维护

网络设备包括路由器、交换机、防火墙等，其正常运行对计算机网络安全至关重要。在网络设备安全维护过程中，需要采取一系列措施以保护和维护网络设备的安全。首先，需要安排专业技术人员定期检查和更新网络设备的操作系统和固件。操作系统和固件的更新可以修复已知的漏洞和弱点，以提高设备的安全性。此外，更新操作系统和固件还可以增加新功能和改进性能，从而为事业单位提供更好的网络体验。其次，网络设备应放置在安全可控的房间或机柜中，只有授权人员才能访问。并定期对设备进行巡检，以确保设备正常运行并检查是否有异常或可疑活动。同时，还应配置和管理网络设备的访问控制表（ACL）。ACL 可以限制访问网络设备的人员和流量，从而减少网络设备被恶意攻击或未经授权的访问的风险。另外，单位还应定期备份网络设备的配置文件和日志文件。配置文件包含了网络设备的各项设置和配置信息，而日志文件则记录了网络设备的运行状况和事件信息。通过备份配置文件和日志文件，技术人员可以在出现故障或安全事件时快速恢复网络设备，并对事件进行追踪和分析。除此之外，在网络设备安全维护过程中，单位还应加强员工的安全意识和培训。组织员工接受相关的网络安全培训，了解和掌握网络设备的基本安全知识，以避免安全漏洞和攻击。

3 设置数据备份与恢复机制

随着信息技术的快速发展和计算机网络的广泛应用，计算机网络安全越来越受到重视。数据备份与恢复机制更是保障计算机网络安全的关键所在。数据是一个单位的重要资产和经营信息，一旦丢失或受损，将会带来巨大的损失和风险。因此，建立有效的数据备份与恢复策略可以有效地应对各种数据丢失、损坏或被破坏的风险，确保数据的完整性和可恢复性。常见的数据备份方法包括完全备份、增量备份和差异备份。完全备份是指将所有数据都备份，无论是否发生变化。增量备份只备份自上次完全备份以来发生变化的数据。差异备份是指备份自上次完全备份以来的所有变化数据。单位可以根据数据的重要性和频繁变化程度选择合适的备份方法。此外，还可以使用磁带备份、硬盘备份、云备份等

多种备份技术，以确保数据备份的安全可靠。与此同时，在数据备份的过程中，还应注意数据备份的频率和存储位置。备份频率应根据数据的实时性和重要性进行合理设置，可以是每天、每周或每月进行备份。备份的存储位置应选择在安全可靠的地方，最好是物理上与主服务器分离的地方，以防止备份数据与主服务器同时受到破坏。

除了备份策略，数据恢复策略也同样重要。当数据发生丢失或受损时，单位技术人员应能够及时恢复丢失或损坏的数据。为实现快速恢复，可以采用增量备份与完全备份相结合的方式，将增量备份的数据应用到最近的完全备份上，以减少数据恢复的时间和成本。此外，还可以使用虚拟化技术和冗余存储技术来提高数据恢复的效率和速度。在数据备份与恢复的过程中，要制定相应的操作规范和流程，明确责任人和操作步骤，保证备份和恢复的顺利进行。同时，还应定期进行备份策略和数据恢复的测试，发现问题并及时解决，以提高备份与恢复策略的可靠性和有效性。

4 结语

综上所述，想要实现计算机网络安全管理需要全面系统地考虑网络安全的各个方面，包括但不限于强化网络权限管理与控制、优化网络设备安全维护、设置数据备份与恢复机制等。只有通过科学合理的安全管理措施和策略，计算机网络设备与系统才能有效应对各种网络安全威胁，同时也能够减轻技术人员的工作压力，从而实现计算机网络安全管理与维护工作质量以及效率的提升。

参考文献

- [1]解春升. 计算机网络安全技术在网络安全维护中的防范研究[J]. 网络安全技术与应用, 2022(8): 162-164.
 - [2]丁雪非, 罗尉平. 计算机网络设备维护与安全管理的措施探讨[J]. 数码世界, 2021(01): 282-283.
- 作者简介：（王嘉，1980年06-06，男，汉族，黑龙江绥化，绥化市公安局，本科，一级技术主管，通讯技术，）