网络运维管理常见安全问题及防范对策

杜 鹃
航宇救生装备有限公司 湖北 襄阳 441003

摘 要：网络运维管理面临多种常见安全问题，包括配置错误与未及时更新、恶意软件入侵、数据泄露等。为确保网络安全，需采取一系列防范对策。建立标准化的配置管理流程，及时更新软件和补丁，防止配置错误和漏洞被利用。加强恶意软件防护，部署防病毒软件和端点保护解决方案，提高系统的抗攻击能力。强化密码与身份认证管理，确保用户访问的合法性。通过综合施策，能有效提升网络运维管理的安全性。

关键词：网络运维管理；安全问题；防范对策

1 网络安全的基本概念

网络安全的基本概念涉及保护网络系统中的数据、设备和通信过程，确保信息的机密性、完整性和可用性。它涵盖了多个层面，包括技术、管理和法律等方面，旨在防止未经授权的访问、使用、泄露、破坏、修改或中断。在技术层面上，网络安全通过一系列安全措施来实现，这些措施包括但不限于：防火墙：作为网络的第一道防线，防火墙用于监控和控制进出网络的流量，防止未经授权的访问。入侵检测系统（IDS）和入侵防御系统（IPS）：IDS能够检测潜在的网络攻击，而IPS则能够主动阻止这些攻击。加密技术：通过对数据进行加密，确保在传输或存储过程中数据不被窃取或篡改。安全认证和授权：通过身份验证和访问控制机制，确保只有授权的用户才能访问网络资源。恶意软件防护：通过防病毒软件、反间谍软件等工具来防止恶意软件的感染和传播。安全审计和日志记录：记录和分析网络活动，以便在发生安全事件时能够迅速响应和恢复。在管理层面上，网络安全需要建立完善的安全政策和流程，包括：安全培训：提高员工对网络安全的认识和意识，培养正确的安全习惯。安全策略制定：制定明确的安全策略，规范网络使用行为和安全操作。风险评估：定期评估网络系统的安全风险，识别潜在的安全威胁和漏洞。应急响应计划：制定详细的应急响应计划，以应对各种网络安全事件。在法律层面上，网络安全需要遵守相关的法律法规和标准，如《网络安全法》、《个人信息保护法》等，确保网络活动的合法性和合规性。

2 网络运维管理中的常见安全问题分析

2.1 网络拓扑暴露问题

网络运维管理中的常见安全问题中，网络拓扑暴露问题是一个重要的安全隐患。网络拓扑是指网络中各个设备之间的连接关系和通信路径的示意图。当网络拓扑被不当地暴露或泄露时，可能会带来一系列的安全风险。网络拓扑的暴露可能导致潜在的攻击者了解网络的结构和布局，从而更容易地找到网络的脆弱点和潜在的安全漏洞。攻击者可以利用这些信息来制定针对性的攻击策略，比如通过识别关键设备和通信路径来实施定向攻击或拒绝服务攻击（DDoS）[1]。网络拓扑的暴露还可能导致敏感信息的泄露，网络拓扑中可能包含有关网络设备的型号、配置、IP地址等敏感信息，这些信息如果被恶意利用，可能会被用于进一步的网络渗透或数据窃取。网络拓扑的暴露还可能对网络的稳定性和可用性造成影响，攻击者可能会利用对网络拓扑的了解，发起分布式拒绝服务攻击（DDoS）或其他形式的网络攻击，导致网络拥堵、设备过载或服务中断，从而严重影响网络的正常运行。

2.2 弱密码与身份认证风险

网络运维管理中的常见安全问题之一便是弱密码与身份认证风险。这些风险对于整个网络系统的安全构成严重威胁，因为它们直接关联到用户身份验证和访问控制机制的有效性。弱密码是指那些容易被猜测或破解的密码，如简单的数字组合、常见的单词或短语等。当使用弱密码时，恶意用户或攻击者可能通过暴力破解、字典攻击等手段快速获取用户账号的访问权限，进而对网络系统进行非法访问和操作。身份认证风险则涉及用户身份验证机制的不足或漏洞，如果身份认证机制设计不当或存在安全漏洞，攻击者可能通过伪造身份、窃取凭据等手段绕过身份验证，获得对系统的非法访问权限。这种风险可能导致数据泄露、系统篡改或拒绝服务攻击等严重后果。

2.3 操作授权及审计漏洞

网络运维管理中的常见安全问题之一，即为操作授权及审计漏洞，这些漏洞对网络安全构成直接威胁。在

网络运维中，如果不遵循最小权限原则，给开发或业务账号授权过多的权限，如直接提供root权限或admin权限，这将大大增加安全风险。攻击者一旦获取这些高权限账号，就能对系统进行深度操作，可能导致数据泄露、系统篡改或瘫痪。当权限分配不清晰或未及时更新时，可能会出现用户拥有不必要权限的情况，这不仅可能导致资源浪费，还可能因为误操作而对系统造成损害。在复杂的网络环境中，如果缺乏有效的审计机制，就无法对用户的操作行为进行有效监控和记录。这将使得在发生安全事件时，无法追溯和定位问题源头，增加了解决问题的难度。审计日志是安全事件追溯的重要依据。如果审计日志不完整或记录不准确，就无法为安全事件的分析和应对提供有效支持。审计员或安全管理员应具有适当的权限来访问和审查审计日志。如果这些权限管理不当，可能会导致审计数据的泄露或被篡改，进而影响审计的准确性和有效性[2]。

2.4 配置错误与未及时更新

网络运维管理中的常见安全问题之一是配置错误与未及时更新。这些问题可能源于多种原因，包括但不限于人为疏忽、系统升级遗漏或管理流程的缺陷。配置错误通常指的是在网络设备、服务器或应用程序的设置中出现了不正确的参数或选项。这些错误可能导致系统性能下降、安全隐患增加或功能失效。例如，防火墙规则设置不当可能允许未授权的访问，而路由配置错误则可能导致网络中断或数据包丢失。未及时更新则指的是软件、操作系统、安全补丁或固件等未能在适当的时间内进行升级或替换。这种滞后可能使系统面临已知的安全漏洞和攻击威胁。攻击者经常利用未修补的漏洞来发动网络攻击，从而获取敏感数据、破坏系统或进行其他恶意活动。

2.5 恶意软件入侵与数据泄露

网络运维管理中的常见安全问题之一是恶意软件入侵与数据泄露，这些问题对组织的信息安全构成严重威胁。恶意软件入侵是一个普遍存在的风险，恶意软件，如病毒、蠕虫、木马等，通过不同的途径，如电子邮件附件、恶意链接、下载的软件包等，悄悄潜入系统内部。一旦感染，这些恶意软件便会在系统中潜伏，执行各种恶意操作，如窃取敏感信息、破坏系统文件、进行网络攻击等。恶意软件的存在不仅威胁到系统的稳定运行，更可能导致数据泄露，给组织带来严重的后果。数据泄露是网络运维中另一个不可忽视的安全问题，数据泄露可能源于多种原因，如内部员工的不当操作、系统漏洞被利用、恶意软件窃取等。一旦敏感数据被泄露，组织的商业机密、客户隐私等重要信息就可能被不法分子利用，导致经济损失、声誉损害等严重后果。恶意软件入侵和数据泄露往往相互关联，恶意软件的入侵往往是为了窃取敏感数据，而数据泄露又可能是恶意软件入侵的直接后果。

3 网络运维管理常见安全问题的防范对策

3.1 网络拓扑保护的防范对策

在网络运维管理中，保护网络拓扑的安全至关重要。网络拓扑的详细信息应该受到严格的保护，避免不必要的暴露。通过限制对拓扑图的访问权限，仅允许授权人员查看和访问，可以有效降低潜在的安全风险。在传输和存储网络拓扑数据时，应使用加密技术来保护数据的机密性和完整性。这可以防止未经授权的访问和恶意篡改。随着网络设备和连接的变化，网络拓扑也会发生变化。运维团队应定期审查和更新网络拓扑，确保拓扑图的准确性和完整性。通过部署网络隔离和分段技术，可以将网络划分为不同的安全区域，限制不同区域之间的通信。这可以降低潜在的安全风险，并减少攻击者对整个网络的威胁。使用网络监控和检测工具，可以实时监控网络流量和异常行为。一旦发现异常，可以立即采取应对措施，防止潜在的安全威胁扩散。

3.2 密码与身份认证管理的防范对策

密码和身份认证是网络安全的重要防线，强制实施强密码策略，要求用户设置复杂度高、难以猜测的密码，并定期更换密码。这可以有效降低密码被猜测或破解的风险。引入多因素身份认证，除了密码外，引入其他因素（如指纹、面部识别、动态令牌等）进行身份认证，可以提高身份认证的安全性。多因素身份认证能够增加攻击者获取访问权限的难度。定期审计和审查用户账号，定期审计和审查用户账号，确保每个账号都是必要且安全的[3]。及时关闭不必要的账号或禁用已离职员工的账号，防止未经授权的访问。使用安全的密码管理工具，使用专业的密码管理工具，帮助用户生成、存储和管理安全的密码。这可以减轻用户记忆密码的负担，并提高密码的安全性。教育和培训用户，加强用户的安全意识教育，提高用户对密码和身份认证重要性的认识。教育用户如何设置强密码、保护个人信息和避免常见的安全陷阱。

3.3 操作授权与审计的防范对策

操作授权和审计是确保网络运维安全的关键环节，遵循最小权限原则，仅授予用户完成其工作所需的最小权限。这可以减少因权限过大而导致的安全风险。定期审查和更新用户账号的权限设置，确保每个用户都拥有

适当的权限。及时删除不必要的权限或调整权限范围，防止权限滥用。通过部署访问控制策略，限制用户对网络资源的访问。使用防火墙、入侵检测系统等工具来监控和控制进出网络的流量，防止未经授权的访问。建立严格的审计机制，记录用户的操作行为和系统事件。通过审计日志，可以追溯和定位问题源头，及时发现和应对潜在的安全威胁。使用安全监控和检测工具，实时监控网络中的异常行为。一旦发现异常，立即触发警报并采取应对措施，防止潜在的安全威胁扩散。

3.4 配置管理与更新的防范对策

在网络运维管理中，配置管理与更新是确保系统安全性的重要环节。制定并遵循标准化的配置管理流程，确保网络设备和系统配置的一致性和准确性。这包括建立配置文档库、制定配置变更审批流程、实施配置备份和恢复策略等。采用自动化配置管理工具和技术，可以大大提高配置管理的效率和准确性。这些工具可以自动检测配置错误、自动推送配置更新、自动备份和恢复配置等，减少人为错误和遗漏。定期审查和更新网络设备和系统的配置，确保配置与业务需求和安全要求保持一致。这包括检查配置参数、安全策略、访问控制等，确保没有过时或错误的配置存在[4]。保持网络设备和系统软件的最新版本，及时安装安全补丁和更新。这可以修复已知的安全漏洞和缺陷，提高系统的安全性和稳定性。建立配置变更监控机制，实时监控网络设备和系统的配置变更情况。这可以及时发现未授权的配置更改、异常行为或潜在的安全风险，并采取相应的应对措施。

3.5 恶意软件防护的防范对策

恶意软件防护是网络运维中必不可少的一环。安装和更新防病毒软件，在网络设备和终端上安装防病毒软件，并定期更新病毒库。防病毒软件可以检测和清除已知的恶意软件，保护系统免受感染。部署端点保护解决方案，使用端点保护解决方案，对终端设备进行全面的安全防护。这些解决方案可以监控设备行为、阻止恶意软件运行、提供数据泄露防护等功能。教育和培训用户，加强用户的安全意识教育，提高用户对恶意软件的识别和防范能力。教育用户避免点击可疑链接、下载未知来源的文件、使用弱密码等不安全行为。定期扫描和检测恶意软件，使用专业的恶意软件扫描和检测工具，定期对整个网络进行扫描和检测。这可以及时发现和清除潜在的恶意软件，防止其扩散和造成损害。监控网络流量和异常行为，通过监控网络流量和异常行为，可以及时发现恶意软件的传播和攻击行为。一旦检测到异常，应立即采取措施进行隔离和清除，防止恶意软件对整个网络造成损害。配置管理与更新以及恶意软件防护是网络运维管理中不可或缺的安全措施。通过建立标准化的配置管理流程、自动化配置管理、及时更新软件和补丁、监控配置变更以及部署恶意软件防护解决方案等措施，可以有效提高网络系统的安全性和稳定性。

结束语

网络安全是组织发展的基石，网络运维管理作为保障网络安全的关键环节，必须高度重视安全问题。通过实施上述防范对策，能够有效降低安全风险，保护组织的数据资产和业务连续性。同时，也应持续关注新的安全威胁和挑战，不断完善网络运维管理体系，确保网络系统的长期稳定运行。让我们携手共进，共同守护网络安全。

参考文献

[1]李巨鸣.杨帆.徐世伟.网络运维管理常见安全问题及防范对策分析[J].中国新通信.2020.22(18):157-158. DOI:10.3969/j.issn.1673-4866.2020.18.081.

[2]张仁飞.李研.网络运维管理常见安全问题与防范对策[J].中国新通信.2019.(19).DOI:10.3969/j.issn.1673-4866.2019.19.147 .

[3]邹同浩.许学添.李俊磊.计算机网络管理及相关安全技术分析[J].网络安全技术与应用.2020.(4).DOI:10.3969/j.issn.1009-6833.2020.04.002 .

[4]吴珍珍.程渊源.何宇.网络运维管理常见安全问题及防范对策探讨[J].数字技术与应用.2018.(11).DOI:10.19695/j.cnki.cn12-1369.2018.11.93 .