计算机网络运维及安全管理设计优化策略

吕　坤
航宇救生装备有限公司　湖北　襄阳　441003

摘　要：计算机网络运维及安全管理设计优化策略是保障企业网络系统安全与稳定运行的重要举措。本文围绕安全风险评估与应对机制建立、安全技术与策略应用、安全意识教育与制度完善三方面展开讨论，提出全面的网络安全管理优化策略设计方案。通过合理利用安全评估工具、应用多层次安全技术、加强员工安全意识培训等措施，企业可有效提升网络安全管理水平，确保网络系统的安全性和可靠性。

关键词：计算机；网络运维；安全管理；优化策略

1 计算机网络运维与安全管理的重要性

计算机网络是现代信息社会的基础设施，其运维与安全管理对于保障网络的稳定运行、数据的安全传输、用户信息的保护至关重要。第一、计算机网络运维是确保网络系统稳定、高效运行的关键环节，网络运维人员负责监控网络设备状态、管理网络资源、维护网络设备和服务，及时排查和解决网络故障，以保障网络正常运行。缜密的网络运维管理可以有效避免网络故障对正常业务运行造成的影响，提高整个网络系统的稳定性和可用性。第二、网络安全管理是维护网络系统安全的核心任务，在网络运营过程中，网络安全始终是一项重要的议题。网络安全管理旨在保护网络系统免受黑客攻击、恶意软件、数据泄露等安全威胁。网络安全管理包括建立安全策略、加强边界防御、监测异常流量、及时处理安全事件等措施，以确保网络数据的机密性、完整性和可用性。网络安全管理不仅关乎个人隐私和财产安全，也关系到企业机密和国家安全，是网络运营中不可或缺的一环。计算机网络运维与安全管理的重要性不言而喻，通过加强网络运维管理，可以提高网络运行效率和可靠性，提供用户更好的网络服务体验；而加强网络安全管理，可以保护网络系统免受各种安全威胁，确保网络数据的安全传输和存储。只有在做好网络运维与安全管理的基础上，才能构建安全可靠、稳定高效的计算机网络系统，助力信息化时代的发展。

2 计算机网络运维及安全管理现状分析

2.1 网络拓扑结构与设备配置现状

当前，计算机网络运维及安全管理已成为各个企业以及组织的重中之重。就网络拓扑结构来说，许多企业采用了复杂多样的网络拓扑，例如分层式、星型、总部-分支等结构，以满足不同应用场景和需求[1]。在设备配置方面，企业常常部署众多网络设备，如路由器、交换机、防火墙等，以构建稳定高效的网络环境。然而，由于网络规模不断扩大、设备类型繁多，网络运维和安全管理面临着日益复杂的挑战。在网络运维方面，许多企业面临着设备管理繁琐、故障排查困难、性能监控不足等问题。运维人员需要花费大量精力在设备配置、日常巡检和故障排查上，导致工作效率低下和运维成本增加。随着网络应用的不断发展，用户对网络服务的需求也变得越来越高，要求网络运维更加及时、高效、灵活。而在网络安全管理方面，随着网络攻击手段的不断升级和演变，网络安全形势日益严峻。许多企业面临着黑客入侵、勒索软件攻击、数据泄露等各种安全威胁。弱密码、网络漏洞、未授权访问等安全隐患成为网络安全管理的主要问题。

2.2 运维流程与安全管理制度实施情况

在运维流程方面，许多企业已建立起了完善的网络运维流程，包括设备巡检、故障排查、性能监控、变更管理等环节。运维团队根据实际业务需求，制定了详细的运维计划和应急响应流程，以确保网络系统的稳定运行。一些企业仍存在运维流程不够规范、信息化程度不够高的问题，导致运维效率低下、故障响应不及时等情况。在安全管理制度实施方面，一些企业已建立了健全的网络安全管理机制，制定了信息安全政策、安全准入规范、安全审计流程等，以保障网络系统和数据的安全性。安全管理团队加强对网络威胁情报的监控与分析，及时更新安全补丁、加固网络边界、加强身份认证等措施，提高网络安全防护能力。但也有一些企业对安全管理的重视程度不够，网络安全制度实施不到位，安全培训和意识普及不足，存在着数据泄露、信息安全漏洞等风险。大部分企业在计算机网络运维及安全管理方面已有一定的规划与实践，但仍有待进一步提升。

2.3 现有运维及安全管理工具与平台评估

在当前信息技术发展迅速的环境下，企业面临着越来越复杂的网络运维与安全管理挑战。为应对这些挑战，众多国产运维管理工具与安全管理平台应运而生，展现出强大的市场潜力和技术实力。在运维管理工具领域，华为作为国内领先的通信与信息技术解决方案供应商，其提供的网络运维工具备受瞩目。华为的网络设备监控系统能够实时监控网络设备的运行状况，实现性能管理和故障排查，为运维团队提供全面、准确的数据支持。其他国内品牌的运维管理工具，如深信服的网络管理平台和中兴通讯的运维监控系统等，也都在市场中占有一定的份额，为企业提供了多样化的选择。在安全管理方面，国产安全产品同样展现出了强大的实力。例如，奇安信的安全威胁管理平台能够有效识别、预警和抵御各类网络安全威胁，确保企业网络数据的安全和保密性。绿盟科技和启明星辰等公司的安全产品也都在市场中获得了广泛的应用和认可。统一管理平台方面，国内厂商也推出了不少优秀的产品。像日志易这样的统一管理平台，能够提供全方位的数据分析、安全事件管理和日志审计功能，帮助企业快速发现和应对各类网络安全威胁。这些平台通过集成多种运维和安全工具，实现对网络环境的集中管理和监控，提高企业的运维和安全效率。

针对这些工具与平台的评估，需综合考量其功能性、易用性、性能稳定性和适应性等方面。有效的运维管理工具应具备实时监控、故障警示、性能优化等功能，帮助运维团队及时调整网络环境，确保网络稳定运行；而安全管理工具需能有效监测、预警和抵御各类网络安全威胁，为企业网络提供有效的安全保护。统一管理平台的集中管理和数据分析功能可帮助企业实现全方位的运维与安全管理，提高效率、降低成本、加强网络安全防护[2]。

3 计算机网络运维管理优化策略设计

3.1 运维流程优化与标准化

在当今数字化时代，计算机网络已成为企业信息化和业务运营的核心基础。为了有效管理和维护企业网络系统，运维流程优化与标准化是至关重要的一环。优化并标准化运维流程可以提高运维效率、降低故障响应时间，确保网络系统的可靠性和稳定性。在设计运维流程优化与标准化的策略时，需要对现有运维流程进行全面的审查和分析，识别存在的瓶颈和优化空间。通过制定明确的运维流程图、设定标准运维操作规范、建立运维任务分工流程，可以使运维工作更加规范有序。在运维流程中整合变更管理、故障管理、性能监控等环节，形成闭环运维管理体系，实现运维流程的全面覆盖和协同作业，提升整体运维效率。持续改进和优化运维流程是提升运维管理水平的关键。运维团队应不断总结和分析运维过程中的问题和经验教训，通过引入持续改进机制和KPI评估体系，保持运维流程的灵活性和高效性，以适应日益复杂的网络环境和业务需求。

3.2 自动化运维工具与平台应用

为了进一步提高运维管理效率和降低运维成本，引入自动化运维工具与平台已成为当今企业的趋势。自动化运维工具能够实现任务自动化执行、故障自愈、报警自动通知等功能，从而减少人工干预和提高运维响应速度。在应用自动化运维工具与平台时，企业应根据实际情况选择适合的工具，并充分考虑自动化与人工操作的结合，确保自动化运维工具与平台的可靠性和稳定性。在运维自动化过程中，建立清晰的自动化执行计划和预案，规范运维自动化操作流程，保证运维自动化的安全性和准确性。运维团队需要进行技术培训，提升自动化运维工具的使用能力和技术水平，确保运维团队能够熟练运用自动化工具解决实际问题。同时也需要加强与供应商的合作与沟通，及时了解自动化运维工具的更新功能和技术支持，为企业的运维自动化提供技术支持和保障。

3.3 运维团队能力提升与培训机制建设

运维团队的技术能力和素质是保障企业网络系统高效运行的关键因素。运维团队的能力提升与培训机制建设至关重要。通过持续的技术培训和团队建设，可以不断提升运维团队的整体素质和技术水平，以适应不断变化的网络环境和技术需求。在运维团队能力提升方面，应建立定期的培训计划，围绕网络运维、安全管理、自动化操作等方面进行培训，提高运维团队的专业知识和技术技能。运维团队还应该注重团队合作和沟通能力的培养，促进团队成员之间的协作和信息共享，提升整个团队的综合应对能力[3]。除了内部培训，运维团队还可以借助外部培训资源，参加行业会议、研讨会，获取最新的技术信息和趋势动向。建立奖惩机制和绩效考核体系，激励运维团队成员的学习和进步，提高团队整体绩效水平。

4 计算机网络安全管理优化策略设计

4.1 安全风险评估与应对机制建立

在现代信息社会，计算机网络的安全性至关重要。为了维护网络系统的安全，企业需要建立完善的安全风险评估与应对机制。通过对网络系统的安全风险进行全面评估，企业可以识别存在的潜在威胁和漏洞，有针对性地制定防范策略和紧急应对计划，从而提高网络的安

全性和稳定性。在进行安全风险评估时，企业可以采用多样化的方法，如定期扫描漏洞、进行安全事件模拟等方式来准确定位安全隐患和威胁。利用所得结果，企业可以规划应急响应机制，确立漏洞修复的紧急程度和时效性，以便可以快速、有效地应对可能的安全事件，减少潜在的损失和风险。建立安全风险评估与应对机制时，企业还应该定期进行安全风险评估和审查，及时更新安全策略和应对机制，以提升网络的安全性。此外，企业还应该加强与安全服务提供商的合作，获取最新的安全信息和技术支持，以提高安全防护的时效性和有效性。

4.2 安全技术与策略应用

安全技术和策略的应用是确保网络系统安全的一项重要措施，通过有效的安全技术和防护策略，企业可以有效减少各类网络安全威胁和攻击，确保网络系统的安全与稳定运行。对于安全技术的应用，企业可以综合运用各种防护技术，如网络防火墙、入侵检测系统以及安全漏洞修复等措施，来建立一个完善的网络安全防护体系。通过实施网络访问控制、数据加密和传输安全等技术手段，可以有效提升网络系统的安全性和抵御能力，从而保障网络数据的保密性和完整性。针对安全策略的应用，企业应根据自身的业务特点和风险情况，制定适用于企业实际情况的安全策略和规则，包括权限管理、数据备份与恢复策略、员工安全管理等方面，以全面提升网络系统的安全管理水平。定期评估并调整安全策略和规则，以提高安全策略的实效性和实施性，不断完善与加强网络安全的保护。

4.3 安全意识教育与制度完善

安全意识教育和制度的完善是企业网络安全管理的基础和关键环节。通过加强员工的安全意识培训和制度规范建设，企业可以提高员工对安全问题的认知和应对能力，减少员工的人为安全风险，确保网络系统的整体安全。要加强安全意识教育，企业应该建立全员参与的安全意识培训机制，包括网络安全知识的培训和安全政策的传达，以提高员工对网络安全问题的认识和重视程度。强调员工遵守合规规范和风险防范意识，提高员工在工作中的安全自我保护能力，降低员工对网络安全风险的可能影响[4]。企业还应该建立健全的安全制度和管理规范，明确安全责任和权限，规范安全策略和操作流程，以确保网络安全管理的规范性和可行性。建立有效的违规行为追责机制和安全事件报告制度，加强对员工行为的监督和管理，维护网络系统的整体安全稳定。在竞争激烈的市场环境中，只有不断改进和加强网络安全管理，才能确保企业信息资产的安全可靠性，为企业的创新和发展提供坚实保障。企业应致力于建立全面且具体的网络安全管理方案，不断完善和更新安全策略，加强员工的安全意识培养，并持续加强与安全技术供应商的合作，以确保网络系统在日益复杂的威胁环境下的长期安全。只有通过坚实的安全基础和持续的优化措施，企业才能在保护信息资产、维护客户信任和遵守法规合规的同时，实现网络系统的安全可靠性，为企业在数字化时代的发展注入新的动力和活力。

结束语

在当今信息化社会，网络安全管理不仅仅是技术问题，更是企业稳定发展的基石。通过优化计算机网络运维及安全管理设计，企业可以建立起坚固的安全防护体系，有效抵御各类网络威胁与攻击，为企业信息资产保驾护航。只有不断完善安全管理策略，加强安全意识教育，才能使网络系统在风云变幻的网络环境中立于不败之地，为企业的持续发展创造更加有利的条件。

参考文献

[1]李小龙.企业计算机网络的运维管理分析[J].集成电路应用.2021.(9).DOI:10.19339/j.issn.1674-2583.2021.09.091.

[2]秦波.计算机网络运维及安全管理设计优化策略研究[J].信息与电脑.2022.34(11).DOI:10.3969/j.issn.1003-9767.2022.11.065.

[3]王骏.韦文亮.计算机网络运维及安全管理设计优化策略探究[J].电脑知识与技术.2021.17(21):46-47.50.

[4]杨兆飞.赵欣.IMS网络运维管理新模式研究[J].长江信息通信.2022.35(1).DOI:10.3969/j.issn.1673-1131.2022.01.061.