计算机网络安全管理与维护

翁升叶
中国民用航空华东地区空中交通管理局　上海　200335

摘　要：计算机网络安全管理与维护是确保网络系统中数据安全和业务连续性的关键任务。通过制定并执行全面的安全管理策略，进行风险评估与漏洞扫描，建立事件响应机制，并提升员工安全意识，可以有效抵御网络威胁。同时，网络设备的安全配置、网络流量的实时监控与日志分析，以及数据的定期备份与恢复演练，为网络系统的稳定运行提供了坚实保障。综上所述，网络安全管理与维护是一个系统工程，需持续投入，确保网络环境的安全与稳定。

关键词：计算机网络；安全管理；维护

引言：在数字化时代，计算机网络的普及与广泛应用极大地推动了社会的进步与发展，但同时也使网络安全问题日益严峻。个人信息泄露、企业数据被攻击、乃至国家关键基础设施受威胁等事件频发，给社会造成了巨大的经济损失和安全风险。因此，加强计算机网络安全管理与维护，已成为维护个人隐私、保障企业运营稳定及国家安全的迫切需求。本文深入探讨了计算机网络安全管理的策略与实践，并提出了有效的维护措施，旨在构建一个更加安全、稳定的网络环境。

1 计算机网络安全概述

1.1 网络安全定义及重要性

网络安全是保护计算机网络系统中的数据免受未经授权的访问、泄露、修改、破坏或窃取的过程。它涵盖了网络系统的硬件、软件以及传输过程中的所有信息的安全保障。随着互联网的普及和技术的飞速发展，网络安全已成为维护国家安全、社会稳定和个人隐私的关键所在。它不仅关乎技术层面的防御与保护，更涉及法律法规、管理策略以及用户行为等多个维度的综合考量。（1）对个人而言，网络安全直接关系到个人隐私的保护。在数字化时代，个人信息如身份证号、银行卡号、住址电话等已成为网络攻击的重要目标。一旦泄露，可能导致财产损失、身份盗用等严重后果。因此，加强网络安全防护，保护个人隐私，是每个网民的基本需求和权利。（2）对企业而言，网络安全更是生死攸关的大事。企业的核心数据、商业秘密和知识产权是其竞争力的关键所在。一旦发生网络安全事件，不仅可能导致数据丢失、业务中断，还可能引发法律纠纷、品牌形象受损等连锁反应。因此，企业必须高度重视网络安全工作，建立健全的网络安全管理体系，确保业务运营的稳定和安全。（3）对社会而言，网络安全是维护社会稳定和国家安全的重要基石。随着互联网的普及和应用，网络已成为信息传播、社会交往和公共服务的重要平台。网络安全问题一旦爆发，可能迅速蔓延至各个领域，引发社会恐慌、混乱甚至危机。因此，加强网络安全管理，防范和打击网络违法犯罪活动，维护网络空间的秩序和安全，是国家和社会的共同责任。

1.2 网络安全威胁类型

在计算机网络环境中，存在着多种多样的安全威胁。其中，病毒、黑客攻击和恶意软件是最为常见且危害严重的三类威胁。病毒是一种具有自我复制和感染能力的恶意软件，它能够在计算机网络中迅速传播并破坏数据。黑客则利用技术手段非法侵入他人计算机系统，窃取数据、篡改信息或实施其他破坏性行为。而恶意软件则涵盖了病毒、蠕虫、特洛伊木马等多种形式，它们通过欺骗、伪装等手段诱骗用户下载并执行，从而对计算机系统造成损害。这些网络安全威胁的表现形式多种多样，包括但不限于邮件诈骗、钓鱼网站、恶意软件下载链接等。它们不仅可能导致用户数据泄露和财产损失，还可能破坏计算机系统的正常运行，影响业务的连续性和稳定性。更为严重的是，一些黑客组织或国家背景的攻击者可能利用网络安全漏洞进行网络战或信息窃取活动，对国家安全和社会稳定构成严重威胁。因此，加强网络安全防护意识和技术手段的应用，对于抵御各类网络安全威胁具有至关重要的意义。

2 计算机网络安全管理

2.1 安全管理策略与规范

（1）制定和执行网络安全策略的必要性。制定和执行网络安全策略是构建网络安全体系的首要任务。随着网络环境的日益复杂和威胁的多样化，一个明确、全面的安全策略能够为组织提供清晰的指导方向，确保所有安全活动都围绕共同目标展开。同时，执行这些策略能够有效预防、检测和响应网络安全威胁，降低潜在风

险，保障数据资产和业务连续性[1]。（2）安全策略的具体内容。安全策略应涵盖多个方面，包括但不限于访问控制策略、数据保护策略等。访问控制策略是确保只有授权用户才能访问特定资源的关键措施，通过实施身份认证、权限分配和访问审计等机制，可以有效防止未经授权的访问和数据泄露。数据保护策略则关注数据在传输、存储和处理过程中的安全性，包括数据加密、数据备份与恢复、数据分类与标识等措施，确保数据的机密性、完整性和可用性。

2.2 安全风险评估与漏洞扫描

（1）风险评估的方法与流程。安全风险评估是识别、分析和评价网络安全风险的过程，为制定针对性的防护措施提供依据。评估方法包括定性和定量分析，通过收集相关信息、识别潜在威胁和脆弱性、评估风险发生的可能性和影响程度等步骤，形成完整的风险评估报告。评估流程应确保全面、客观和可重复，以便持续监控和更新风险状况。（2）漏洞扫描技术与工具。漏洞扫描是发现网络系统中潜在安全漏洞的重要手段。现代漏洞扫描工具利用自动化技术和最新的漏洞信息库，对网络系统进行全面扫描和检测，快速识别潜在的安全隐患。这些工具不仅能够帮助组织发现已知漏洞，还能发现一些未知的、隐蔽的漏洞，为漏洞修复提供有力支持。（3）漏洞修复与补丁管理。发现漏洞后，组织应及时采取措施进行修复和加固。这包括安装安全补丁、更新系统配置、调整安全策略等。同时，组织应建立有效的补丁管理机制，定期检测和更新系统补丁库，确保所有系统都能及时获得最新的安全修复措施。漏洞修复和补丁管理是一个持续的过程，需要组织投入足够的资源和精力来保持网络系统的安全性。

2.3 安全事件响应与处理

（1）建立网络安全事件响应机制。建立网络安全事件响应机制是应对网络安全威胁的重要保障。该机制应包括事件报告流程、应急响应团队组成及职责、事件处理流程等关键要素。通过明确责任分工、建立紧急联络机制和制定详细的响应计划，组织可以在安全事件发生时迅速启动应急响应程序，有效控制事态发展并降低损失。（2）事件应急响应流程。事件应急响应流程通常包括事件发现与报告、事件初步评估与分类、应急响应启动、事件处置与恢复以及事件分析与总结等阶段。在每个阶段，组织都应按照既定流程进行操作，确保快速、准确地处理安全事件。特别是在事件处置与恢复阶段，组织应优先恢复关键业务功能并减少对用户的影响。（3）减小事件影响与恢复措施。为了减小安全事件对组织的影响并尽快恢复系统正常运行，组织应制定详细的恢复计划和措施。这包括数据恢复与备份验证、业务连续性计划（BCP）与灾难恢复计划（DRP）的实施、沟通与协调机制的建立以及后事评估与改进等。通过这些措施的实施，组织可以最大限度地降低安全事件带来的损失，并快速恢复业务运营[2]。

2.4 安全培训与意识提升

（1）定期对员工进行网络安全培训。定期对员工进行网络安全培训是提升组织整体安全水平的有效途径。培训内容应涵盖网络安全基础知识、最新威胁趋势、安全操作规范以及应急响应流程等方面。通过培训，员工可以了解网络安全的重要性、识别潜在的安全风险并采取必要的防范措施。此外，培训还应注重实践操作和案例分析，以提高员工的实战能力和应对能力。（2）提升员工的安全意识和操作技能。除了定期培训外，组织还应采取多种措施提升员工的安全意识和操作技能。这包括制定并实施安全政策和操作规程、建立安全激励机制和惩罚措施、定期发布安全提示和警示信息以及鼓励员工参与安全漏洞报告等。通过这些措施的实施，可以激发员工对网络安全的重视和责任感，促进员工自觉遵守安全规范和操作流程，从而提升组织的整体安全水平。

3 计算机网络安全维护

3.1 网络设备的安全配置与管理

网络设备作为网络连接的基础，其安全配置与管理是确保网络安全的第一道防线。（1）防火墙配置与管理。防火墙是网络安全的重要屏障，通过制定和执行安全策略，对进出网络的数据包进行过滤和控制，阻止潜在的恶意访问和攻击。防火墙的配置应基于组织的安全需求进行定制化设置，包括定义访问控制列表（ACLs）、实施网络地址转换（NAT）、配置虚拟专用网络（VPN）等。此外，定期对防火墙进行管理和维护，如更新规则库、检查日志文件等，以确保其有效性和响应能力。（2）入侵检测系统的部署与监控。入侵检测系统（IDS）能够实时监测网络中的异常行为，识别潜在的安全威胁，并及时发出警报。IDS的部署应根据网络结构和安全需求进行合理规划，以确保对关键区域和流量进行全面监控。同时，需要定期更新IDS的规则库和签名库，以应对不断演变的网络威胁。通过IDS的实时监控，组织可以及时发现并应对潜在的安全事件，防止事态的恶化[3]。（3）网络设备的定期更新与升级。随着网络威胁的不断演进，网络设备的安全漏洞也在不断被发现。因此，定期更新和升级网络设备是至关重要的。这包括操作系统、安全软件、固件等的更新，以确保设备

能够抵御最新的安全威胁。同时，需要关注厂商发布的安全公告和补丁，及时对设备进行补丁管理，以防止已知漏洞被利用。

3.2 网络流量监控与日志分析

网络流量监控与日志分析是网络安全维护的重要手段，通过对网络流量的实时监测和对日志的深入分析，可以发现潜在的安全威胁。（1）实时监控网络流量。实时监控网络流量可以帮助组织了解网络的使用情况和潜在的安全风险。通过分析流量数据，可以发现异常流量模式，如DDoS攻击、恶意扫描等。此外，监控网络流量还可以帮助组织优化网络性能，提升用户体验。为了实现实时监控，组织可以部署网络流量分析工具，如NetFlow、sFlow等，对流量数据进行采集和分析。（2）日志的收集、分析与保存。日志是记录网络设备和系统活动的重要信息源。通过收集、分析和保存日志，组织可以发现潜在的安全威胁、追踪攻击来源并评估安全事件的影响范围。为了有效管理日志数据，组织应建立日志管理系统，对日志数据进行集中存储、分类和索引。同时，需要定期对日志进行审查和分析，以发现潜在的异常活动和安全事件。此外，为了确保日志数据的完整性和可追溯性，需要对日志数据进行加密和备份。（3）通过日志分析发现潜在的安全威胁。日志分析是发现潜在安全威胁的关键步骤。通过对日志数据的深入挖掘和关联分析，可以发现异常登录尝试、恶意软件活动、数据泄露等安全事件。为了提升日志分析的效率和准确性，组织可以引入自动化分析工具和机器学习算法，对日志数据进行智能分析和预警。此外，建立应急响应机制，以便在发现安全威胁时能够迅速采取行动并降低损失[4]。

3.3 备份与恢复管理

备份与恢复管理是确保数据安全和业务连续性的重要手段。（1）定期备份重要数据与系统。定期备份重要数据与系统可以防止因硬件故障、人为错误或恶意攻击导致的数据丢失。备份策略应根据数据的重要性和恢复时间目标（RTO）进行定制化设置。对于关键业务数据和系统，应实施定期全量备份和增量备份相结合的策略，并确保备份数据的完整性和可用性。（2）灾难恢复计划的制定与实施。灾难恢复计划是应对严重网络安全事件或灾难性事故的重要方案。该计划应明确灾难恢复的目标、范围、流程和资源需求，并定期进行演练和验证。通过制定和实施灾难恢复计划，组织可以在发生严重安全事件时迅速恢复业务运营和数据访问能力。（3）数据恢复演练与验证。数据恢复演练与验证是确保灾难恢复计划有效性的关键环节。通过模拟实际的安全事件或灾难场景，组织可以检验恢复流程的执行情况和恢复时间是否符合预期。同时，还可以发现恢复过程中可能存在的问题和不足，并及时进行调整和优化。通过定期的数据恢复演练与验证，组织可以不断提升其应对安全威胁的能力和数据恢复的效率。

结束语

综上所述，计算机网络安全管理与维护是一项复杂而持续的工作，它要求我们在技术、管理和人员等多个层面共同努力，形成全方位的安全防护体系。通过制定科学的安全策略、加强安全监控与应急响应、提升人员安全意识与技能，我们可以有效抵御各类网络威胁，保障数据资产的安全与业务的连续性。未来，随着技术的不断进步和威胁形势的变化，我们还需要不断探索和创新，以应对新的挑战，确保计算机网络环境的安全与稳定，为数字经济的健康发展提供有力保障。

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(08):162-164.

[2]刘雯雯.基于云计算环境下的计算机网络安全存储系统的设计与实现[J].电脑知识与技术,2022,18(12):38-40.

[3]刘成.计算机网络安全技术在网络安全维护中的应用分析[J].网络安全技术与应用,2022(04):16-17.

[4]徐晨.计算机网络安全技术在网络安全维护中的应用分析[J].中国管理信息化,2022,(08):189-191.