网络信息安全的运维技术分析

郝彦甲[1] 孙 慧[2] 岳文彬[3]
1.2. 北方魏家峁煤电有限责任公司 内蒙古 鄂尔多斯 010308
3. 内蒙古蒙电华能热电股份有限公司 内蒙古 呼和浩特 010020

摘 要：随着信息技术的迅猛发展，网络信息安全成为企业信息化建设的核心要素。运维技术作为保障网络安全的基石，其重要性日益凸显。本文深入剖析安全风险评估、入侵检测、数据备份及安全培训等运维关键技术，旨在为企业提供全方位的技术支撑。同时，通过实际案例分析，展示这些技术在应对安全事件、保障数据安全方面的关键作用。这些成功案例不仅验证运维技术的有效性，也为其他企业提供宝贵的借鉴经验。

关键词：网络信息；运维技术；运维技术

1 网络信息安全概述

随着信息技术的迅猛发展和互联网的普及，网络信息安全已经成为当今社会不可或缺的重要议题。网络信息安全涉及保护网络系统的硬件、软件及其系统中的数据，防止其因偶然的或者恶意的原因而遭受到破坏、更改、泄露，确保系统连续可靠正常地运行，网络服务不中断。这不仅是技术问题，更涉及管理、法律、道德等多个层面。从技术层面来看，网络信息安全涉及诸多领域，如密码学、网络安全协议、防火墙技术、入侵检测系统等。密码学是信息安全的核心，它为数据的加密、解密提供了理论基础和实用方法。网络安全协议则确保网络中的信息在传输过程中不被窃取或篡改。防火墙技术和入侵检测系统则是防止外部攻击者非法进入网络系统的重要手段。技术手段并非万能，网络信息安全还需要依赖完善的管理制度和法律法规。企业需要建立完善的网络信息安全管理制度，包括安全策略、安全标准、安全操作流程等，以确保员工在日常工作中能够遵守安全规范，减少安全漏洞。政府也需要制定相关法律法规，对网络信息安全进行规范和监管，打击网络犯罪活动，维护网络空间的秩序和稳定[1]。网络信息安全还需要注重道德层面的建设，网络空间是一个开放、共享的空间，每个网络用户都应该遵守网络道德规范，尊重他人的隐私和权益，不从事网络攻击、网络诈骗等违法行为。

2 网络信息安全在当今数字化环境中的重要性

网络信息安全在当今数字化环境中的重要性，已经上升到了国家安全、经济发展和社会稳定的战略高度。随着科技的飞速发展，数字化技术已经渗透到我们生活的方方面面，从个人的衣食住行，到企业的经营管理，再到国家的战略决策，都离不开网络信息的支撑。与之相伴的是网络信息安全问题的日益凸显，其重要性不容忽视。第一，网络信息安全是保障个人隐私和权益的重要基石，在数字化环境中，我们的个人信息、财产信息、社交关系等都被存储在网络空间中。一旦这些信息被非法获取或滥用，不仅可能导致财产损失，还可能威胁到个人的生命安全和名誉。保护网络信息安全，就是保护我们每个人的合法权益和隐私。第二，网络信息安全对于企业的运营和发展至关重要，在当今数字化经济时代，企业的运营数据、商业机密、客户资料等都是企业的核心资产。一旦这些信息被泄露或被恶意攻击者利用，企业的正常运营将受到严重影响，甚至可能导致企业破产。加强网络信息安全建设，是保障企业稳健发展的必要条件。第三，网络信息安全还关系到国家的安全稳定，在数字化环境中，国家的政治、经济、军事等领域都面临着来自网络空间的威胁。

3 网络信息安全挑战分析

3.1 网络攻击的复杂性与隐蔽性

在数字化浪潮席卷全球的今天，网络攻击呈现出前所未有的复杂性与隐蔽性，给网络信息安全带来了严峻的挑战。网络攻击的复杂性主要体现在攻击手段多样、攻击路径复杂、攻击目标广泛等方面。攻击者可以利用各种技术手段，如漏洞利用、钓鱼攻击、恶意软件等，对目标系统进行渗透和破坏。攻击路径也变得更加复杂，攻击者可以通过多个跳板、代理服务器等方式隐藏自己的真实身份和攻击来源，使得追踪和防御变得异常困难。网络攻击的目标也日益广泛，从个人用户到大型企业，从政府机构到关键基础设施，无一不成为攻击者的潜在目标。网络攻击的隐蔽性同样令人担忧，攻击者往往采用高级持久性威胁（APT）等攻击方式，长期潜伏在目标系统中，窃取敏感信息或破坏关键业务。这些攻击通常不易被察觉，因为它们能够绕过传统的安全防护

措施，如防火墙、入侵检测系统等。即使被发现，攻击者也能迅速销毁证据、转移阵地，使得追踪和打击变得异常困难[2]。

3.2 数据泄露与隐私保护问题

在数字化环境中，数据泄露与隐私保护问题日益凸显，成为网络信息安全领域的一大挑战。随着大数据、云计算等技术的广泛应用，海量数据被存储在云端或网络空间中，这些数据往往包含个人隐私、商业机密等敏感信息。一旦这些数据被非法获取或泄露，将给个人和企业带来不可估量的损失。数据泄露的原因多种多样，包括技术漏洞、人为失误、恶意攻击等。技术漏洞可能是由于系统设计缺陷、软件缺陷等原因导致的，这些漏洞可能被攻击者利用来窃取数据。人为失误则可能发生在数据处理、传输、存储等各个环节，如操作不当、密码泄露等，这些都可能导致数据泄露。恶意攻击则是最为严重的一种情况，攻击者可能利用各种手段对目标系统进行渗透和破坏，窃取敏感数据。隐私保护问题同样不容忽视，在数字化环境中，个人隐私往往难以得到有效保护。一些不法分子可能通过网络攻击、钓鱼诈骗等手段获取个人信息，进而进行诈骗、敲诈等违法活动。

3.3 安全防护与业务发展的矛盾

在追求业务快速发展的同时，安全防护往往成为被忽视的一环，这导致了安全防护与业务发展之间的矛盾日益凸显。许多企业为了抢占市场先机、提高业务效率，往往将安全防护置于次要地位，甚至牺牲部分安全性来换取业务的发展。这种做法无疑给企业的信息安全带来了极大的隐患。安全防护与业务发展之间的矛盾主要体现在资源投入、技术选择和管理策略等方面，在资源投入方面，企业往往面临有限的预算和人力资源，需要在业务发展和安全防护之间进行权衡。有时，为了降低成本或提高效率，企业可能会减少对安全防护的投入，导致安全漏洞和风险的增加。在技术选择方面，业务发展可能要求企业采用新的技术或平台，而这些技术或平台可能存在未知的安全风险或漏洞。企业需要在追求技术创新和业务发展的同时，确保所选技术的安全性和稳定性。在管理策略方面，业务发展可能要求企业更加灵活和开放，而安全防护则要求企业建立严格的安全制度和流程。如何在保证业务发展的同时，确保安全管理的有效性和执行力，成为企业需要解决的一大难题。

4 网络信息安全运维技术分析

4.1 安全风险评估与监控

安全风险评估与监控是网络信息安全运维的基础和前提。通过定期进行安全风险评估，企业可以全面、系统地识别和分析网络环境中潜在的安全风险，包括系统漏洞、恶意软件威胁、人为失误等。评估结果可以为制定针对性的安全防护策略提供重要依据。在安全风险评估的基础上，实施有效的监控措施是确保网络信息安全的关键，监控手段包括网络流量监控、日志分析、入侵检测等，通过对网络行为和系统状态的实时监控，可以及时发现异常情况和潜在威胁，并采取相应措施进行处置。建立安全事件响应机制，对发生的安全事件进行快速响应和处置，减少损失和影响[3]。在安全风险评估与监控的实施过程中，应注重技术和管理相结合。利用先进的技术工具和手段，提高评估的准确性和监控的实时性；加强安全管理，建立健全的安全制度和流程，确保评估与监控工作的有效性和持续性。

4.2 入侵检测与防御系统

入侵检测与防御系统（IDS/IPS）是网络信息安全运维中的重要技术手段。IDS主要用于检测网络中的恶意行为和潜在威胁，通过对网络流量、系统日志等数据的分析，发现异常模式和攻击行为。IPS则侧重于在检测到威胁时主动采取防御措施，阻止攻击行为的发生。IDS/IPS系统能够实时检测和分析网络流量，识别出潜在的攻击行为和恶意软件，为网络安全运维人员提供及时、准确的警报信息。通过合理配置和部署IDS/IPS系统，可以实现对网络关键节点的全面监控和防护，有效防范外部攻击和内部威胁。在实施IDS/IPS系统时，需要注意几点：（1）要选择合适的系统和设备，确保其能够满足企业的实际需求和性能要求；（2）要合理配置和部署系统，避免漏报和误报的情况发生；（3）要定期对系统进行更新和维护，确保其能够持续有效地发挥作用。

4.3 数据备份与恢复策略

在数字化环境中，数据是企业的重要资产，一旦数据丢失或损坏，将给企业带来严重的损失。数据备份是指将重要数据定期复制到其他存储介质或位置，以防止数据丢失或损坏。备份策略应考虑到数据的完整性、可用性和可恢复性，确保在发生意外情况时能够迅速恢复数据。还需要定期对备份数据进行验证和测试，确保其可用性和有效性。数据恢复则是在数据丢失或损坏后，通过备份数据或其他技术手段恢复数据的过程，恢复策略应明确恢复流程和责任人，确保在发生数据丢失或损坏时能够迅速、准确地恢复数据。还需要制定应急响应计划，以应对突发事件导致的数据丢失或损坏。在制定数据备份与恢复策略时，企业应根据自身的业务特点和实际需求进行选择。

4.4 安全培训与意识提升

安全培训与意识提升是网络信息安全运维中不可忽视的一环。员工是网络信息安全的第一道防线，他们的安全意识和行为直接关系到企业的网络安全状况。安全培训应涵盖网络安全基础知识、安全操作规程、应急响应流程等内容，帮助员工了解网络安全的重要性和风险点，掌握基本的安全防护技能。培训形式可以多样化，包括线上课程、线下讲座、实战演练等，以提高员工的参与度和学习效果。除了安全培训外，提升员工的安全意识同样重要。企业可以通过安全宣传、安全提示等方式，不断提醒员工关注网络安全问题，养成良好的安全习惯。建立安全激励机制，对在网络安全方面表现突出的员工进行表彰和奖励，以激发员工的安全责任感和积极性。在安全培训与意识提升的过程中，企业应注重实效性和持续性，培训内容应紧密结合企业实际和业务需求，确保培训成果能够转化为实际的安全防护能力。

5 运维技术在网络信息安全中的实际案例分析

5.1 安全事件监控与应急响应案例

在某大型金融企业，曾遭遇了一起严重的网络攻击事件。由于该企业的网络规模庞大，系统复杂，传统的安全防护手段难以有效应对。为提升安全防护能力，企业引入先进的安全事件监控与应急响应系统。该监控系统通过实时收集和分析网络流量、系统日志等数据，能够及时发现异常行为和潜在威胁。在这次攻击事件中，监控系统迅速检测到了异常流量和恶意行为，并自动触发报警机制。安全运维团队立即收到报警信息，并启动应急响应流程。在应急响应过程中，安全运维团队首先对攻击来源进行追踪和定位，确定攻击者的身份和攻击路径。团队迅速采取隔离措施，切断攻击者与系统之间的连接，防止攻击的进一步扩散。团队对受影响的系统进行详细的安全检查和分析，找出被利用的漏洞和弱点，并制定相应的修复和加固措施。通过安全事件监控与应急响应系统的有效运用，该企业成功应对这次网络攻击事件，避免重大损失。

5.2 数据备份恢复案例分析

某知名电商企业在一次意外停电事故中，核心数据库遭受了严重损坏。由于该数据库存储着企业的关键业务数据和客户信息，一旦丢失或损坏，将给企业带来不可估量的损失。幸运的是，该企业提前建立完善的数据备份与恢复机制，成功避免了数据丢失的风险。在数据备份方面，该企业采用定期全量备份和增量备份相结合的方式[4]。每天定时对数据库进行全量备份，确保数据的完整性和一致性；在业务高峰期或数据变动较大的时段，进行增量备份，以捕获数据的变化。备份数据存储在专门的备份服务器上，并定期进行验证和测试，确保其可用性和有效性。当意外停电事故发生时，企业的核心业务被迫中断，数据库也遭受了严重损坏。由于有完善的数据备份机制，运维团队迅速启动了数据恢复流程。从备份服务器中获取最新的备份数据；利用专业的数据恢复工具，对损坏的数据库进行修复和恢复。在整个恢复过程中，运维团队密切协作，严格按照恢复流程操作，确保数据的完整性和准确性。经过几个小时的努力，受损的数据库得到了成功恢复，企业的核心业务也得以迅速恢复运行，这次数据备份恢复的成功实践，不仅避免企业因数据丢失而遭受的巨大损失，也验证企业数据备份与恢复机制的有效性和可靠性。这个案例告诉我们，数据备份与恢复是网络信息安全运维中不可或缺的一环。

结束语

网络信息安全运维技术是企业信息化建设不可或缺的一部分。通过不断研究和实践，可以更好地掌握和应用这些技术，提升企业的网络安全防护能力。同时，也应认识到，网络信息安全是一个持续的过程，需要企业不断加强管理和投入，确保网络信息系统的安全和稳定运行。随着技术的不断进步和攻击手段的不断变化，还应继续探索和创新运维技术，以适应不断变化的网络环境，为企业的发展提供坚实的网络安全保障。

参考文献

[1]王明芬,林婷.基于WAF的网络运维系统设计[J].电信快报,2020(11):26-29.

[2]张浩,戴凯明,姚丹.数据中心网络运维数字化转型探索[J].金融电子化,2020(10):97-98.

[3]董靓.计算机网络运维及安全管理设计[J].中国新通信,2020,22(15):119.

[4]杨朝晖,李飞,付永振.微服务编排在网管支撑系统中的研究与应用[J].电信工程技术与标准化,2019,32(6):31-36.