信息安全新形式下的信息安全运维管理研究

唐　颖　殷懿鸿
上海外高桥造船有限公司　上海　200137

摘　要：在信息安全新形势下，新兴技术广泛应用、网络攻击手段演变，给信息安全运维管理带来诸多挑战。传统运维管理模式局限性凸显，安全运维人员能力短缺，数据安全与隐私保护难题待解，安全运维工具也存在不足。本文针对这些挑战，提出优化策略，包括构建智能化运维管理体系、加强安全运维人员培养与管理、强化数据安全与隐私保护措施、优化安全运维工具的选择与应用，旨在提升信息安全运维管理水平，适应新形势发展需求。

关键词：信息安全；新形式下；信息安全；运维管理

引言：在数字化浪潮迅猛发展的当下，信息安全已成为关乎国家、企业及个人利益的关键要素。随着云计算、大数据、物联网等新兴技术的广泛应用，信息系统的复杂性和开放性大幅增加，信息安全面临着前所未有的挑战。与此同时，网络攻击手段不断演变，高级持续性威胁（APT）攻击、勒索软件攻击、供应链攻击等层出不穷，传统信息安全运维管理模式已难以有效应对。此外，国家和行业对信息安全的监管政策日益严格，企业需不断提升信息安全运维管理水平以满足合规要求。在此背景下，深入研究信息安全新形势下的信息安全运维管理具有重要的现实意义。

1 信息安全新形势分析

1.1 新兴技术带来的安全挑战

1.1.1 云计算安全

云计算通过弹性资源分配与按需服务模式重塑了IT架构，但其多租户共享、虚拟化层级复杂等特性导致安全边界模糊。攻击者可利用云平台接口漏洞发起跨租户攻击，或通过恶意软件感染共享存储资源。2024年AT&T云数据泄露事件中，攻击者通过劫持云服务账号窃取超1亿条用户数据，凸显了云环境身份认证与访问控制失效的严重后果。

1.1.2 大数据安全

大数据的分布式存储与高频流动特性使其成为APT攻击的核心目标。攻击者通过注入恶意代码篡改数据流，或利用数据关联分析挖掘敏感信息。2025年某金融机构因未对日志数据脱敏，导致客户交易模式被算法解析，引发系统性欺诈风险。此外，数据生命周期管理缺失导致30%企业存在过期数据未清理问题，为攻击者提供长期潜伏基础。

1.1.3 物联网安全

物联网设备数量预计2025年达750亿台，其低功耗、长生命周期特性与安全投入不足形成矛盾。智能摄像头固件漏洞导致2024年全球超200万台设备被劫持组建僵尸网络，发起DDoS攻击使北欧电网瘫痪6小时。医疗物联网设备更面临致命风险，某品牌胰岛素泵因无线协议缺陷被远程操控，直接威胁患者生命安全。

1.2 网络攻击手段的演变

1.2.1 APT攻击

APT（高级持续性威胁）攻击通过长期潜伏、定制化恶意软件及社会工程学手段，针对政府、金融等关键领域实施隐蔽渗透。攻击者利用零日漏洞、供应链感染等途径建立持久化访问，结合多阶段横向移动窃取敏感数据。2025年APT攻击已呈现AI赋能特征，通过自然语言处理生成定制化钓鱼内容，并利用强化学习模型加速0day漏洞挖掘，显著提升攻击精准度与隐蔽性。

1.2.2 勒索软件攻击

勒索软件通过加密数据或锁定系统实施勒索，2025年呈现三大特征：技术融合化采用无痕驻留内存技术规避检测，目标定向化聚焦高价值企业，战术隐蔽化结合边缘设备漏洞实现多端协同。攻击者利用自动化工具批量挖掘NAS设备RCE等未公开漏洞，结合"双重勒索"策略，既加密数据又威胁泄露，迫使企业支付赎金以避免法律与声誉风险。

1.2.3 供应链攻击

供应链攻击通过渗透软件、硬件或服务全链条实施立体化作战，2025年呈现三大趋势：利用AI扫描开源组件依赖树定位低维护频率库作为突破口；滥用云服务API临时权限漏洞注入后门；通过二级供应商植入恶意代码实现"一次入侵，全网扩散"。典型案例包括攻击者劫持软件供应商代码签名，在云服务商API漏洞中植入持久化后门，导致企业核心系统被间接控制[1]。

2 信息安全运维管理在新形势下的挑战

2.1 传统运维管理模式的局限性

传统运维管理模式多依赖人工操作与经验判断，在面对海量数据处理和复杂网络环境时，效率低下且易出错。其缺乏自动化与智能化手段，难以快速响应安全威胁。同时，传统模式各部门间信息流通不畅，协同困难，无法形成整体安全防护合力。在新形势下，网络攻击手段日益多样，传统模式已难以满足信息安全运维管理的实时性、精准性和全面性要求。

2.2 安全运维人员的能力要求与短缺

新形势下，安全运维人员需具备多领域知识，涵盖网络安全、系统运维、数据分析等，还要熟悉各类安全工具和法规标准。然而，现实中此类复合型人才短缺。一方面，专业人才培养周期长，高校相关专业设置和课程体系更新滞后；另一方面，行业对安全运维重视不足，人才吸引力和留存率低。这导致企业在面对复杂安全挑战时，运维力量捉襟见肘，影响信息安全保障水平。

2.3 数据安全与隐私保护的难题

随着数字化发展，数据量呈爆炸式增长，数据安全与隐私保护面临严峻挑战。数据泄露途径增多，如网络攻击、内部人员违规操作等。不同行业数据隐私要求各异，合规难度大。同时，数据跨境流动频繁，国际间数据保护规则差异大，协调困难。此外，新技术如人工智能、大数据的应用，在提升数据处理效率的同时，也带来新的隐私风险，使得数据安全防护更加复杂。

2.4 安全运维工具的不足

现有安全运维工具存在诸多不足。部分工具功能单一，仅能处理特定类型安全问题，无法满足综合防护需求。一些工具兼容性差，难以在不同系统和环境中稳定运行。而且，面对新型网络攻击手段，工具更新速度滞后，不能及时有效识别和防范。此外，工具产生的海量安全数据缺乏有效分析手段，难以挖掘潜在威胁，无法为安全决策提供有力支持，影响安全运维效果[2]。

3 信息安全运维管理的优化策略

3.1 构建智能化运维管理体系

3.1.1 引入人工智能和机器学习技术

在智能化运维管理体系中，引入人工智能和机器学习技术是关键一环。人工智能可模拟人类智能处理复杂问题，机器学习则能通过数据训练不断优化模型。利用机器学习算法对海量安全日志、网络流量等数据进行分析，能精准识别异常行为模式，提前预警潜在安全威胁。例如，通过分析历史攻击数据训练模型，可快速识别新型APT攻击特征。同时，人工智能还能实现智能决策，自动调整安全策略，提高运维效率和准确性，有效应对日益复杂的网络攻击环境，为信息安全运维提供强大技术支撑。

3.1.2 实现自动化运维流程

实现自动化运维流程是构建智能化运维管理体系的重要举措。传统运维依赖大量人工操作，效率低且易出错。自动化运维可借助脚本、工具和平台，对系统监控、故障排查、配置管理等任务进行自动化处理。比如，通过自动化脚本定期检查系统漏洞并修复，利用监控工具实时收集设备性能数据，自动触发告警机制。自动化运维不仅能减少人力成本，还能大幅缩短故障响应时间，提高运维的及时性和一致性，确保信息系统稳定运行，增强企业应对安全风险的能力。

3.1.3 建立安全态势感知平台

建立安全态势感知平台对于智能化运维管理体系至关重要。该平台能整合多源安全数据，包括网络流量、系统日志、安全设备告警等，通过大数据分析和可视化技术，全面呈现企业安全态势。它可实时监测安全状况，及时发现潜在威胁，预测安全趋势。例如，通过分析网络流量数据，识别异常流量模式，判断是否存在DDoS攻击风险。同时，平台还能为安全决策提供数据支持，帮助运维人员制定针对性策略。借助安全态势感知平台，企业能实现主动防御，提升整体信息安全防护水平。

3.2 加强安全运维人员的培养与管理

3.2.1 制定针对性的培训计划

安全运维领域技术迭代迅速，制定针对性培训计划是提升人员能力的核心。需结合企业业务场景与安全威胁趋势，设计分层培训体系：初级课程聚焦基础技能，如操作系统加固、日志分析；中级课程涵盖威胁狩猎、应急响应实战；高级课程引入AI安全、零信任架构等前沿技术。同时，联合安全厂商开展红蓝对抗演练，模拟勒索软件、供应链攻击等场景，提升人员实战能力。

3.2.2 建立人才激励机制

为缓解安全运维人才短缺问题，需构建多元化激励机制。物质层面，设立安全专项奖金，对发现重大漏洞、阻止攻击事件的人员给予高额奖励；提供具有竞争力的薪资涨幅，匹配行业技术溢价。精神层面，设立“安全卫士”等荣誉称号，在内部平台公开表彰；为优秀人才提供参与行业峰会、技术研讨的机会，拓宽职业视野。职业发展上，设计“技术专家-管理双通道”，允许人员根据特长选择晋升路径，避免因晋升瓶颈导致人才流失，激发团队创新活力。

3.2.3 明确岗位职责与权限

安全运维涉及多环节协作，需通过RACI矩阵（负

责、批准、咨询、知情）明确职责边界。例如，安全分析师负责威胁监测与初步处置，运维工程师执行系统加固与补丁管理，安全架构师设计整体防护方案。权限分配遵循最小化原则，结合零信任理念，通过动态访问控制技术，根据角色、设备、环境等因素实时调整权限。例如，仅允许特定IP段的运维终端访问核心系统，离职人员权限自动冻结。定期审计权限使用记录，防止越权操作，确保安全运维流程规范高效。

3.3 强化数据安全与隐私保护措施

3.3.1 完善数据安全管理体系

完善数据安全管理体系是强化数据保护的基础。需构建涵盖数据全生命周期的管理框架，从数据采集、存储、使用到销毁，制定标准化流程与规范。建立数据分类分级制度，依据敏感程度划分等级，实施差异化保护策略。同时，设立专门的数据安全管理团队，负责制定策略、监督执行与应急响应。定期开展数据安全风险评估，识别潜在威胁与漏洞，及时调整防护措施。

3.3.2 采用数据加密与脱敏技术

数据加密与脱敏技术是保障数据安全的关键手段。对敏感数据在传输和存储过程中采用高强度加密算法，如AES、RSA等，确保数据即使被窃取也难以解密。在数据使用环节，运用脱敏技术对敏感信息进行替换、遮蔽等处理，使数据在不影响使用价值的前提下降低泄露风险。例如，在测试环境中使用脱敏后的真实数据，既能保证系统测试的准确性，又能避免敏感信息泄露。通过加密与脱敏技术的结合应用，为数据安全提供双重保障。

3.3.3 加强数据安全合规管理

加强数据安全合规管理是适应监管要求、避免法律风险的重要举措。密切关注国家和行业的数据安全法规政策，确保企业数据处理活动符合相关标准。建立合规审查机制，对数据收集、使用、共享等环节进行严格审查，防止违规行为发生。同时，积极参与行业自律组织，借鉴先进经验，提升企业合规水平。加强与监管部门的沟通，及时了解政策动态，调整合规策略。

3.4 优化安全运维工具的选择与应用

3.4.1 选择综合性的安全运维工具

综合性安全运维工具能整合多种安全功能，满足企业复杂的安全需求。它应涵盖漏洞扫描、入侵检测、日志分析、资产管理等核心模块，实现一站式安全防护。例如，一款优质的综合工具可自动扫描系统漏洞，实时监测网络攻击行为，集中收集和分析各类日志，清晰呈现资产状况。选择时，要考量工具的兼容性，确保与企业现有系统无缝对接；关注其可扩展性，以便适应未来业务发展和安全威胁变化。

3.4.2 推动安全运维工具的智能化升级

随着安全威胁日益复杂，推动安全运维工具智能化升级迫在眉睫。利用人工智能和机器学习技术，使工具具备自主学习和决策能力。例如，智能入侵检测工具可通过学习正常网络行为模式，精准识别异常流量和攻击行为；智能漏洞扫描工具能根据历史数据预测新漏洞出现位置，提高扫描效率和准确性。同时，智能化工具可实现自动响应和修复，快速处理安全事件。企业应积极引入先进技术，与工具厂商合作，推动工具智能化发展，提升安全运维的主动性和有效性。

3.4.3 建立安全运维工具的协同机制

安全运维涉及多种工具，建立协同机制至关重要。不同工具应实现数据共享和交互，打破信息孤岛。例如，漏洞扫描工具发现漏洞后，能自动将信息传递给补丁管理工具进行修复；入侵检测工具检测到攻击时，可联动防火墙进行阻断。同时，建立统一的管理平台，对各类工具进行集中监控和管理，实时掌握工具运行状态和安全事件处理进度。通过协同机制，各工具可形成合力，发挥最大效能，提高安全运维的整体响应速度和处理能力，有效应对各类安全挑战[3]。

结束语

在信息安全新形势下，信息安全运维管理面临着传统模式局限、人员能力短缺、数据保护难题及工具不足等诸多挑战。通过构建智能化运维管理体系、加强人员培养与管理、强化数据安全隐私保护以及优化安全运维工具选择与应用等策略，可有效提升信息安全运维水平。然而，信息安全领域技术迭代迅速、威胁不断演变，未来仍需持续探索创新。

参考文献

[1]蔡暮章.电网信息系统安全工程的管理流程体系研究.上海交通大学，2022.134-136

[2]王景川.基于智能电网的电力调度数据网运维管理研究.华北电力大学，2022.176-178

[3]李长征.电子政务运维管理的关注因素[J].信息化建设，2021（02）：198-199