 DOI: https://doi.org/10.12349/iser.v6i5.5671

Integrated development of enterprise system configuration, operation and maintenance and digital projects from the perspective of network security

Xinyu Fu

Fujian Huadian Shaowu Energy Co., Ltd., Shaowu, Fujian, 354000, China

Abstract

from the perspective of network security, this paper discusses the key countermeasures for enterprises in the integrated development of system configuration, operation and maintenance and digital projects. Based on the basic principles of security priority, minimum authority, continuous monitoring, and automated operation and maintenance, this paper proposes specific measures such as establishing a security system, strengthening identity authentication, implementing access control, and strengthening log management, aiming to improve the security and stability of system operation. Enterprises can effectively prevent security risks by fully integrating the security mechanism into the whole process of system operation and maintenance and project construction, and promote the steady progress of digital transformation on a controllable and reliable basis.

Keywords

network security; Enterprise system configuration; Digital project

网络安全视角下企业系统配置运维与数字化项目融合发展

傅欣瑜

福建华电邵武能源有限公司，中国 · 福建 邵武 354000

摘　要

本文从网络安全视角出发探讨了企业在系统配置运维与数字化项目融合发展中的关键对策，文章围绕安全优先、最小权限、持续监测、自动化运维等基本原则提出了建立安全体系、强化身份认证、实施访问控制、加强日志管理等具体措施，旨在提升系统运行的安全性与稳定性，企业通过将安全机制全面融入系统运维与项目建设全过程能够有效防范安全风险，推动数字化转型在可控与可靠的基础上稳步前行。

关键词

网络安全；企业系统配置；数字化项目

1 引言

在数字化转型加速推进的背景下，企业面临日益复杂的网络安全威胁，系统安全管理已不再是单一技术环节，而是保障业务连续性与数据安全的关键，通过将网络安全融入数字化项目全过程，实现配置运维与安全管理一体化已成为企业高质量发展的必然趋势。

2 网络安全视角下企业系统配置运维的概念

从网络安全视角看，企业系统配置运维是指在保障信息系统稳定运行的同时将安全策略、权限控制、漏洞管理等安全措施全面融入系统的配置与日常运维过程中，它不仅涵盖了服务器、网络设备、数据库等基础设施的配置管理，还包括对系统运行状态的监控、日志审计、补丁更新等操作，确保系统在运行过程中具备良好的安全性、可用性与可控性，企业通过标准化、自动化和持续优化的配置运维管理能够有效应对日益严峻的安全威胁，防范潜在攻击风险，为数字化业务提供坚实的技术保障 [1]。

3 网络安全视角下企业系统配置运维与数字化项目融合发展的基本原则

3.1 安全优先原则

在企业系统配置运维与数字化项目融合发展的过程中，安全优先原则是保障整体信息化建设稳健推进的核心理念，安全优先原则强调在系统设计、部署、运维各阶段必须将网络安全置于首位，将安全因素纳入所有技术与管理决策中，确保信息系统在功能实现的同时具备应对各种潜在威胁的能力，安全优先不仅意味着要防止黑客攻击、病毒侵扰等外

【作者简介】傅欣瑜（1994–），女，中国泉州南安人，本科，从事研究数字化与网络安全相关研究。

部风险，还要求及时识别和防范内部潜在漏洞与配置失误，做到“安全内建、安全默认、安全运维”，落实安全优先原则需要企业建立从高层战略到基层执行的全方位安全管理机制，例如在系统配置阶段应优先考虑采用最小权限原则与默认加密策略；在运维过程中需加强对日志的持续监控与风险行为的自动预警响应；而在数字化项目推进中则需制定涵盖安全需求的项目规范，确保开发、测试与上线环节始终嵌入安全控制措施，企业通过将安全作为系统生命周期管理的核心要素不仅能有效提升业务连续性和服务可靠性，也能在数字化转型中占据更加稳固的优势地位 [2]。

3.2 最小权限控制

在网络安全视角下，最小权限控制原则是指在系统配置与运维过程中，为用户、设备和系统进程分配完成其工作所必需的最低权限，避免赋予超出职责范围的访问权，最小权限控制原则可显著降低误操作、系统滥用以及权限被恶意利用的风险，是保障系统安全性和可控性的重要手段，特别是在多用户、多角色的企业环境中最小权限控制可以有效防止内部安全事件的发生，提高整体运维的安全等级，企业要有效落实最小权限控制需建立科学的权限分级与分配机制，对各类账号和系统组件进行细粒度的权限配置，并结合身份验证、访问审计与行为监控等技术手段强化管理，例如普通员工账号应禁止访问关键配置文件，运维人员应根据具体职责分配访问权限，并定期审查权限使用情况，同时企业应在权限变更、人员流动、岗位调整等情况下及时更新权限配置，确保权限始终与实际需求相匹配，企业通过持续优化权限管理体系可以最大限度地减少权限滥用带来的安全隐患，增强系统整体的抗攻击能力和可追溯性 [3]。

3.3 持续监测审计

在网络安全视角下，持续监测审计是企业系统配置运维与数字化项目融合发展过程中不可或缺的安全原则，其核心在于通过对系统运行状态、访问行为、配置变更等关键环节的实时监测与全面审计，及时发现异常情况，防范安全事件的发生，系统结构随着企业数字化程度不断提高而日趋复杂，传统的定期检查已难以满足现代化安全需求，必须依赖持续的、动态的监测与日志审计手段，确保系统处于受控状态，落实持续监测审计原则需要企业构建完善的监控平台，部署入侵检测系统（IDS）、安全信息与事件管理系统（SIEM）等工具，对网络流量、用户行为、配置变更、权限使用等数据进行实时采集和分析，同时企业应建立日志审计机制，对关键操作进行留痕记录，确保安全事件“可追踪、可还原、可问责”，此外企业还应制定预警和响应机制，对监测到的异常行为及时处理，降低风险扩散的可能性，企业通过实现安全数据的持续可视化与闭环管理能够在保障业务连续性的同时有效提升整体安全防护水平 [4]。

3.4 自动化运维管理

在网络安全视角下，自动化运维管理是提升企业系统安全性与效率的关键原则之一，随着系统架构日趋复杂、业务需求不断变化，传统手工运维方式已难以满足高效、可靠与安全并重的目标，企业通过引入自动化运维工具与平台可以实现对系统配置、部署、监控、补丁更新等关键环节的标准化和自动执行，减少人为操作失误，提高响应速度，同时增强系统在面对安全威胁时的快速应对能力，

自动化运维不仅提升运维效率，更是在安全控制中扮演着重要角色。通过自动化流程可以统一执行安全策略配置、批量下发补丁和更新、自动检测配置偏差以及自动修复已知漏洞，大大降低因配置不一致或管理疏漏带来的安全隐患，同时自动化系统还能结合日志分析和智能预警机制，快速识别异常行为并触发响应措施，实现运维与安全的一体化管理，企业随着技术不断发展应积极推动自动化工具的部署与优化，将自动化能力深度融入系统生命周期各阶段，从而在保障业务稳定运行的同时，构建起更为稳固的安全防线。

4 网络安全视角下企业系统配置运维与数字化项目融合发展的对策

4.1 建立安全体系

在企业系统配置运维与数字化项目融合发展的过程中，建立完善的安全体系是确保信息资产安全、业务稳定运行的基础性对策，安全体系不仅是防范外部攻击的防线，更是内部管理规范与风险防控能力的集中体现，从网络安全视角出发构建安全体系应涵盖技术防护、制度保障、人员管理和应急响应等多个方面，形成“制度规范＋技术手段＋人员意识”相结合的综合防护机制，企业应从顶层设计出发，明确安全战略目标，制定包括访问控制、数据保护、身份认证、权限管理等在内的制度规范，建立统一的安全管理架构。企业应部署防火墙、入侵检测系统、漏洞扫描平台等关键技术工具，配合运维流程中的安全配置和实时监测手段，确保系统运行全流程可控、可查、可防，此外企业还需加强员工的安全意识培训，推动安全责任落实到岗位与个人，建立分级分类的应急响应机制，一套科学、系统、持续优化的安全体系不仅能有效防范各类安全风险，还将为企业数字化转型和持续发展提供坚实的保障。

4.2 推行自动化运维

在企业系统配置运维与数字化项目融合发展的背景下，推行自动化运维是提升效率与安全水平的重要对策，随着业务系统的规模日益扩大和复杂性不断提升，传统依赖人工操作的运维方式已难以满足高效稳定运行的需求，同时也易引发安全漏洞和配置错误等问题，自动化运维通过预设脚本、自动化平台及智能化工具的广泛应用，实现对系统配置、部署、监控、故障修复等流程的自动执行，这不仅提高了工作效率，还显著降低了人为干预带来的安全风险 [5]。在实际应用中，企业可通过引入华为公司的自动化工具，实现对服务器配置的标准化管理，减少环境不一致性；结合监控告警系

统，可对系统运行状态进行实时跟踪，并在发现异常时自动触发响应机制，同时自动化工具还可用于定期更新安全补丁、清理冗余权限、自动备份数据等日常运维任务，提升整体安全防护能力，企业通过自动化与网络安全策略的深度融合能够建立起更加智能、高效、可控的运维体系，为数字化项目的企业安全坚实基础。

4.3 强化身份认证

在网络安全视角下，强化身份认证是保障网络安全的重要对策，随着企业数字化程度不断加深，越来越多的用户、设备和系统需要接入核心业务系统，若身份认证机制薄弱极易被恶意攻击者利用，导致敏感数据泄露或系统被非法控制，因此企业必须建立起严格、可靠的身份认证体系，从源头上阻断未经授权的访问行为，确保每一次系统访问都有明确、可验证的身份依据。企业可以实施强化身份认证的策略，采用多因素认证（MFA）方式，结合密码、生物识别、短信验证码、硬件令牌等多种手段，以此有效提升账号安全性，同时企业应推行基于角色的访问控制（RBAC），严格限定用户权限范围，防止超权限操作，企业对于运维人员和高权限账号还应配合行为审计和操作记录，形成可追溯的使用痕迹。在系统配置层面，企业应统一认证入口，实现单点登录(SSO)与身份集中管理,减少分散认证带来的管理盲区，企业通过强化身份认证机制不仅能够有效防范内部越权操作和外部入侵行为，还可全面提升系统整体安全防护能力，为数字化项目稳步推进提供坚实保障。

4.4 实施访问控制

在企业系统安全管理过程中，实施访问控制是确保信息系统安全稳定运行的关键对策之一，访问控制的核心在于通过对用户、设备、应用程序等主体的访问权限进行精细化管理，防止未经授权的访问行为，确保系统资源仅在合法范围内被使用，随着企业业务系统复杂化和多元化，访问控制已不仅仅是权限分配的问题，更关系到系统整体安全架构的科学性与风险控制的有效性，企业还需建立完善的访问控制策略与机制，根据岗位职责推行基于角色的访问控制（RBAC），确保用户仅能访问与其职责相关的资源与功能；企业应引入动态访问控制技术，如基于属性的访问控制（ABAC）和基于风险的访问控制（RBAC+），以适应动态环境下的权限管理需求。在系统层面，企业应采用分层授权策略，对不同系统模块、数据资源设置不同访问等级，结合身份认证机制，强化权限校验，企业在运维过程中还需配合日志审计和行为监控，实时记录和分析访问行为，及时发现越权操作或异常访问事件，此外企业需要定期对权限配置进行审查和清理，防止“权限膨胀”现象的出现，企业通过构建科学、高效、可持续的访问控制体系不仅能提升系统安全性，还能优化资源使用效率，推动数字化项目在安全可控的基础上健康发展。

4.5 加强日志管理

在企业系统配置运维与数字化项目融合发展的过程中，加强日志管理是提升系统安全防护能力的重要对策，日志记录是系统运行的重要“证据链”，涵盖了用户行为、系统事件、安全警报、配置变更等关键信息，对于事前风险预警、事中行为追踪以及事后事件溯源都具有不可替代的作用，特别是在面临网络攻击或系统故障时，详尽、准确的日志记录能够为安全事件分析与响应提供有力支持，有助于快速识别攻击路径与受影响范围，提升安全应对效率。为有效加强日志管理，企业应从制度和技术两个层面同步推进，企业在制度上应制定统一的日志采集、存储、审计和保留规范，明确各类系统和业务场景下的日志记录内容与时限要求；企业在技术上应部署集中式日志管理平台，将分散在各系统中的日志信息统一归集，并引入日志分析工具，实现对异常行为的自动识别和预警，同时企业应设置合理的日志访问权限，防止日志被篡改或泄露；而对于关键系统，企业还应启用审计日志和安全日志双重机制，实现精细化的操作记录，企业通过建立覆盖全系统、全流程的日志管理机制可以提升运维透明度、增强安全事件可追溯性，为系统运行提供更强的安全支撑与保障。

5 结语

在网络安全日益严峻和数字化转型加速推进的双重背景下，企业必须将系统配置运维与数字化项目深度融合，并以网络安全为核心导向，构建科学、高效、可持续的管理体系，企业通过强化身份认证、实施访问控制、推行自动化运维、加强日志管理等多项对策能够有效提升信息系统的安全性与稳定性，保障业务连续性与数据资产安全，未来唯有坚持安全优先原则，持续优化配置与运维机制，方能实现高质量、安全化的数字化发展目标。

参考文献

[1] 黄捷.浅谈网络安全与系统运维领域的新技术应用[J].通讯世界, 2024, 31(3):30-32.

[2] 段文凯.视频网“安全+运维”一体化建设浅析[J].中国安防, 2020(8):4.

[3] 崔向娜,南宇辉.云计算环境下的网络运维管理和安全挑战[J].移动信息, 2024, 46(1):135-137.

[4] 周颖.新形势下的网络信息安全运维[J].信息周刊, 2020(12):1.

[5] 马威风,冯波.大数据背景下企业运维数据治理研究与实践[J].网络安全和信息化, 2024(12).