

Research on the scheme of “level protection 2.0” for the network security of the application system of petrochemical enterprises

Lu Li

CNOOC Petrochemical Engineering Co., Ltd., Qingdao, Shandong, 266101, China

Abstract

With the acceleration of the information process, the application system of petrochemical enterprises is increasingly dependent on the network technology, and the network security problem has become an important factor affecting the operation of enterprises. In recent years, the network security “hierarchical protection 2.0” scheme, as an effective security management system, has been widely used in various industries. This paper deeply studies the implementation plan of “grade protection 2.0” in the application system of petrochemical enterprises, analyzes the main problems and challenges faced by the network security of petrochemical enterprises, combines with the characteristics of the petrochemical industry, and puts forward a specific solution based on the framework of “grade protection 2.0”. Through the optimization design of the risk assessment, system classification, network protection, data security and emergency response of the information system of petrochemical enterprises, this paper provides feasible technical support and implementation path for the network security protection of petrochemical enterprises.

Keywords

petrochemical enterprise; network security; grade protection 2.0; application system; scheme research

石化企业应用系统的网络安全“等级保护 2.0”的方案研究

李璐

中海油石化工程有限公司, 中国·山东 青岛 266101

摘要

随着信息化进程的加速, 石化企业的应用系统日益依赖于网络技术, 网络安全问题已成为影响企业运营的重要因素。近年来, 网络安全“等级保护 2.0”方案作为一种有效的安全管理体系, 已在各类行业中得到了广泛应用。本文深入研究了“等级保护 2.0”在石化企业应用系统中的实施方案, 分析了石化企业网络安全面临的主要问题与挑战, 结合石化行业的特点, 提出了基于“等级保护 2.0”框架的具体解决方案。通过对石化企业信息系统的风险评估、系统分级、网络防护、数据安全、应急响应等方面的优化设计, 本文为石化企业的网络安全防护提供了可行的技术支持和实施路径。

关键词

石化企业; 网络安全; 等级保护 2.0; 应用系统; 方案研究

1 引言

随着信息技术的飞速发展, 石化企业在业务操作、生产监控、数据分析等方面依赖的计算机网络和信息系统越来越多。这些信息系统的安全问题日益严重, 尤其是随着生产环境中涉及的设备和系统之间相互连接, 网络攻击、病毒感染、数据泄露等问题的威胁也在不断升级。网络安全不仅关乎企业的日常运营, 还直接影响到企业的核心竞争力、品牌形象和客户信任度。石化行业的网络安全防护更为复杂, 因为石化企业的应用系统通常涉及庞大的生产流程、敏感数据

和高风险的业务操作, 如何保障这些系统的安全, 避免网络安全事件带来的损失, 成为石化企业亟须解决的重要问题。

“等级保护 2.0”方案是我国在网络安全领域提出的一种基于等级保护的安全管理框架, 旨在通过分级管理, 提升信息系统的安全防护能力。该方案已广泛应用于政府部门、金融机构以及能源、交通等行业, 尤其对石化企业的应用系统安全起到了积极的促进作用。随着“等级保护 2.0”方案的进一步推进, 石化企业应当通过深入了解该方案的框架与实施步骤, 结合自身的具体需求, 建立起一套符合行业特点的网络安全保障体系。

本文的研究目标是探讨“等级保护 2.0”在石化企业应用系统中的实施方案。首先, 本文分析了石化企业在应用系统中的网络安全风险, 并阐述了“等级保护 2.0”方案在实

【作者简介】李璐 (1984–), 男, 中国河南郑州人, 本科, 中级, 从事网络安全研究。

际应用中的价值与意义；接着，提出了针对石化企业应用系统的具体实施方案，包括风险评估、系统分级、数据保护等关键环节；最后，本文结合石化企业的特点，提出了实施过程中应注意的问题与挑战。

2 石化企业应用系统的网络安全现状与挑战

2.1 石化企业应用系统的网络安全风险

石化企业的应用系统通常涉及生产调度、设备控制、物料管理、财务审计等多个核心业务环节，这些系统的正常运行对企业的日常运营至关重要。尤其是与生产设备、控制系统、监测系统等相关的应用系统一旦遭遇网络攻击或发生故障，可能会导致严重的生产中断、设备损坏，甚至环境污染，进而造成重大的经济损失和社会影响。因此，石化企业的网络安全工作必须从源头入手，严格防范各类安全风险，以确保企业运营的稳定和安全。

首先，网络攻击已经成为石化企业面临的主要安全风险之一。随着黑客技术的不断升级，网络攻击手段日趋多样化，DDoS攻击、恶意软件传播、勒索病毒等攻击方式可能危及企业网络的安全。特别是在石化企业，生产系统和控制系统的网络化程度较高，这些系统往往涉及工业控制网络（ICS）和监控系统，一旦遭受网络攻击，可能导致生产过程的中断、生产设备的损坏，甚至可能引发安全事故。攻击者不仅能够通过外部网络入侵控制系统，还可能通过内部网络渗透造成更严重的后果。例如，石化企业的监控系统一旦受到攻击，可能导致设备故障、生产停滞，甚至可能危及人员的安全。

其次，信息泄露是石化企业面临的另一个重大隐患。石化企业的内部数据传输频繁，涉及商业机密、生产数据、技术资料等敏感信息。如果这些信息被非法获取或泄露，可能对企业的市场竞争力、运营效率及品牌信誉造成极大影响。尤其是在高端技术领域，技术资料的泄露可能导致竞争对手通过抄袭、窃取知识产权等手段，损害企业的创新能力，甚至对国家能源安全构成威胁。为此，石化企业必须加强数据加密、访问控制和信息审计，防止信息泄露带来的潜在风险。

2.2 网络安全防护中的关键问题

尽管石化企业已经在网络安全方面投入了大量资金和技术，但在实施网络安全防护时仍面临一系列挑战。首先，石化企业的网络安全防护普遍缺乏统一的管理体系和标准化的安全措施。许多企业仍然停留在传统的网络安全防护模式下，采取单一的技术手段，如防火墙和入侵监测系统，而未能充分运用现代信息技术来进行有效的风险预测和系统防御。因此，网络防护策略往往不能适应快速变化的网络安全环境，导致系统容易受到恶意攻击和入侵。

其次，随着信息化程度的不断提升，石化企业的网络安全管理变得愈加复杂。信息系统的多元化、跨部门的协作

以及高度集成的技术环境，使得企业的网络安全管理变得错综复杂。很多系统之间缺乏良好的协调与整合，导致信息流动不畅，管理难度加大。同时，网络攻击手段和技术手段不断进步，黑客的攻击策略也日益复杂，面对这种复杂的安全形势，石化企业往往难以采取有效的防护措施，导致防护体系的漏洞频发。此外，企业的网络安全管理人员普遍缺乏足够的专业培训和实践经验，这使得企业在应对复杂安全事件时缺乏足够的应急能力。

3 “等级保护 2.0” 方案在石化企业中的应用

3.1 “等级保护 2.0” 框架与原则

“等级保护 2.0”是我国为应对日益复杂的网络安全威胁，针对信息系统安全提出的分级管理方案，旨在通过多层次的保护措施确保系统的安全。不同于传统的安全管理方式，等级保护 2.0 方案通过对信息系统进行分类、分级，为每一个系统设置合适的安全防护标准和措施，依据信息系统对社会、经济、国家安全的重要性及其所面临的安全风险提供定制化的保护策略。

在具体实施过程中，“等级保护 2.0”方案要求各类信息系统根据其数据的重要性、业务的复杂性和对外界的依赖程度等因素，划分为多个安全等级，并对每个等级的安全防护措施进行详细的规定。这些安全措施包括但不限于物理安全、网络安全、数据安全、身份认证、访问控制等，目的是防止恶意攻击、非法访问、数据泄露等风险。例如，对于涉及企业核心生产控制系统和敏感数据存储的高等级系统，要求采用更为严密的加密技术、更加复杂的身份认证机制以及更高强度的访问控制；而对于一般业务系统，则可以采取基础的防火墙保护和入侵检测措施，达到不同等级保护的目的。

该方案的实施并不仅仅依赖于技术手段的保障，还注重安全管理措施与技术防护手段的结合。通过建立完善的安全管理体系，制定清晰的安全责任分工和管理机制，确保信息系统在运行过程中能够始终保持高效、可靠和安全。

3.2 “等级保护 2.0” 在石化企业应用系统中的实施路径

针对石化企业的特殊需求，实施“等级保护 2.0”方案时需要充分考虑到行业特性、信息系统的复杂性以及不同生产线对信息安全的不同要求。为了高效落地该方案，企业应从以下几个方面着手：

风险评估与资产识别：实施“等级保护 2.0”方案的首要步骤是对石化企业现有信息系统进行全面的风险评估。通过识别关键资产，分析可能的安全威胁和风险点，评估系统在遭遇攻击时可能带来的损失，从而为系统分级提供依据。特别是对于核心生产系统和数据存储系统，需要重点评估其安全风险，并识别出关键的数据保护需求。

系统分级：在石化企业的应用系统中，信息系统通常

涉及多个业务环节与生产过程,因此对其进行分级管理显得尤为重要。企业需要根据不同系统的风险评估结果,结合业务的重要性与敏感度,对信息系统进行分类和分级。核心生产控制系统、企业管理系统、财务审计系统等应该被划分为高等级系统,而一般的辅助系统和办公系统则可以分为较低等级系统。每个等级的系统应配备相应的安全保护措施。

安全防护措施的设计与实施:根据不同等级的需求,设计相应的安全防护措施。对于高等级的系统,可以引入更为严格的数据加密、身份认证机制、多因素验证和严格的访问控制,以确保系统免受外部恶意攻击和内部滥用的威胁;对于低等级的系统,采取基础的防火墙、入侵检测和常规的系统日志审计等手段即可满足安全需求。

应急响应与恢复计划:信息安全事件的应对和系统恢复能力是保障网络安全的重要环节。石化企业需要为每个分级系统建立应急响应机制和灾难恢复计划。在系统出现安全事件时,能够迅速有效地进行处理,及时恢复系统的正常运行。应急预案的制定不仅需要涵盖事件响应流程、沟通渠道,还要明确责任分工、应急资源的调配与使用等内容。

持续监控与改进:信息系统的安全保障是一个动态过程,石化企业应当实施持续监控和定期评估机制。通过对系统进行实时监控和定期的安全检查,及时发现潜在的安全威胁和漏洞。利用漏洞扫描、风险评估、数据审计等工具,企业可以对系统的安全性进行定期评估并对其进行优化改进。安全管理不仅仅是一个初期的实施过程,更需要在日常运维中不断加强。

3.3 石化企业在实施过程中的挑战与对策

尽管“等级保护 2.0”方案为石化企业提供了一个切实可行的安全框架,但在实施过程中,仍然存在着一些挑战,尤其是在技术、人员和管理等方面。

技术人员短缺问题:由于石化行业网络安全技术人员普遍短缺,许多企业缺乏足够的专业人才来进行系统的安全设计和维护。为了应对这一挑战,石化企业需要加大对网络安全人才的培养和引进,提升技术团队的专业能力。通过建立培训机制,提升现有技术人员的安全防护能力和解决实际问题的能力。

系统集成与信息孤岛问题:石化企业的应用系统通常是由多个独立的子系统组成,各子系统之间的信息流动与协作较为复杂。如何在实施“等级保护 2.0”时,统一管理这些子系统,并确保全局层面实施有效的安全防护,成为一个关键问题。对此,企业应当通过系统集成和数据共享策略,确保各系统之间的协同工作,提高信息流通效率,同时避免信息孤岛现象。

安全威胁不断升级,需不断更新安全防护措施:随着网络安全技术的快速发展和黑客攻击手段的不断演化,石化企业面临的网络安全威胁变得更加复杂和多样化。为了应对这一挑战,企业需要加强与网络安全技术供应商的合作,及时了解并应用最新的安全防护技术,并对系统进行定期的漏洞修补和升级,确保防护体系始终处于最新状态。

4 结语

石化企业的网络安全问题越来越受到重视,尤其是随着信息化进程的推进,企业的应用系统面临的安全威胁也在日益增加。通过实施“等级保护 2.0”方案,石化企业可以有效提高信息系统的安全防护能力,减少网络攻击和数据泄露的风险。然而,实施过程中仍面临技术、人员、管理等方面的挑战,企业应根据实际情况不断优化安全措施和管理策略,确保信息系统的长期安全运行。随着信息技术和网络安全技术的不断进步,石化企业的网络安全防护能力将得到不断提升,从而推动整个行业朝着绿色、智能、可持续的方向发展。

参考文献

- [1] 石松.石化企业安全生产中智能控制系统的应用探讨[J].中国石油和化工,2024,(12):47-49.
- [2] 刘砚哲,田向煜,王薇.基于化工安全教育平台的危化品企业安全培训空间建设[J].化工安全与环境,2024,37(12):53-56.
- [3] 吕似蕴,李翰庭,刁旭,等.基于风险与脆弱性评估的危险化学品企业安全生产责任保险计算方法研究[J].中国安全生产科学技术,2024,20(S1):18-24.
- [4] 王树国.石化行业新型电力系统构建及再电气化发展综述[J].电气时代,2024,(11):28-32.