工程与管理科学
Engineering and Management Science
第 6 卷◆第 08 期◆版本 1.0◆2024 年
文章类型：论文|刊号（ISSN）：2705-0637(P) / 2705-0645(O)

浅谈工业生产行业的网络安全协同防御机制

商圣光
中国石化共享服务有限公司东营分公司
DOI：10.12238/ems.v6i8.8785

[摘　要] 工业控制系统是工业生产运行的基础核心，工业控制系统的网络安全直接关系到企业的生产安全、经济利益乃至国家安全。然而从行业和企业层面看，工控系统安全未形成定期的检测评估机制，制度标准缺失，评估隐患能力不足，无法全面、深入地发现存在的问题。因此，构建工业生产行业的网络安全协同防御机制，有效保护工业网络安全，成为了石油石化企业亟需解决的重要问题。
[关键词] 工业生产；网络安全；协同防御机制

A Brief Discussion on the Network Security Collaborative Defense Mechanism in the Industrial Production Industry

Shang Shengguang
Sinopec Shared Services Co., Ltd. Dongying Branch

[Abstract] Industrial control systems are the fundamental core of industrial production operations, and the network security of industrial control systems is directly related to the production safety, economic interests, and even national security of enterprises. However, from the perspective of the industry and enterprises, the security of industrial control systems has not formed a regular detection and evaluation mechanism, there is a lack of institutional standards, and the ability to assess hidden dangers is insufficient, making it difficult to comprehensively and deeply discover existing problems. Therefore, building a network security collaborative defense mechanism for the industrial production industry and effectively protecting industrial network security has become an important issue that petroleum and petrochemical enterprises urgently need to address.
[Keywords] industrial production; Network security; Collaborative defense mechanism

自 2010 年“震网病毒”事件被披露以后，工控安全问题开始引起世界范围的关注。2021 年 5 月，美国大型成品油管道运营商科洛尼尔管道运输公司遭到一个名为“阴暗面”（DarkSide）的网络犯罪团伙发起的勒索软件的攻击，再次向世界证明了工控安全的重要性和紧迫性。目前世界各国纷纷将工控安全问题提升到国家安全的层面，工控安全已成为信息安全领域研究的热点。因各行业的工业生产场景的特殊性和工控网络普遍存在的基础脆弱性，工业生产安全防线牵一发动全身，每个薄弱点可能会成为攻击行业、横向渗透的突破点。因此需要建立行业内的网络安全协同防御机制。

1、建立行业内的常态化联系机制

实现行业内协同抵御网络安全威胁，首先要建立常态化的联系和协调关系。定期组织会商，分析研判面临的主要威胁、可能遭受攻击的安全漏洞及危害后果，研究制定网络安全突发事件联合处置预案，做到预防在前、应变在先。还要深入研究网络防御协同机制体制建设面临形势和问题，探索网络态势的客观规律，了解行业内各企业的能力需求，研究制定应对措施，部署安排相关任务。

2、提升关键信息基础设施安全保护水平

参照《关键信息基础设施认定指南》，编制形成行业关键信息基础设施认定规则，确定支撑行业重要核心业务的网络设施、信息系统、工控系统等关键信息基础设施。在全面研究关键信息基础设施定级保护制度，深入分析关键信息基础设施技术、业务特点的基础上，对关键信息基础设施采取更有针对性的安全保障措施，确保关键信息基础设施的安全。

建设关键信息基础设施的网络安全防护和风险监测技术体系。建立边界保护机制，部署安全设备对边界进行安全访问控制及安全检测，保护关键信息基础设施内的物理连接和逻辑连接。对数据进行分级分类，重点保护关键信息基础设施的敏感信息，加强数据收集、存储、使用、加工、传输、销毁的安全保护措施。对关键信息基础设施安全保护开展自查工作，挖掘发现零日漏洞，通过整改和复测对安全问题进行修复，同时加强网络边界和主机层面的访问控制，确保系统平稳安全运行。对关键信息基础设施开展年度检测评估，根据检测评估发现的问题，制定安全建设整改方案并开展整改工作。

3、提升网络安全监测预警能力

建立以行业监管部门为主、企业为辅的网络安全监测预警模式。由企业针对行业重要信息系统和工控系统比较集中的全部重要信息系统、工控系统与关键信息基础设施进行重点监控，开展信息系统日常防护，定期组织开展安全检查，向行业监管部门上报入侵网络检测数据、网络环境数据、漏洞扫描数据等。行业监管部门利用网络安全相关数据，以及技术方面的优势，依托大数据等新一代信息技术，对海量数据进行人机结合侦测，通过行业沟通机制向企业提供行业相关网络安全情况的通报，实现一体化网络威胁防护机制。

搭建工业仿真环境，通过虚拟仿真技术模拟真实工业环境的网络、主机、流量和威胁，并接入真实工业设备和输入输出模块复现真实生产工艺流程。一方面，帮助用户完成重要信息系统网络安全测试、攻防演练、安全防护技术研究、教育培训等工作。另一方面，可以客观评估当前的网络安全风险，了解信息设备自身安全性能，提高技术人员的安全意识和安全技能，为企业网络安全防护方案提供有效验证。

4、提升工控系统网络安全防护能力

当前，大量工业控制系统被应用于企业生产过程中。从行业和企业层面看，工控系统安全未形成定期的检测评估机制，制度标准缺失，评估隐患能力不足，无法全面、深入地发现存在的问题。

应对照《工业控制系统信息安全防护指南》，深入分析工控系统安全现状，识别企业工控系统资产、威胁及脆弱性，进而认清风险、找出漏洞，对工控系统各项配置进行细致检查，评估工控系统风险发生概率和负面影响，从而制定有针对性的安全防控方案，构建覆盖安全软件选择与管理配置和补丁管理、边界安全、物理和环境安全、身份认证、远程访问安全、安全监测、应急预案演练、资产安全、数据安全、供应链管理等方面的工控安全防护技术体系。

行业各单位网络安全管理体系框架下，完善工控安全管理体系。明确工控安全防护的基本原则、管理职责和流程，形成工控安全建设和运维指导意见，规范防护思路、对象、措施、方法等，推动提升工控系统安全防护水平。

建立健全工控系统安全标准体系，包括安全建设标准、安全运行技术规范、安全评测指标方法等。安全评测指标分为管理类和技术类指标，安全管理类指标主要从安全管理制度、安全管理机构和人员、安全建设管理、安全运维管理四个安全域进行细化要求，建立控制项和评测控制点；安全技术类指标主要以工厂网络的过程监控层、生产管理层为研究对象，外加机房环境要求，建立控制项和评测控制点。

5、建立行业协同的网络安全应急处置机制

建立行业协同管控体系。吸收业务专家和网络安全专家成立专家咨询组，负责为决策提供咨询建议，建立协同管控机构；在行业监管部门的指挥下，发生重大网络安全事件时，协同管控机构负责应急处置的指挥决策和控制协调。

建立应急预案体系。针对可能发生的网络安全事件，从最复杂情况出发，分门别类制定完善各类应急预案。协同管控机构牵头，负责编制应对各级事件的总体规划及预案。

建立安全威胁通报制度。在协同管控机构领导下，行业依托现有信息化资源，构建稳定可靠、纵横贯通、全面覆盖、互联互通的通信联络和预警报知网络体系，及时通报情况，综合分析信息，实现信息共享，对各类威胁事件做到早发现、早预测、早处置。

建立应急处置协调机制。基于行业网络安全态势感知平台，研究形成行业网络安全监测与协同应急响应的措施和做法，增强行业协同的态势感知、分析研判、应急处置能力，实现联防联控。发生网络安全事件时，优先保障重要信息系统安全，最大限度降低危害程度。同时，组织专业力量，尽快恢复受损网络，保证信息系统的正常运行。

6、联合开展攻防技术和工具研发

推进网络安全技术研究和工具研制，丰富协同网络安全防御工具库。结合行业网络安全防御需求，利用电子、信息通信等领域企业的网络资源与技术优势，联合开展网络安全技术攻关，跟踪研究攻击机理，研制相关检测、监测、防御、追踪、溯源、反制等装备工具，形成体系化的协同防御、监听、攻击和反制能力，共同保护国家关键信息基础设施安全。建设行业共享网络安全靶场，为有关单位开展网络安全研究和演练提供平台，打造网络安全协同防御训练场，组织开展联合演习演练等活动。

7、加强网络安全人才培训

打造一支既懂网络安全又懂行业业务的队伍，建设符合当前网络安全需求的网络安全预备役队伍。针对需要，有组织有计划地采取岗位自学、集中培训等形式加强网络安全学习，提高人员素质。组织网络安全专项培训、比赛，磨练队伍人员能力，达到熟悉业务、增强技能、提高各级力量以及各级领导指挥、决策水平的目的。基于网络安全实验室和仿真基地等，开展网络安全攻防技术培训和演练活动，提升人员技能水平。

8、建立信息资源共享目录

开展行业信息资源共享的顶层设计。建立共享目录，研究信息资源共享方式、共享内容、产权保护、安全保密等规范和实施细则。加强关键信息基础设施合建共用，基于资源共享平台，实现资源共用共享。

搭建网络威胁情报共享平台，形成异构系统的网络安全威胁情报一体化共享机制。按照《网络产品安全漏洞管理规定》对于网络安全漏洞发现、收集、发布等活动的规定，行业应积极建立健全安全漏洞的发现、上报、收集、验证、修复等机制，接收公安部、CNCERT、知名网络安全企业等多种来源的威胁情报，对接 CNVD、CNNVD 等知名漏洞库。进而建设基于威胁情报的安全运营能力与威胁情报输出能力，实现网络安全威胁情报共享与联动响应。

9、建设行业网络安全管控平台

通过建设行业级网络安全漏洞库、网络安全态势感知平台及应急指挥平台，统一行业网络安全平台技术要求、数据和接口规范，聚合行业网络安全资源、信息、能力，依托网络安全平台、大数据和网络安全态势感知预警能力提升应急指挥与响应处置等能力。

行业网络安全管控平台的共性功能需求包括行业态势感知信息汇聚、威胁情报整合共享、网络安全通报管理、应急响应协同，以及攻防人员和漏洞管理等功能。

行业态势感知信息汇聚基于目前各企业具备的网络安全态势感知监测预警平台和数据，实现行业级态势感知信息的汇聚，对整个行业网络运行状态、网络流量、用户行为、网络安全事件等进行动态监测分析，达到实时态势分析和监控攻击行为与安全事件，传递告警监控信息，确保对威胁及时发现、及时防御、及时处理。

威胁情报整合共享规范行业威胁情报数据格式，整合各单位局部攻击信息资源，构建完整的攻击链，降低情报搜集成本，对整合的情报进行聚合分析，及时利用其它网络中产生的高效威胁情报提高防护方应对能力，对抗不停进化的安全威胁，实现网络安全威胁管理和应用的自动化。

网络安全通报管理提供了不同层级系统间，统一的威胁信息上传下达格式，主要用于向下发信息安全月度通报、信息安全紧急通报、信息安全整改通知书，各单位上报信息安全整改通知书、信息安全紧急通报。

应急响应协同针对网络安全联动处置需求，主要是根据监测预警情况，监测网络安全事件行为，根据安全事件分类分级标准确定安全事件级别。

漏洞管理是对行业的主要漏洞信息的管理和维护，包含漏洞管理、任务管理和扫描器管理等功能模块。漏洞管理提供系统漏洞数据的查询展示和漏洞处置等功能，任务管理提供漏洞扫描任务管理和导入漏洞报告功能，扫描器管理提供扫描器新增编辑等管理功能。

[参考文献]

[1]赵刚. 网络安全数据治理在石油石化行业中的关键作用与挑战[J].中国石油和化工标准与质量，2024，44（07）：56-58.

[2]网络安全态势感知技术探讨与行业实践[J]. 网络安全和信息化，2024，（04）：43.

[3]彭轶华，刘明远，郜帅，等. 轨道交通行业网络空间安全现状与未来发展[J]. 中国工程科学，2023，25（06）：137-149.

[4]王科，刘宇航，侯慧，等. 化工行业工业控制网络安全防护的探索与实践[J].中国石油和化工标准与质量，2023，43（12）：69-71.

[5]霍朝宾，武蕊. 石化行业工控系统网络安全防护体系建设探析[J].网络安全与数据治理，2022，41（08）：55-60.