文章类型：论文|刊号（ISSN）：2737-4505(P) / 2737-4513(O)

工控网络安全监测方法与运用分析

景凯鹏
晋能控股装备制造集团寺河煤矿二号井
DOI:10.12238/etd.v6i2.12965

[摘　要] 在工控网络管理中,有效运用各类安全监测方法,可以进一步保障工控网络安全。基于此,本文从工控网络概述展开论述,分析了实时监测网络流量、实时监测工控设备、定期评估安全风险、部署使用入侵检测系统这几项工控网络安全监测方法,并提出了完善配套软硬件设施、推进技术团队建设、健全配套技术应用制度这几个工控网络安全监测方法运用策略,实现了对工控网络安全监测的探讨,希望能够为工控网络安全监测工作的开展提供一定的参考。
[关键词] 工控网络；网络安全；安全监测
中图分类号：TN711　文献标识码：A

Analysis of Monitoring Methods and Applications for Industrial Control Network Security

Kaipeng Jing
Jinneng Holdings Equipment Manufacturing Group Sihe Coal Mine No.2 Well, Jincheng City
[Abstract] Effective use of various security monitoring methods in industrial control network management can further ensure the security of industrial control networks. Based on this, this article discusses the overview of industrial control networks, analyzes several methods of industrial control network security monitoring, including real-time monitoring of network traffic, real-time monitoring of industrial control equipment, regular assessment of security risks, and deployment and use of intrusion detection systems. It also proposes strategies for improving supporting software and hardware facilities, promoting technical team building, and improving supporting technology application systems. This exploration of industrial control network security monitoring aims to provide some reference for the development of industrial control network security monitoring work.
[Key words] industrial control network; Network security; safety monitoring

引言

工控网络属于一种专门应用于工业领域的综合性集成网络,其通过服务于各类涉及工业作业的信息技术应用,可以支持工业领域的信息化、智能化发展。但工控网络的应用也受信息安全因素的制约,所以,需积极运用合适的安全监测方法,对各类潜在的安全风险因素予以排除,从而提高工控网络的应用效果。

1 工控网络概述

工控网络,即工业控制网络或工业网络,其融合了计算机技术、现场总线技术、通信技术、多媒体技术等多种信息技术,现阶段专门服务于工业自动化和控制系统的运作,并能够通过实现设备之间的通信和数据交换,达到生产过程监控、控制和管理的信息化、智能化运作。就目前来看,一套完整的工业网络可以跨地区进行信息与控制集成,并可以支持涉及LAN、WAN、现场总线等不同网络的互联。整体来看,工控网络的功能聚焦于实现工业作业全范围内的信息资源共享以及与外界的信息沟通,而这一功能的运作主要依托于两个核心的工控网络结构部分,即信息网络结构、控制网络结构。其中,信息网络结构位于工控网络的中上层,负责处理工业控制系统管理与决策信息,而控制网络结构则位于工控网络的中下层,负责处理控制现场实时测控信息[1]。

而工控网络对生产过程自动化、设备远程监控、数据采集与传输等智能化功能的有力支持,使其广泛地应用于制造业、能源电力、石油化工等多个工业行业领域,极大地支持了工业领域的发展。但工控网络本身具有一定的开放性,且面临着控制协议安全缺陷、不正确使用引起安全漏洞等风险因素,这使得对其的安全监测具有重要意义。

2 工控网络安全监测方法

2.1实时监测网络流量

流量监测是识别异常行为的有效途径。在流量监测中,通过对流量数据予以分析和处理,可以得到数据包大小、传输速率等

流量特征,而网络流量的正常与否均能够反映到这些特征上,为潜在恶意行为的识别提供参考。在此过程中,可以采用SNMP定期从交换机、路由器等网络设备中提取流量数据,用于分析流量特征,也可以考虑采用流量镜像技术,通过将网络中的数据包复制一份到指定的监控设备上,再对这些数据包进行分析,即可获取到实时的网络流量信息,用于监测异常行为,以便于及时发现和排除工控网络中的安全风险因素。在流量监测中,还可以使用NetFlow和sFlow技术,对网络流量予以实时、高精度的采集,为流量监测提供支持。为了更高效地获取流量特征,在监测工作中,还要积极运用Tcpdump、Wireshark等命令行工具,对网络数据包予以实时捕获和分析,再使用Cacti、Nagios等监控工具,将网络流量数据以图表、趋势图等方式展现,以更有效地识别异常行为,实现安全监测。此外,如果有条件,也可以使用基于人工智能的流量监控系统,并通过构建机器学习或深度学习模型对网络流量进行实时分析,以识别安全风险因素。但需要提前对大量标注好的样本进行训练,让模型得以有效识别正常流量和异常流量之间的差异,以便于其能够在检测到与正常流量模式不符的数据时及时输出报警信息[2]。

2.2实时监测工控设备

在工控网络运行中,配套的设备故障损坏是影响网络安全的重要因素,所以,在安全监测中,也应将此因素纳入考虑范围,并针对电机、电表、传感器等所有工控设备进行实时监测,以确保其能够在安全参数内运行,规避硬件层面的安全风险。在工控设备的监测上,可以运用机器学习、自然语言处理、深度学习等AI技术,构建出一个智能安全检测平台,专门负责监测工控设备的参数变化,并对异常的参数变化予以识别,支持管理者及时采取处理措施,保证工控设备的安全、稳定运行。在此过程中,需要先将设备状态监测传感器安装在工控设备上,用于获取设备的运行参数,然后利用上述AI技术,集成多种数据分析算法,构建工控设备参数实时处理、分析模型,再对模型予以训练,使其能够识别异常参数。之后,即可将其部署到工控网络中,用于实时监测、预警异常参数情况,以便于管理者及时采取处理措施,保证工控网络的安全运行[3]。

2.3定期评估安全风险

定期的安全风险评估是安全监测中的一项重要工作内容。在监测中,通过此环节可以有效识别工控网络中的弱点和潜在漏洞,以便于及时采取相应的补救措施,保证工控网络的安全。在安全风险评估中,需要先明确评估的范围、对象和边界,再分析潜在攻击者可能利用的威胁,并寻找工控系统中存在的安全漏洞,然后基于此,评估工控网络面临的安全风险。在此过程中,应采用定量风险评估、定性风险评估相结合的方式,对工控网络的安全状态予以整体评估。其中,定量评估可用故障树分析、事件树分析、贝叶斯网络等分析方法,定性评估则可运用德尔菲法、层次分析法等,由此得出更加准确、具体、有指导意义的评估结果。在评估工作中,也可以利用基于需求工程的威胁建模进行评估,并通过对ICS网络中的系统和设备进行模型化,描绘出系统中的威胁,得出评估结果,同时还可以考虑使用攻击模拟,对网络中存在的漏洞和弱点予以识别评估,为后续的安全防护工作提供更具参考价值的评估结果。此外,在安全风险评估中,除了评估网络本身的安全性以外,还要对各类现有的安全防护措施的执行效果予以评估,由此进一步收集工控网络安全状态信息,为后续的工控网络安全管理工作提供参考。在安全风险评估结果的输出上,还要注意,尽量将风险等级分为高、中、低等不同级别,以支持管理者优先处理高风险因素,更好地保障工控网络安全。

2.4部署使用入侵检测系统

在工控网络的外部边界区域设置入侵检测系统,不仅可以实现对通过网络的所有数据包的实时监视,还可以配合防火墙阻止未经授权的访问和攻击,提高安全监测工作的效果。在此过程中,还可以考虑部署一套基于主机的入侵检测系统,用于监视用户和文件访问活动,识别异常行为,同时,也要积极运用分布式入侵检测系统,以适应大规模工控网络的安全监测需求,从而监视包括网络设施本身,以及配套主机系统的整个网络环境,进一步提高安全监测工作的效果。在部署和使用上,应注意将入侵检测系统部署在网络边界、内部重要节点和敏感区域等工控网络的关键位置,借此全面监控和识别来自不同方向的恶意行为,同时还要根据实际需求选择合适的部署方式。一般来说,如果针对攻击行为进行监测,就应采用旁路部署,若需要配合其他防护措施,对攻击行为予以实时阻断,则可采用直路串接。在此过程中,还要注意,需根据实际情况和需求,合理调整入侵检测系统的检测规则、警报级别、阈值等参数,以保证监测结果的准确性,同时也要为检测系统配置IDS传感器,支持其顺利地接收和处理网络流量和数据包。待部署完毕后,为了提高入侵检测系统在安全监测工作中的使用效果,还要对系统予以测试,并根据测试结果开展相应的优化和调整,深入优化系统的检测效率和准确性,提升工控网络安全监测工作水平。

3 工控网络安全监测方法运用策略

3.1完善配套软硬件设施

上述各项安全监测方法的应用均需要依托于配套软硬件设施的运作,所以,为了更好地支持安全监测方法的运用,还要推进配套软硬件设施的健全建设,为工控网络的安全提供保障。在配套软硬件设施建设中,应当优先选择经过市场检验、稳定可靠的软硬件产品,而且在软硬件架构设置上,需充分考虑维护方面的需求,以便于后续更好地借助运维工作,保持软硬件设施的稳定运作,让各类安全监测方法能够顺利发挥效能,同时也要考虑到未来业务的发展和技术的更新,尽量选择扩展性良好的软硬件设施,支持安全监测方法的应用升级。

就目前来看,工控网络安全监测所需的硬件通常包括VPN设备、网闸、运维堡垒机等,而软件则涵盖漏洞扫描软件、集中安管平台等,数量较多,加之工控网络可能存在规模较大的情况,所以,配套软硬件的配置架构也比较复杂。为此,在软硬件设施配置上,需要先做好需求分析,并根据工控网络运行的安全需求

和监测目标，明确具体的软硬件设施类型和数量，再基于此，选择性能好、有扩展性、配置高的软硬件产品进行采购，然后即可立足于对可维护方面的考量，按照厂商提供的部署指南，将软硬件设施部署到工控网络中。之后，还要对配置好的软硬件设施予以测试和验证，确认无问题后，才能将其投入使用。此外，也要注意做好定期的运维工作，并及时修复、更换有问题的软硬件设施，更好地支持上述各类安全监测方法的有效运用，提升工控网络安全作业水平。

3.2推进技术团队建设

上述各项安全监测方法的应用都需要专业的技术人员予以操作、部署和维护，所以，为了保证安全监测工作的顺利开展，还要积极推进配套技术团队的建设，以支持安全监测工作的高质量开展。在技术团队建设中，需设置网络安全分析师、安全工程师等多元化的团队角色，并招聘和培养合适的人才担任相应决策，以支持上述多样化，且涉及多种信息安全细分专业的安全监测工作的开展。在此过程中，可以采用线上线下结合的方式开展招聘活动，以多渠道吸纳优秀的技术人才，同时还可以考虑与高校建立合作，共同推进人才定向培养，以获取充足的人才储备。但在此过程中，需注意，要定期开展人才市场调研，并根据调研结果合理调整薪资待遇，增强岗位的吸引力，从而更好地吸纳优秀人才，推进团队建设。

在团队建设中，也要建立有效的沟通和协作机制，并运用即时通讯软件、项目管理工具等现代化工具，支持团队内部沟通和交流，同时结合定期的团队会议和讨论，持续强化团队整体的效率和协作效果，支持各类安全监测工作的高质量开展。此外，还要积极推进人才培训，并与安全厂商和专家建立合作伙伴关系，共享相关的技术知识、信息，然后设计出相应的培训内容，借此不断更新团队的知识储备，强化其对安全监测工作的支持能力，同时也要设置线上化、移动化的培训模式，通过将培训内容录制为视频，或整理为电子文本，让团队成员能够随时随地的用手机移动端或PC端查看、学习培训内容，推动其专业能力水平的提升。在此过程中，还可以考虑组织定期的培训考核，检验培训效果，并针对技术人员在专业能力上薄弱点，及时调整培训内容，进一步推动团队整体专业能力的发展，为各项安全监测方法的有效落实提供支持。

3.3健全配套技术应用制度

为了进一步规范安全监测方法的应用，还要健全配套技术应用制度，以确保监测方法的准确应用，从而更好地维护工控网络的安全。在制度建设中，需先根据所用的安全监测方法，制定详细的安全监测流程，明确数据采集、分析、报警、响应和处置等环节的技术操作标准和要求，再基于此，结合工控系统的实际情况，制定出具有针对性、指导性的技术应用制度，而且需在制度条款中，表明各级人员的安全职责和权限，有效地规范技术人员的操作行为，保证监测方法的应用效果。在此过程中，需建立安全审计和评估制度，对各类安全监测技术方法的应用予以监督检查，并应根据工控网络的安全运作需求，制定出具体详细的审计、评估制度条款，指导管理者规范化、标准化地落实各项技术应用管理监督工作，从而确保各项安全监测技术方法的准确运用。

4 结论

综上所述，工控网络安全监测工作对于工业信息化、智能化作业的稳定开展具有重要的意义。在安全监测工作中，应当立足于实际情况，采用多样化的监测方法，并从设施、人员、制度等方面做好保障措施，支持安全监测工作效能的充分发挥，提升工控网络安全作业水平。

[参考文献]

[1]王海达,杨龙保,胡传超.流域集控中心工控网络节点安全态势感知方法探析[J].数字技术与应用,2025,43(02):77-79.

[2]刘慧芳.工业控制系统网络安全应急响应模型的研究和应用[J].工业信息安全,2025,(01):74-79.

[3]张兴时,颜诗羚.基于改进Markov算法的工控物联网安全态势感知方法[J].智能物联技术,2025,57(01):148-152.

作者简介：

景凯鹏(1989--),男,汉族,山西晋城人,大专,从事安全仪器监测研究。