工业互联网安全监测及态势感知探析

邹少军
江门职业技术学院 广东 江门 529090

【摘 要】工业互联网是“第三张网”，其开放、跨域、互联的特点，给工业行业带来了更多的发展机遇，但同时也造成了一些信息安全挑战，必须要得到重视。基于此，文章就工业互联网安全监测及态势感知问题展开探析，先对工业互联网存在的安全风险进行阐述，然后从态势感知技术角度入手，进一步研究如何更好地落实安全监测，让安全态势感知核心技术得到更好的发展。

【关键词】工业互联网；安全监测；态势感知；可视化

引言

大数据、物联网、5G、人工智能等新一代信息技术推动着工业互联网在能源、交通、电力、智能制造等关键领域数字化升级，工业互联网日趋信息化和智能化，开放、跨域、互联的特点也使工业互联网面临严峻的安全形势，因此建立协同的工业互联网安全监测与态势感知平台，应用多种安全技术手段，增强工业互联网安全技术支撑能力，提升隐患排查、攻击发现、攻击溯源和应急处置等技术能力，为国家工业提供安全的业务数据源和技术支持。

1 工业互联网面临的安全风险

工业互联网出现后，让工业产业链的发展能力得到答复度提高，但也带来了一定的危险，如 2016 年以色列电力系统网络受到大规模攻击，导致当地政府关闭了大量运行中的核心计算机，又如 2017 年 Wannacry 勒索病毒导致国内部分工业、能源企业的正常运行受到影响，一些企业的生产活动被迫中断，无独有偶，2018 年变种 Wannacry 勒索病毒攻击了全球最大的代工芯片制造商台积电，直接损失高达 13 亿元，由此可见，加强工业互联网的安全保障工作非常重要。工业互联网安全风险较为特殊，具体包括以下几种风险：

第一，设备风险。工业互联网控制着大量的设备，包括智能空调、智能冰箱等终端，这其中不乏一些体积较小、计算能力有限、缺少安全机制的设备，很容易被入侵。比如，存在安全问题的设备连接到工业互联网中，会导致这些采用嵌入式技术的物联网终端设备被利用，进而造成僵尸网络问题，甚至会引发 DDoS 攻击。

第二，控制风险。工业互联网中最为关键的就是控制技术，如 PLC、SCADA、DCS 等，都属于控制系统。这些控制系统被广泛应用在市政、轨道、交通、电力等基础设施行业，承担着工业生产的重要任务。尤其是 TCP/IP 这一以太网技术大面积推广后，工业控制系统可攻击面也随之增加，漏洞数量逐年提高，必须要得到重视。

第三，网络风险。这一风险主要指的是网络信息数据传输过程中产生的安全问题，近几年来出现了很多全新的公共工业互联网，为新的网络攻击提供了条件，如 Handle 等标准标识解析系统的应用，在无形之中加重了工厂通讯网络的安全防护难度，木马病毒、蠕虫病毒、勒索病毒等都可以向工程内部蔓延。

第四，平台风险。工业互联网平台中大部分属于边缘计算技术，包括工业控制系统、工业机器人、物联网终端的核心数据，尤其是大量设备和系统在接入后，让工厂内部的安全风险有了向外扩散的机会，最大程度提高了安全防护难度。另外，虚拟化技术的使用，进一步强化了平台的脆弱性，增加了攻击渠道，常见的风险问题包括：虚拟机逃逸、跨虚拟机侧信道攻击等。比如，现阶段，很多工业互联网平台都采用了 PaaS 层核心架构以及 CloudFoundry 和 Docker 等开源技术，这些技术很可能为病毒等网络攻击留有“后门”，增大安全风险。

第五，数据风险。在工业生产过程中会产生大量的数据，这些数据的采集、处理、存储、传输和使用都关系到最终的工业质量，必须要得到重视，仿真测试数据、现场生产数据、运维管理数据、供应链数据等得到重点关注，如果发生篡改或者窃取事件，会对工业生产造成严重的负面影响，严重的情况下，还会影响到工厂内工人的生命安全。

2 工业互联网安全监测及态势感知技术分析

由上可知，工业互联网的存在让大量的设备和系统得到一体化发展，但同时也加大了安全防护难度，攻击路径增加。大数据和云计算环境下，数据安全风险与日剧增。工业互联网是一种新型技术领域，安全产品有限，防护能力相对较弱，加强对工业互联网安全监测及态势感知的探究，全面落实核心技术，具有至关重要的意义。

从当前工业互联网的发展现状来看，找出一个高效率、高精确度、高监测性能的安全威胁识别方法势在必行。层次化网络安全威胁态势量化监测方法，在分析网络内部威胁频率的基础上，针对不同网络模块和网络中的威胁指数展开分析，高质量完成实际。其通过构建网络预测模型、网络威胁函数以及主机风险指数以及主机重要性权重函数，计算分析最终权重值计算结果。总的来说，层次化网络安全威胁态势量化监测方法是将工业互联网风险指数和重要性函数进行比较分析，最终得到量化监测结果。首先，建立监测模型。按照工业互联网中不同的层次进行划分，实现自上而下、先局部后整体、横向关联等策略开展监测工作，建立形成监测模型。该监测模型以 IDS 报警和漏洞扫描结果为主要数据，对工业互联网安全威胁进行监测，实现量化分析，在这个过程中，需要确保此监测方法可以对每个主机服务器的每个数据进行分析，完成安全性综合评定。为了保证监测结果符合合理性标准，确保得到的威胁指数准确性，适当增加了威胁严重程度，以此避免出现特殊事故时，出现计算错误。采用定时监测的方式，在晚 12 点 – 早 8 点、早 8 点 – 晚 6 点、晚 6 点 – 晚 12 点这三个时间段进行划分，以此保证可以获得足够的分析数据。通过数据的扫描处理实现分析。在实际计算过程中，各层次的威胁程度指数、重要性权重和网络宽带占有率都要得到确定，并且排除无效攻击，保证监测结果的准确性，对网络宽带占有量进行测定，并且手机服务器上的动态数据，作为服务和主机重要性权重的确定依据。只有保证上述内容得到全面的落实，建立形成科学合理的模型，才能够对整个安全链条进行监控。在此基础上，建立形成的层次化网络安全威胁态势量化监测方法可以让管理人员及时掌握管理动态，并且辅助其制定出相应的安全策略，确保整个系统安全。

在工业互联网中不仅要落实安全监测，还要完善态势感知，以此将工业互联网中存在的风险降至最低。在态势感知体系建设过程中，主要分为实时感知和可视化展示，在体系建设过程中，常见的核心技术包括：在线监测技术、蜜罐仿真技术、网络流量分析技术、工业企业侧探针技术。借助上述五种核心技术，使用 Docker、Hadoop、Spark、Flink、HBase、Elastic Search、Neo4j、Tensorflow 等组件，让先进的云计算和海量数据处理技术得到真正的应用。从实际应用效果来看，成功拦截数十次木马病毒入侵，并且实现了成功的溯源分析。工业企业在利用这一项目系统后，可以有效降低安全运维成本，提高安全质量，支持 50 多种数据建模模型、20 多种工业场景模型和机器学习自主建模，能够让网络安全能力得到最大程度的提高。

3 结束语

综上所述，工业互联网和工业生产之间有着无法分隔的关系，互联网技术的融入不仅可以提高生产效率，也可以降低成本。但工业互联网的出现打破了传统的制造环境，让病毒、木马和高级持续性威胁等网络攻击有机可乘。强化工业互联网安全监测及态势感知，全面落实态势感知核心机制，为产业发展提供参考。

【参考文献】

[1] 刘峰 . 网络安全态势感知和应急处置平台解决方案 [J]. 信息技术与标准化 ,2018(009):16-18.
[2] 傅扬 . 国内外工业互联网安全态势和风险分析 [J]. 信息安全研究 ,2019,5(008):P.728-733.
[3] 张玫 , 曾彬 , 朱成威 . 工控系统安全监测及溯源系统的设计与实现 [J]. 信息技术与网络安全 ,2019,38(01):14-19.