

数据驱动工业信息安全防护

吴力

天津商业大学 天津

【摘要】 在传统模式下，所构建的信息安全防御体系会将网络边界以及主机防护作为关键，但是随着人工智能等现代化技术的发展以及在工业行业中的普遍应用，如果仍然沿用传统信息安全防御体系将很难处理出现的问题，从某种角度来说，提高了出现工业信息安全问题概率。需要相关人员加大力度进行探究，借助于数据驱动提高工业信息安全防护效果。

【关键词】 数据；工业信息；安全

【收稿日期】 2022 年 9 月 10 日

【出刊日期】 2022 年 12 月 9 日

Data-driven Industrial Information Security Protection

Li Wu

Tianjin University of Commerce, Tianjin, China

【Abstract】 In the traditional mode, the information security defense system constructed will take the network boundary and host protection as the key, but with the development of modern technology such as artificial intelligence and the common application in the industrial industry, it will be difficult to deal with the problems that arise if the traditional information security defense system is still used, which, in a way, increases the probability of industrial information security problems. Relevant personnel need to make more efforts to explore and improve the effectiveness of industrial information security protection with the help of data-driven.

【Keywords】 Data; industrial information; security

工业信息安全是推动我国工业发展，增强我国整体实力的关键措施。近些年来，随着工业数字化的进一步发展，工业控制系统在应用过程中安全问题频发，需要应对诸多新挑战。因此，相关工作人员要将大数据等现代化技术作为依据，打造完善的工业信息安全产品体系，为工业控制系统的稳定应用提供保障。

1 传统模式下工业信息安全防护体系存在的问题

在传统模式下，所构建的工业信息安全防护体系是由防火墙、杀毒软件以及入侵检测等产品构成的，能够抵御一定程度上的安全威胁。但是，随着信息化技术水平的提升，工业信息安全防护体系需要应对更加严峻的信息安全问题，已经无法满足工业企业进一步发展需要。可以将传统模式下工业信息安全防护体系存在的问题总结为以下几点内容：

1.1 APT 攻击频繁

APT 攻击主要是指借助于精准程度较高的军事级数字武器进行打击。特征较为明显，可以被总结为：能够锁定目标、攻击手段多样、检测难度较高、持续时间比较长等，传统安全防御体系很难应对这一攻击^[1]。

1.2 传统安全边界逐步减弱

随着信息技术水平的提升，IT 技术和 OT 技术的联系更加紧密，网络边界的安全性明显减弱。在传统模式下，所构建的安全防护体系会将边界防御作为关键，但是随着云计算以及物联网等现代化技术的发展，形成了较多网络场景。在接入和访问网络时，对其移动性有了新的标准，能够使网络安全边界拓展到企业外部，改变各个工业厂区相互独立的现状。

1.3 出现了多种不同攻击技术

新型攻击技术的出现和应用,使传统安全防线受到了明显冲击。比如说,借助于 0 day 漏洞躲过 IDS / IPS 的漏洞利用攻击,会使用过加密、加花、加壳等不同类型的病毒攻击安全防护体系,导致安全防护体系已经难以抵御病毒、黑客的入侵。

2 数据驱动下的工业信息安全防护

工业信息安全的实质在于攻防对抗,需要确保其处在动态平衡状态下,管理水平、人才专业素养、技术实力以及基础设施是否完善等都会对于工业信息安全性产生影响。而传统模式下的工业信息安全是将互联网技术作为依据获得的发展,较为关注防护。虽然可以为提高当前安全防护水平提供一定条件,但是却并不具备应对 0 day 漏洞攻击或者是 APT 攻击能力,难以达成预期防护目标^[2]。

IT 信息安全行业近些年来出现了明显变化,形成了更多现代化思维与手段。信息安全工作人员要将数据驱动安全作为基础,灵活应用大数据、人工智能等技术改善出现的问题,达成工业信息安全防护目标。在数据驱动下工作人员可以从以下几点出发开展工业信息安全防护:

2.1 使用工业威胁检测技术

威胁情报是将云端中所存储的大量工业数据作为支持的,可以借助于数据搜集、处理、加强数据之间的联系、明确优先级、格式化等操作形成。威胁情报会借助于统一格式来明确多项攻击特征。基于威胁情报发展而来的工业威胁检测技术可以明确工业控制系统的特征以及各项信息的联系,并以可视化的方式进行呈现。这一技术不但可以及时发现威胁作出处理,还能够加强各部门的衔接,达成协同防护目标,延长攻击者进行攻击需要花费的时间,增加其成本投入。这一技术可以从源头出发找出攻击者,帮助企业解决出现的安全问题,为企业的健康、长远发展提供保障。

2.2 运用工业态势感知技术

大数据背景下,出现了更多现代化技术,为工业企业信息安全提供了技术条件,能够集中管控工业行业的数据资料、设备应用情况以及外部数据等,使工业大数据技术和工业云形成密切联系,在搜集本地数据的同时了解云数据,并从多个角度出发进行处理、应用。工业企业在开展研发、设计、生产、销售等工作时,要借助于大数据技术进行动态监督

管控,并有针对性的作出整改,打造出能够适应企业现实需求的设备、信息与软件。将大数据处理作为依据的工业态势感知技术已经变为了搜集工业大数据、分类存储以及对于资产进行控制的重要手段,能够满足人们的可视化需求,精准分析发展过程中可能会出现风险并进行防控^[3]。

2.3 打造完善的工业信息安全防护体系

考虑到功能层次、数据以及威胁情报流向,可以将工业信息安全产品体系划分为防护监测阶段、安全运转阶段以及态势感知阶段。这三个阶段的功能是不同的,可以明确数据、指令、威胁情况流转情况,达成协同联动目标^[4]。

第一,防护监测阶段。防护监测工作处在安全防护体系最底层,一般会借助于相关网站、防火墙、软件、评估道具等开展防护工作。这一产品可以对于出现的不同类型数据进行搜集、汇总,并接收上级部门的指令,开展简单分析。

第二,安全运营阶段。安全运营阶段是安全防护体系的关键构成,可以在工业企业内部开展各项工作,及时感知工业信息安全问题,并进行预警,统一管控。这一产品是由安全运营中心、云安全管理平台构成的,要在威胁情报利用技术、安全可视化技术、大数据技术支持下开展各项工作。

第三,态势感知阶段。态势感知阶段处于产品体系的最顶端,可以深度挖掘数据价值、进行情报搜集,打造完善的威胁情报库。这一类型产品一般是指威胁情报库和工业态势感知平台,在大规模工业企业以及政府部门较为常见,可以对于主要工业企业发展情况进行安全管控^[5]。

安全服务人员在开展工作时,要借助于威胁情报分析会对于工业企业产生威胁的内容,并进行调查和溯源工作,分析这一企业是否被病毒所感染,并有针对性的进行紧急处理。除此之外,还需要应用软件对于主机进行防护,避免未知程序、木马、病毒的入侵,确保主机可以稳定运营。除此之外,还可以借助于可视化技术将威胁事件和企业业务相关联,借助于态势感知,以图形方式呈现可能会产生的风险,使其更加直观,为后续的安全防控工作顺利开展提供支持,确保信息处在安全状态下。

总而言之,在传统模式下所用的工业信息安全会将攻击的某一时刻作为关注重点,难以从整体

角度出发分析被攻击情况。而对于新型安全体系进行应用能够改善传统安全技术在实际应用中出现的问题,从实质上来看,其是将数据作为依据的,能够借助于大数据系统全面分析可能会产生的威胁以及威胁发展情况,追溯来源^[6]。

将传统信息技术和新型工业信息安全技术相结合,可以提高工业控制系统的安全程度。但是,在对于这一工业控制系统进行应用时,仍然要坚持将人作为核心,确保工业运转的安全性。需要注意的是,工业控制企业的安全威胁具有较强不确定性,借助于这些技术很难预防全部的安全隐患。需要在关注工业大数据态势感知和工业威胁情报技术的基础上,确保以人为本原则可以被落到实处。在开展工业安全体系建设时,要将人作为核心,构建安全技术体系以及业务体系,加强人和技术的衔接,打造完善的安全生态。除此之外,还需要将事前的风险防控、主动进行防御以及在结束后开展的取证工作相衔接,确保工作人员能够按照流程,有针对性的开展各项工作,达成综合防御目标^[7-9]。这从某种角度来说,可以使安全防护体系更加符合企业现状,提高工业信息安全程度。

3 总结

根据上文来进行分析,在打造数据驱动下的工业安全体系时,要将数据作为前提,分析、判断可能会产生的安全隐患,并将大数据等现代化技术作为支持,制定适宜措施进行安全攻防,进而确保工业企业能够稳定运营,获得更好的发展。

参考文献

- [1] 张运锋. 数据驱动的工业过程故障诊断方法研究[D]. 武汉理工大学, 2021
- [2] 刘祎, 王玮. 工业大数据时代技术示范性研究综述与未来展望[J]. 科技进步与对策, 2019, 36(20)
- [3] 周明, 吕世超, 游建舟, 等. 工业控制系统安全态势感知技术研究[J]. 信息安全学报, 2022(002):007.

- [4] 王秀英. 工业控制系统的信息安全防护体系分析[J]. 电子技术(上海), 2022(002):051.
- [5] 赵梦蝶. 模型与数据相结合的工业信息物理系统风险评估方法研究[D]. 华中科技大学, 2019
- [6] 黄开兴. 数据与模型驱动的工业信息物理系统动态信息安全防护方法研究[D]. 华中科技大学, 2018
- [7] 刘戈. 数据挖掘技术在工业信息化中的应用研究[J]. 现代工业经济和信息化, 2021.
- [8] 孙飞. 工业互联网信息安全问题及防护技术分析[J]. 中文科技期刊数据库(文摘版)工程技术, 2021(8):2.
- [9] 郭庆, 宁玲玲. 可视化优化技术在工业控制系统入侵检测中的研究与应用[J]. 2021.
- [10] 王弢. 数据驱动工业信息安全防护[J]. 中国工业和信息化, 2021, 000(008):P.32-36.
- [11] 王弢, 崔君荣. 基于数据驱动的工业信息安全防护[J]. 微型机与应用, 2018, 037(006):3-5.
- [12] 刘洪太. 数据驱动的软件可靠性模型在石油工业信息系统中的应用[J]. 石油工业技术监督, 2017, 33(11):4.
- [13] 张雷. 基于数据驱动的复杂工业过程软测量方法研究与应用[D]. 湖南大学, 2019.
- [14] 郑羽. 铁道工业信息资源管理中的元数据驱动框架[J]. 四川兵工学报, 2011, 32(009):117-120.
- [15] 彭源. 模型与数据相结合的工业信息物理系统信息安全风险评估[D]. 华中科技大学.
- [16] 王弢, 崔君荣. 基于数据驱动的工业信息安全防护[J]. 信息技术与网络安全, 2018, 37(6):3.

版权声明: ©2022 作者与开放科学出版研究中心 (OSPRC) 所有。本文章按照知识共享署名许可条款发表。

<http://creativecommons.org/licenses/by/4.0/>



OPEN ACCESS