2020 年工业物联网安全趋势

简译版

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	Essential IIoT Security Trends for 2020		
原文作者	Seema Haji	原文发布日期	2019 年 6 月 27 日
作者简介	Seema Haji 是 Splunk 新兴市场团队的产品营销负责人，负责物联网和业务分析解决方案。		
原文发布单位	Security Week		
原文出处	https://www.securityweek.com/essential-iiot-security-trends-2020		
译者	安天技术公益翻译组	校对者	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块		
免责声明	• 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 • 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 • 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 • 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。		

2020 年工业物联网安全趋势

Seema Haji

2019 年 6 月 27 日

人工智能（AI）、增强现实（AR）和机器学习（ML）等技术曾经只存在于科幻小说中；而现在，这些技术在工业环境中扮演着越来越重要的角色。但是，这种变化伴随着一些风险。市场研究公司 IoT Analytics 预测，企业在工业 4.0 产品和服务方面的支出将会飙升——从 2020 年的 1190 亿美元飙升至 2023 年的 3100 亿美元。那些最有可能率先在工业物联网（IIoT）方面投资，且从投资中获得最大收益的公司，包括制造、运输、物流和公用事业公司——预计到 2020 年，这些公司将会在物联网（IoT）平台、系统和服务方面投入 400 亿美元。

在传统的模拟环境中引入新技术意味着，随着更多的设备联网，安全风险也会随之增加。虽然自动化和 AI 赋能的工具可简化操作、维护量少并带来友好的用户体验，但它们也为攻击者的入侵打开了新的大门，最终会产生各种负面结果，如知识产权（IP）遭窃、停机甚至物理伤害。

以下是最值得关注的两个趋势，它们会显著影响企业管理安全和风险的方式。

AI 和 ML 技术用于恶意网络活动

利用 AI 和 ML 技术，攻击者可以更轻松地、以机器速度执行恶意网络活动。在传播过程中不断学习和适应的 AI 恶意软件、协调全局攻击的机器学习，以及用于优化攻击的预测分析——它们都比我们想象的更接近现实。

在工业环境中，越来越多的生产（OT）安全团队将采用 AI 赋能的防御机制，来阻止这些 AI 威胁。但是，即使是 AI 工具也有可能受到破坏。例如，攻击者可以向训练这些工具的数据集投毒，而被投毒的数据集会导致算法的训练出现偏差。

鉴于上述原因，即使在部署了智能、自动化资产和流程的工业环境中，也需要操作人员的参与。企业需要考虑“人在闭环中”（Human in the Loop）的框架，将技术方法、管理与 AI 和 ML 的部署和使用结合起来，而不能盲目信任 AI 和 ML 技术。

边缘计算导致攻击面扩展

随着越来越多的 IoT 设备联网，这些设备生成日益庞大的数据量。在这种情况下，“边缘计算”（edge computing）的概念应运而生，成为一种受欢迎的数据处理方式。特别是，处理和分析网络设备的数据是在边缘上进行的，而不是在集线器或者数据中心进行。其目的是提供更好的性能，以减少运营压力和成本。

实施边缘计算基础设施，会增加新的攻击向量，进而扩展企业的攻击面。当考虑到 IoT 案例的多样性，以及它们与旧的传统 IT 技术的不同之处时，问题就更糟糕了。目前，还没有出台相关的 IoT 标准，无法帮助规范 IoT 的安全性。

只是跟踪和监控边缘设备就可能会导致很多问题。此外，这些设备还存在默认凭证和弱凭证的问题，以及不安全通信的问题。并非所有设备都被认为是关键设备，但即使看似微不足道的信息，对攻击者来说也可能是有价值的——例如，监控恒温器的日常使用就可以了解用户是否在室内。此外，边缘计算还存在物理安全风险，如篡改和损坏。

AI 赋能的解决方案和边缘计算都有巨大的潜力，可以帮助实现工业 4.0 的愿景。但是，我们不能只看到它们表面的价值。那些一马当先实施和使用这些新技术的企业，需要确保这些技术带来的风险远低于其带来的利益。

安天简介

安天是引领威胁检测与防御能力发展的网络安全国家队，始终坚持自主先进的能力导向，依托下一代威胁检测引擎等先进技术和赛博超脑大平台工程能力积累，研发智甲、探海、镇关、捕风、追影、拓痕等系列产品，为客户构建端点防护、流量监测、边界防护、导流捕获、深度分析、应急处置的安全基石。安天致力于为客户建设实战化的态势感知体系，依托全面持续监测能力，建立系统与人员协同作业机制，指挥网内各种防御机制联合响应威胁，实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报的有机结合，协助客户开展深度结合与全面覆盖的体系化网络安全规划与建设，支撑起协同联动的实战化运行，赋能客户筑起可对抗高级威胁的网络安全防线。

安天是全球基础安全供应链的核心赋能方，全球近百家著名安全企业、IT 企业选择安天作为检测能力合作伙伴，安天的威胁检测引擎为全球超过三十万台网络设备和网络安全设备、超过十五亿部智能终端设备提供了安全检测能力。安天的移动检测引擎获得国际知名测试机构颁发的 2013 年度权威评测奖项。

安天是中国应急响应体系中重要的企业节点，在“红色代码”、“口令蠕虫”、“心脏出血”、“破壳”、“魔窟”等重大安全威胁和病毒疫情方面，实现了先发预警和全面应急响应。安天针对“方程式”、“白象”、“海莲花”、“绿斑”等几十个高级网空威胁行为体（APT）及其攻击行动，进行持续监测和深度解析，协助客户在“敌情想定”下形成有效防护，通过深度分析高级网空威胁行为体的作业能力，安天建立了以实战化对抗场景为导向的能力体系。

安天被行业管理机构、客户和伙伴广泛认可，已连续五届蝉联国家级安全应急支撑单位，是中国国家信息安全漏洞库六家首批一级支撑单位之一，亦是国家网络与信息安全信息通报机制技术支撑单位，国家信息安全漏洞共享平台成员单位。

2016 年 4 月 19 日，在习近平总书记主持召开的网络安全和信息化工作座谈会上，安天创始人、首席架构师作为网络安全领域发言代表，向总书记进行了汇报。2016 年 5 月 25 日，习近平总书记在黑龙江调研期间，视察了安天总部，并对安天人说，“你们也是国家队，虽然你们是民营企业”。

安天实验室更多信息请访问： http://www.antiy.com（中文）
http://www.antiy.net（英文）

安天企业安全公司更多信息请访问： http://www.antiy.cn

安天移动安全公司（AVL TEAM）更多信息请访问： http://www.avlsec.com