Claroty 保护食品和饮料行业供应链的网络安全

2023 年 5 月 23 日
Claroty 团队编写

食品和饮料行业与其他行业一样，已经在数字化转型中取得了巨大的投资回报。物联网（IoT）、工业物联网（IIoT）、工业控制系统（ICS）等技术、人工智能(AI)、云计算和大数据已经改变了食品的生产、分配和消费方式。随着自动化水平的提高，企业能够通过简化流程来降本增效，通过降低人为错误的风险来改善质量控制，并通过降低污染风险来加强食品安全。虽然自动化、信息技术(IT)与运营技术(OT)之间的连接、网络化物理系统(CPS)的应用使食品和饮料行业受益匪浅，但在工业网络安全方面带来了重大挑战。

食品和饮料行业面临的三大工业网络安全挑战

一、IT 和 OT 的融合

食品和饮料行业中的CPS正被用于优化处理，并为运营决策提供信息，但也引发了对网络安全的担忧，因为越来越多CPS与物理世界交互。

- **对食品和饮料行业的运营影响**

IT和OT的融合对食品和饮料行业产生了重大影响，使公司能够实时分析数据，从而优化生产并提高效率。IIoT传感器和其他OT技术使企业能够通过监测温度、湿度和化学成分来改善质量控制，提高自动化程度和加强食品安全也是IT和OT融合的关键结果，从而减少了对体力劳动的需求，并提高了网络安全性和食品质量。

- **对食品和饮料行业的网络安全影响**

更深层次的问题是，有些食品和饮料公司在运营过程中使用老旧的OT系统，这些系统当时开发没有考虑到网络安全性，运行过时软件会很容易受到恶意攻击。食品和饮料公司还需要认清一个问题，就是在很多时候缺乏保护OT系统所需的网络安全专业知识，从而导致安全漏洞随时可能被黑客利用。

二、粮食生产压力

据联合国统计，到2050年世界人口将达到98亿，到本世纪末将达到112亿。这种令人震惊的人口增速会对粮食生产和交付造成重大压力。

- **对食品和饮料行业的运营影响**

随着全球粮食需求的增加，农业生产系统面临的压力也将越来越大，需要在更短的时间内，以更少的资源去生产更多的粮食。这无疑意味着耕种土地的使用面积会不断扩大，将给大自然生态系统带来破坏，可能会引发与可持续性发展相关的问题。如果发生水资源短缺的情况，农业部门就会与其他部门争夺水资源。还有，粮食供应的压力可能会导致生产过程的资源耗损，从而出现资源缺乏效率的现象，对生态环境产生不利影响，并致使食品安全隐患等诸多问题。

- **对食品和饮料行业的网络安全影响**

食品和饮料行业正在努力应对人口快速增长带来的粮食危机，同时也面对更严峻的网络安全风险。由于生产流程进一步自动化和数字化，对技术越来越依赖，风险漏洞便会增加。另外，食品和饮料公司试图通过使用IIoT传感器、控制器和ICS来应对这一挑战，却扩大了攻击面，以前留下的物理隔离OT系统处于危险之中。全球化生产和连通性进一步加剧了网络安全风险，使供应链变得越来越脆弱，物流和运输系统更容易受到恶意攻击。

三、需要可持续发展

第三个食品和饮料行业挑战在于需要可持续发展。随着全球粮食增产，温室效应和环境退化会持续加剧。

- **对食品和饮料行业的运营影响**

在众多行业中，食品和饮料行业的电力和淡水资源消耗量非常高，因为种植、收获、运输、加工和包装都需要能源配合。如今，越来越多的食品被生产出来，食品垃圾也在增多。需要被处理的垃圾得进入垃圾填埋场，在分解时会排放大量温室气体。

United Nations

联合国经济和社会事务部出版的《世界人口前景：2017年修订版》全面回顾了全球人口趋势和未来前景。

根据联合国统计，食品和饮料行业每年排放的温室气体约占全世界总排放量的三分之一，淡水抽取量接近全世界的三分之二，这对土地和海洋都造成了相当大的危害。

- **对食品和饮料行业的网络安全影响**

食品和饮料公司意识到及时应对挑战的必要性，并慢慢地推动可持续发展。通过使用互联设备，食品和饮料行业采用了精准农业和智能包装等实践，更加依赖数据、收集环境指标和供应链信息，从而优化效率。尽管这些生产上的进步对环保有所帮助，但恶意攻击者依然有机会利用其软件或硬件中的漏洞，还是会给网络安全带来新的风险。

食品和饮料行业面临的三大挑战都是相互关联的。如果其中一个问题变得严重，就会产生连锁反应，影响到其他两个问题，使补救变得更加困难。保护这些互联的系统和数据免受网络攻击，对于维护整个食品生产过程的完整性和安全性至关重要。

影响食品和饮料公司业务的网络安全事件

2021年，全球销售额最大肉类加工商 JBS Foods 遭遇勒索软件攻击，导致在澳大利亚、加拿大和美国的一些业务暂时关闭，数千名员工受到影响。规模庞大的JBS生产计划是7x24运作，对多家工厂瘫痪和工人被迫停工的容忍度很低。最后，JBS向黑客支付了1100万美元赎金。本次攻击除了造成JBS财务和声誉受损，还导致肉类短缺、价格上涨和破坏消费者的信心。JBS的勒索攻击事件向全球食品和饮料行业敲响了警钟。总体而言，特别是在食品和饮料行业，关键基础设施在网络攻击中是非常脆弱的。所以，实施有效的网络安全措施显得格外重要。

NEW Cooperative 是一家在爱荷华州拥有 60 个营业地点的农业合作社，在 2021 年遭到Black Matter 勒索软件攻击，勒索软件团伙声称已经获取了该合作社的财务和人力资源信息、网络信息和密码、研发结果以及Soilmap软件（农业生产者技术平台）的源代码，并要求合作社为解密密钥支付590万美元。本次攻击影响了合作社的计算机系统、电子邮件和电话系统，致使他们无法接收和履行客户的订单。针对农业合作社的攻击可能会直接导致食品供应链中断，最终引发的意外后果可能是带来全国粮食短缺问题。这一安全事件促使美国农业部长敦促合作社加强对网络攻击的防御，以避免对国家收成造成干扰。

“我们将不得不就此次攻击联系监管机构和 CISA 。”
NEW Cooperative 回应 Black Matter

与食品和饮料行业相关的网络安全标准

对于食品和饮料公司而言，了解适用于其运营的相关标准来改善网络安全态势变得非常重要。

- 《信息安全技术 关键信息基础设施安全保护要求》（GBT39204-2022）国家标准正式实施，这项标准给出了关键基础设施安全的三项保护原则，从分析识别、安全防护、检测评估、监测预警、主动防御、事件处置等6个方面提出了111条安全要求，为运营者开展关键信息基础设施保护工作需求提供了强有力的标准保障。

- ISO27001是一项被广泛认可的国际标准。该标准可用于企业的网络安全管理体系的建立和实施，保障企业的网络安全。

- NIST网络安全框架得到全球认可，符合现代网络安全标准，旨在帮助关键基础设施所有者和运营商管理，降低网络安全风险。

尽管食品和饮料行业有许多法规和标准，实施和遵守以上网络安全标准并非易事，但借助Claroty工业网络安全解决方案，食品和饮料公司可以简化对准则的遵守，支持工业互联网安全策略最佳实践。

《信息安全技术 关键信息基础设施安全保护要求》于2023年5月1日正式实施

Claroty 保护食品和饮料行业 OT 环境安全

一、实现完全可视化

保护食品和饮料行业OT环境的关键方法之一是获得对您环境中所有CPS的可视化。使用Claroty能厘清每个工厂 OT 环境的所有 OT、IoT、IIoT 和 BMS 资产清单，通过详细的设备信息了解需要保护的内容，为有效的工业网络安全奠定基础。

二、将现有的 IT 工具、工作流程与 OT 集成

许多食品和饮料公司CPS与传统 IT 解决方案存在不兼容的专有协议和老旧系统。为了保护其OT环境，Claroty建议食品和饮料公司从IT和OT扩展现有的工具和工作流程。Claroty不会扩展其已经存在的技术堆栈，只需简单地与它们集成，即可进一步优化从IT到OT环境的用例和治理领域。

三、将 IT 安全控制和治理扩展到 OT

与IT环境不同，许多OT环境缺乏必要的网络安全控制和统一的治理。一旦建立了企业范围可视化，并且现有IT工具、工作流与OT集成，Claroty可以通过将IT控制扩展到OT来帮助消除管理差距。通过统一安全治理，Claroty可以帮助食品和饮料公司实现网络和运营弹性之旅中的所有用例。

对于许多食品和饮料行业而言，工业网络安全风险已经超过了自动化、IT和OT连接和CPS带来的好处。逐年增长的勒索软件和其他恶意网络攻击，继续利用食品和饮料公司XIoT中的安全漏洞，影响其生产可用性、完整性和安全性。为了减轻工业网络安全风险并建立网络运营弹性，需要一种超越传统IT解决方案的全新方法。通过与Claroty合作，食品和饮料公司可以实施以上三项关键方法来保护OT环境，并确保遵守其行业众所周知的复杂标准和所需法规。

关于 Claroty

Claroty使工业、医疗保健和商业机构能够保护其环境中的所有网络化物理系统——扩展物联网 (XIoT)。Claroty平台可以与客户现有的基础设施集成，提供可视化、漏洞和风险管理、威胁检测、安全远程访问的全方位控制。Claroty得到了全球领先的工业自动化供应商的支持和采用，拥有广泛的合作生态系统以及屡获殊荣的Team82研究团队。

Cyberworld
广州科明大同科技有限公司
中国区总代理
官方网站 www.cyberworld.com.cn
业务电邮 info@cyberworldchina.com
服务专线 400-9988-792

CLAROTY