Rockwell Automation

工业网络安全案例研究

跨行业的挑战、解决方案及成果

目录

分享经验教训

罗克韦尔自动化寄语

尊敬的读者朋友：

我们认识到关键基础设施供应商正处于艰难时期。面对无情的网络攻击、复杂的数字化转型举措和看似无法阻止的疫情大流行，许多组织都在努力确保运营技术 (OT) 系统安全。

随着威胁主体证明其有能力并且将入侵 IT 系统以作为渗透 OT 和工业控制系统 (ICS) 的踏板，OT 安全变得越来越重要。正如您将看到的那样，这种入侵也会破坏 IT 系统和关键基础设施。

如果说有什么令企业高管都忌惮的安全威胁，那正在全球激增的勒索软件攻击无疑是其中之一。例如，随着俄罗斯入侵乌克兰后紧张局势加剧，美国网络安全和基础设施安全局 (CISA) 向美国各州和地方政府以及航空和能源部门网络发出警告，称来自俄罗斯境内的勒索软件攻击风险在不断加大。

更为复杂的是，许多关键基础设施组织缺乏自动威胁检测和响应能力，如针对网络和系统的持续监控。其他常见问题包括与数字化转型、传统系统和应用程序、非联网数字资产以及缺乏集中网络和威胁管理相关的风险。

此外，新冠疫情也引发了相关挑战，包括对安全远程办公能力的需求以及周期性运营中断和供应链崩溃。

您是否设想过企业如何应对如此多样的风险？ 在本罗克韦尔自动化客户案例研究摘要中，我们探讨了对各行各业的其他组织行之有效的解决方案，这些行业包括制药、生命科学、能源、石油和天然气、汽车制造、食品和饮料、快消品以及制造垂直领域。

如果您担心您的 OT 和 ICS 基础设施受到威胁，请参考以下成功案例。我们的资深团队已帮助多个行业的公司实施更安全的工业运营模式。虽然没有任何基础设施计划能够保证 100% 无风险，但仍有一些久经考验的解决方案可以显著降低关键基础设施安全风险。

Kamil Karmali

网络安全咨询服务事业部全球经理

罗克韦尔自动化

市场一览
OT 行业网络安全威胁

勒索软件继续肆虐

如果说亲身经历是最好的老师，那么其次可能就是来自业内同行的经验教训。遭受内部或外部威胁主体攻击的组织通常会获得网络安全方面的宝贵经验，包括如何识别和弥合漏洞，以及如何防御未来攻击。

在本报告提到的案例研究中，我们将剖析 10 家关键基础设施供应商如何在网络犯罪分子窃取密码并渗透网络和应用程序之前改善安全防御措施。不过，让我们先浏览一下网络安全和基础设施安全局 (CISA) 所确定的 16 个关键基础设施行业中 6 个行业的网络攻击及安全现状。

制药和生命科学行业

直击新冠疫情响应的核心

制药和生命科学公司处于新冠疫情响应的核心地位。

网络犯罪分子通过部署恶意软件、勒索软件、网络钓鱼和 URL 骗局，继续利用疫情获取商业利益，通常使用新冠疫情和冠状病毒主题作为诱饵。与其他行业一样，威胁主体也试图入侵为居家办公员工新建的远程访问基础设施。

更重要的是，来自朝鲜、俄罗斯和中国等国家的民族国家袭击事件数量不断增多且日益复杂，其目的是破坏从事新冠肺炎疫苗、治疗药物和医疗设备研发的公司。攻击目标包括工业间谍活动、盗取知识产权以及获取受保护的患者健康信息等。

医疗设备制造商也是威胁主体的目标，他们试图入侵穿戴式和植入式医疗设备。而其中有些设备（如联网起搏器和葡萄糖监测仪）通过互联网连接到医院网络。许多医疗行业高管担心，联网医疗设备为针对医院和医疗设施的网络攻击开启了大门，可能会造成危及生命的后果。

鉴于风险如此之高，负责监管此类设备的食品和药物管理局已将更新需求列为优先事项，以便妥善保护这些设备。

86% 的组织报告称 ICS 环境缺乏可见性。

资料来源：DRAGOS

石油和天然气行业

输送管道安防与震惊全球的网络攻击事件

石油和天然气行业高管对美国最大的输油管道 Colonial Pipeline 被攻破后面临的勒索软件攻击感到担忧，这是可以理解的。而他们的担忧也不无道理。该攻击关闭了部分业务系统，并导致美国东部天然气短缺。

据彭博社报道，黑客于 2021 年 4 月 29 日通过一个 VPN 帐户成功入侵公司网络，而该帐户在攻击发生时已不再使用，但仍可用于访问 Colonial 的网络。最近的一份报告发现，77% 的美国大型能源公司至少有一个密码在网上被泄露。

一方面，石油和天然气公司将运营技术 (OT) 系统与工业控制系统 (ICS) 数字化和互联化，以实现运营环节的集中管理；另一方面，公司的安全事件也在增加。在美国，石油和天然气行业是仅次于金融服务和制造业的第三大攻击目标行业。

Colonial Pipeline 攻击事件突显了威胁主体破坏 OT 系统的能力、攻击对关键基础设施供应商的潜在灾难性影响以及进而对消费者日常生活造成的影响。

汽车行业

日益增长的连通性引发新的网络安全担忧

在汽车行业领域，汽车制造商和零部件制造商面临不断激增的勒索软件攻击，这会危及融合后的 IT 和 OT 系统的安全。一项研究发现，领先汽车制造商中有 49% 极易受到勒索软件攻击。在许多情况下，这些攻击从入侵 IT 系统开始，随后蔓延到相连的 OT 资产。

例如，在一家跨国汽车制造商近期遭遇的攻击中，网络犯罪分子实施了网络钓鱼活动，将勒索软件植入该公司的 IT 系统，随后又传播到 OT 资产。此次攻击使其全球各地的生产工厂停产，并造成公司 IT 和电子邮件系统瘫痪。

勒索软件并不是让高管们夜不能寐的唯一威胁。针对汽车行业供应商的网络攻击所带来的中断造成了供应链阻滞，这种情况已在各个行业和地区蔓延，导致运营业务缩减，在某些情况下，甚至会导致整座工厂停业。

快消品行业 (CPG)

网络攻击频率和成本攀升

在快消品公司中，网络安全事件呈上升之势。超过 40% 的快消品制造商在 2020 年遭遇过网络攻击。黑客入侵造成的经济损失巨大，而且会越来越大。快消品行业数据泄露的平均成本在 2021 年飙升至 370 万美元，相比上一年度增长了 42.9%。

可能推动网络安全需求增加的趋势包括物联网 (IoT) 传感器和设备的更广泛应用、5G 技术的日益普及以及 IT/OT 网络融合。越来越多的设备和操作系统将联网并在网络间传输数据，这使得攻击面明显扩大。

为应对供应链攻击，快消品制造商不得不重新构思采购、调整仓库空间并重新考虑交付模式，以及重新评估供应商的供货能力。

食品和饮料行业

勒索软件攻击破坏性日益增强

食品和饮料行业正在经历消费者偏好的结构性转变，他们向往更健康的食品和更愉快的购物体验。例如，年轻消费者日益青睐当地采购并以环保包装配送的植物性营养食品。与此同时，针对食品和饮料企业的网络攻击在成本和停机时间方面的破坏性越来越大。

新冠疫情也接踵而来。食品和饮料公司迅速实施了远程办公平台，以满足新的工人安全、安防和隐私要求。企业纷纷发现他们的传统系统和应用程序往往与现代网络安全解决方案不兼容。对最新、基于风险的安全计划的需求愈加明显，尤其是在攻击数量增加时。

例如，针对巴西大型肉类加工商 JBS 的勒索软件攻击也波及到了其在美国、加拿大和澳大利亚的工厂。威胁主体加密了该公司的系统和数据，然后要求支付数百万美元赎金用于恢复访问权限。JBS 最终支付了 110 亿美元。此外，据《芝加哥论坛报》报道，在 JBS 遭遇攻击之前的 12 个月里，估计还发生过 40 起针对食品生产商的攻击。

此类恶意软件活动突显了食品和饮料企业备受针对的趋势，而这些企业的一个共同点就是使用了融合 IT 和 OT 系统来改善生产管理。但是如果没有合适的网络安全计划和控制措施，这种融合可能会将 OT 系统暴露在各种复杂的网络威胁中。

借鉴他人的成功经验

以下案例研究揭示了罗克韦尔自动化客户所面临的各种挑战。而所有这些挑战都具有共同点。

最好的 OT 网络安全解决方案（体现在保护质量、部署速度和持续服务方面，能够最大限度缩短停机时间并抵御网络攻击）需要工业运营经验。

在这些案例中寻找与自己相似的挑战。我们认识到，本摘要中分享的见解对于理解可用于克服各行业 OT 威胁的解决方案非常有价值。

制药业

跨国制药公司在全球 64 个站点实现实时 ICS 威胁可见性和每日资产盘点

制药公司长期以来一直是高级网络犯罪分子最喜欢的目标。而新冠疫情深化了企业对基于风险的网络安全计划的需求，而且发展速度很快。

一家跨国药品制造商在制定 IT 和 OT 系统网络安全计划方面需要帮助。未修补的 OT 资产增加了制造厂的安全风险，而且缺乏对 ICS 控制器所面临威胁的实时可见性导致几乎无法检测到 OT 恶意软件。

更糟糕的是，公司尚未将业务网络与工业工厂网络隔离，也没有限制制造系统的进出站流量和路径。

放眼未来，公司知道其需要对团队开展教育，促成良好的网络安全卫生，以创造持久的文化安全改进。

88% 的美国医疗科技领导者认为他们的公司尚未做好应对网络安全事件的准备。

资料来源：IRDETO

方案部署

在评估风险后，这家制药巨头与罗克韦尔自动化合作，通过网络分段和加强端点和边界安全，朝着完善网络安全保护迈出了重要一步。

最初，公司快速设计并实施了一个三阶段网络安全计划。

第一优先事项就是在全球 64 个站点实现逻辑和物理网络分割，以帮助遏制威胁来袭时在网络和系统中的传播。公司还加强了边界设备的安防以阻挡威胁主体，并部署了应用程序“允许列表”，仅在完成预先批准后才允许使用应用程序，从而保护端点。

接下来，公司实施了一套威胁检测服务以及 USB 清洗来集中管理和监控 OT 网络上的 USB 介质，防止来自网络内外的威胁或攻击。威胁检测服务还能确定可用作基线的正常网络行为，使用全天候威胁监测功能来检测异常活动，并在检测到异常活动时以示警红旗标记出来。这有助于公司更快或在攻击发生之前识别出可能对系统构成风险的活动。

成果

罗克韦尔自动化在短短九个月内帮助该制药公司在全球 64 个站点设计并实施了经过扩展的安全策略。此举提高了该公司保护 OT 和 ICS 资产免受日益复杂的网络威胁的能力。该公司现在可以实时、一致地了解在全球各地面临的 ICS 威胁。

数字解读

快速构建应对网络威胁的全面防御措施

范围

- 9 个月部署期
- 全球 64 个站点

解决方案

- 网络安全计划
- 网络分段
- 端点和边界安防
- 威胁检测
- USB 介质管理

生命科学行业

医疗设备制造商进行网络基础设施现代化，以改善 OT 网络安全并促进业务增长

一家总部位于美国的医疗设备制造商制定了扩大全球产能的宏大计划。

其增长预测催生了对标准化基础设施蓝图的要求，以便支持扩展其数字化转型举措以及实现 OT 基础设施现代化。公司还需要通过 IT 和 OT 网络分段来加强网络安全。

多年来，OT 方面的投资并没有跟上 IT 发展步伐，公司需要重新设计 IT 和 OT 系统，以加强对不断发展和扩张的数字化企业的网络安全保护。

速度至关重要。这家设备制造商需要制定并快速部署集中式网络安全和现代化战略，以帮助保护其日益扩增的网络和数字资产。但是，公司缺乏足够资源来快速实施新功能，无法满足企业日程要求。

全球安防领域领导者中有 80% 认为，勒索软件不仅危及公众安全，并且威胁程度也在不断增加。

资料来源：世界经济论坛

方案部署

罗克韦尔自动化与该医疗设备制造商合作，制定了一项用于评估和重新设计网络的综合性计划，并为其在全球四个地区的七个站点增设了工业非军事隔离区 (IDMZ)。

接下来，为该组织的虚拟基础设施制定了标准设计蓝图。公司首先从 IT 和 OT 网络分段入手，以更好地保护环境之间的数据流动。另一项关键举措是在 IT 和 OT 网络之间创建数字安全边界，即 IDMZ。该技术使用网络和应用程序安全控制措施来管理和保护跨区数据流。

在为期 12 个月的部署期中，公司需要了解实现自动化的精确要求和成本，以及网络和 IDMZ 实施情况和一致的网络设计标准。公司与罗克韦尔自动化生态圈的多家合作伙伴合作，获得了所需见解并加以实施，包括由美国泛达负责物理安装和布线，以及由我们的 LifecycleIQ Services 业务部负责在全球部署监控和数据采集 (SCADA) 系统。

公司还实施了一项托管服务计划来监控和管理其网络、数据中心和应用程序。

成果

该解决方案帮助公司达成了建立标准网络和 IDMZ 基础设施蓝图的目标，为实现快速安全的业务增长以及产能提升提供了有力支持。该蓝图为新建站点的分阶段实施提供了正确的框架，也可用于现有站点的网络基础设施现代化以及远程管理网络扩展需求。

该医疗设备制造商现在可以了解满足这些要求所需的资本支出 (CapEx)，从而做出更好的战略规划和决策，并确保网络安全问题随着公司的发展得以解决。

数字解读

实现现代网络基础设施的安全扩展

范围

- 12 个月部署期
- 全球 7 个站点

解决方案

- 网络设计与蓝图
- IDMZ
- 托管式网络安全服务

能源公司

天然气存储和输送管道公司通过实时威胁检测和资产盘点增强 62 个压缩机站和终端的网络安全

随着石油和天然气公司争相避免日益增多的网络攻击，许多公司明白他们需要部署一项全面的网络安全计划来保护 IT 和 OT 网络。

美国一家大型州际天然气管道供应商就是例子。由于缺乏统一的网络安全计划，公司业务和 IT 负责人对设备、网络和有效生产时间面临的当前和未来威胁不甚了解。在任何特定时刻，攻击者都可以在未被发现的情况下渗透公司的数字资产，这可能会扰乱运营，甚至破坏或关停工厂和设施。

随着公司将互联 IT 和 OT 系统作为数字化转型项目的组成部分，企业领导层认识到，需要认真实施一项基于风险的集中式网络安全计划，以使公司能够快速检测和应对网络威胁。

美国大型能源公司中有 77% 至少有一个密码被泄露到网上，导致其极易受到攻击。

资料来源：《休斯敦纪事报》

方案部署

罗克韦尔自动化帮助天然气管道公司设计和部署了 62 个北美压缩机站与终端的统一威胁保护解决方案。

罗克韦尔自动化与其生态圈合作伙伴 Claroty 合作，设计了一套托管式威胁检测服务，其中包含资产清单监控，以识别公司网络中的所有 IT 和 OT 资产。既有资产盘点是揭示安全漏洞以及制定规划以阻挡内外威胁的关键步骤，有助于更快地应对和遏制网络攻击。管道供应商还与 Claroty 合作，实施了实时威胁监测解决方案，并确定了事件响应工作流程。

凭借现代化的威胁检测能力，管道供应商现在已做好在现场和业务据点快速发现并应对网络安全威胁的准备。该公司还制定了员工最佳实践，可以清晰地了解不断变化的需求。

成果

罗克韦尔自动化帮助该公司在约 11 个月内完成了现代安全计划基础性工作，这是一项复杂又紧迫的任务。如今，随着对 IT 和 OT 网络中所有数字资产的全面了解，该公司的安全态势得以改善，能够持续实时识别安全威胁，并快速响应事件，以帮助减少攻击带来的影响。

数字解读

保障管道安全

范围

- 11 个月部署期
- 62 个北美站点

解决方案

- 托管式威胁检测
- 威胁监控
- 资产盘点
- 事件响应计划

石油和天然气行业

通过实时威胁检测和网络资产盘点，石油和天然气供应商在短短一个月内降低了网络停机风险

随着威胁主体将能源行业视为勒索软件和其他恶意软件的攻击目标，石油和天然气系统面临的网络威胁不断攀升。Colonial Pipeline 攻击事件证明，攻击行为会严重破坏关键基础设施服务与供应，给数百万人带来影响，并造成重大经济损失。

与此同时，新冠疫情也加快了数字化步伐，伴随着员工远程办公的需求，进一步加剧了安全风险。

为了降低风险，一家跨国能源公司需要加强其公司风险管理战略。其中一个关键因素就包括更新 OT 系统，确保在发生网络攻击时最大限度降低风险。

公司还知道他们需要通过实施可扩展威胁检测平台实现数字资产的主动式防御，这样可以快速识别漏洞和潜在威胁，并生成数据驱动型运营见解，最终提升决策能力。

同时公司还需要其他方面的帮助，力求有效管理技术老化和现代化相关成本，以及将不一致的解决方案工程设计改造为更统一的基础设施。

79% 的石油和天然气公司报告称，在过去 12 个月，破坏性攻击事件有所增加。

资料来源：《2021 安永全球信息安全调查报告》

方案部署

公司与罗克韦尔自动化公司合作，设计并部署了一项全面的威胁检测计划。该解决方案确定了正常网络行为基线，并实现了实时网络资产盘点。接下来就是持续监控行为活动，以检测和报告异常行为，防止威胁演变为实际攻击。通过威胁检测解决方案还可深入了解 OT 系统和网络活动，进而全面改进决策。

罗克韦尔自动化和其生态圈合作伙伴 Claroty 为能源公司的 12 家炼油厂、3 套中游设施、1 个 SCADA 系统以及 1 个集中式企业管理控制台实施了威胁管理解决方案。

49% 的美国顶级能源公司由于系统过时而存在严重漏洞。

资料来源：BLACK KITE 调查

成果

这家石油和天然气公司现在拥有一套用来保护 OT 和 IT 网络免受破坏的统一战略，其中包括威胁检测服务和实时资产盘点，让公司能够检测、响应和缓解网络安全威胁，同时降低网络安全事件造成停机的可能性，从而最大限度减少业务连续性风险。

该解决方案在试点部署后的一个月内就实现了安防能力提升。目前，它可以帮助企业领导层更好地了解运营状况和员工绩效，减少安防团队工作量，并支持数据驱动型决策。

数字解读

通过增强威胁检测最大限度降低业务连续性风险

范围

- 1 个月试点期
- 17 个站点
- 生态圈合作伙伴：Claroty

解决方案

- 威胁检测
- 实时资产盘点

汽车行业

汽车制造商如何以创纪录的速度完成 OT 安全评估以实现改进

汽车制造商正面临多重挑战，他们需要应对快速发展的产品需求和正在转型的行业生态圈。在如此混乱的市场环境中，一家跨国汽车制造商开始担心其网络安全缺陷。

具体来说，该公司担心 OT 漏洞可能会让网络犯罪分子潜入其 IT 和 OT 网络，从而窃取敏感信息并扰乱运营和生产线。尽管该公司最近已斥资保护关键制造环境，但领导层还是认为网络极易被攻破。鉴于个别员工已遭受大量网络钓鱼和勒索软件攻击，该公司知道增强员工的威胁意识将有助于降低公司 IT 和 OT 基础设施的网络安全风险。

48% 的汽车制造商正面临很高的勒索软件攻击风险。

资料来源：BLACK KITE 公司，勒索软件风险：2021 年汽车制造业 - 2021 年 6 月

方案部署

罗克韦尔自动化通过渗透测试帮助汽车公司评估网络安全能力，渗透测试是一种由专家对系统实施的模拟网络攻击，目的是找出安全漏洞。

在此案例中，汽车公司的诉求是确定外部主体是否能渗透并控制其 IT 和 OT 环境。凭借罗克韦尔自动化团队的 OT 网络安全专业知识，所需的测试服务很快完成，相比一般第三方供应商缩短了六周。

事实上，罗克韦尔自动化团队在短短两天内发现，工厂车间的多个区域都安装了远程控制软件，这让安全从业人员能够轻松快速地建立连接。我们的网络安全专家与该公司的 CIO 和 CISO 协作测试了实际应用场景，发现潜在攻击者完全能够从公共互联网绕过防火墙加固的边界直接连接到每个生产环境。

换言之，在为期两天的渗透测试中，罗克韦尔自动化发现，网络犯罪分子可以完全控制 IT 和 OT 网络并访问数字资产和设备，包括人机界面 (HMI) 服务器和控制系统、机密性制造计划、客户数据、安防摄像头，甚至是 Microsoft Office 365 电子邮件帐户的用户密码，连 CEO 本人的密码也难以幸免。

成果

渗透测试与评估服务快速识别出多个关键漏洞，揭示了可能会让威胁主体控制制造商资产和生产环境的访问路径。现在，高管层对漏洞以及如何更好地保护 IT 和 OT 基础设施有了真实的了解。评估完成后，罗克韦尔自动化根据渗透测试期间发现的漏洞以及汽车制造商需求量身制定了一套完整的保护计划。该汽车企业计划扩展安全评估和缺口补救范围，并帮助员工了解保障良好网络安全卫生的重要性。

数字解读

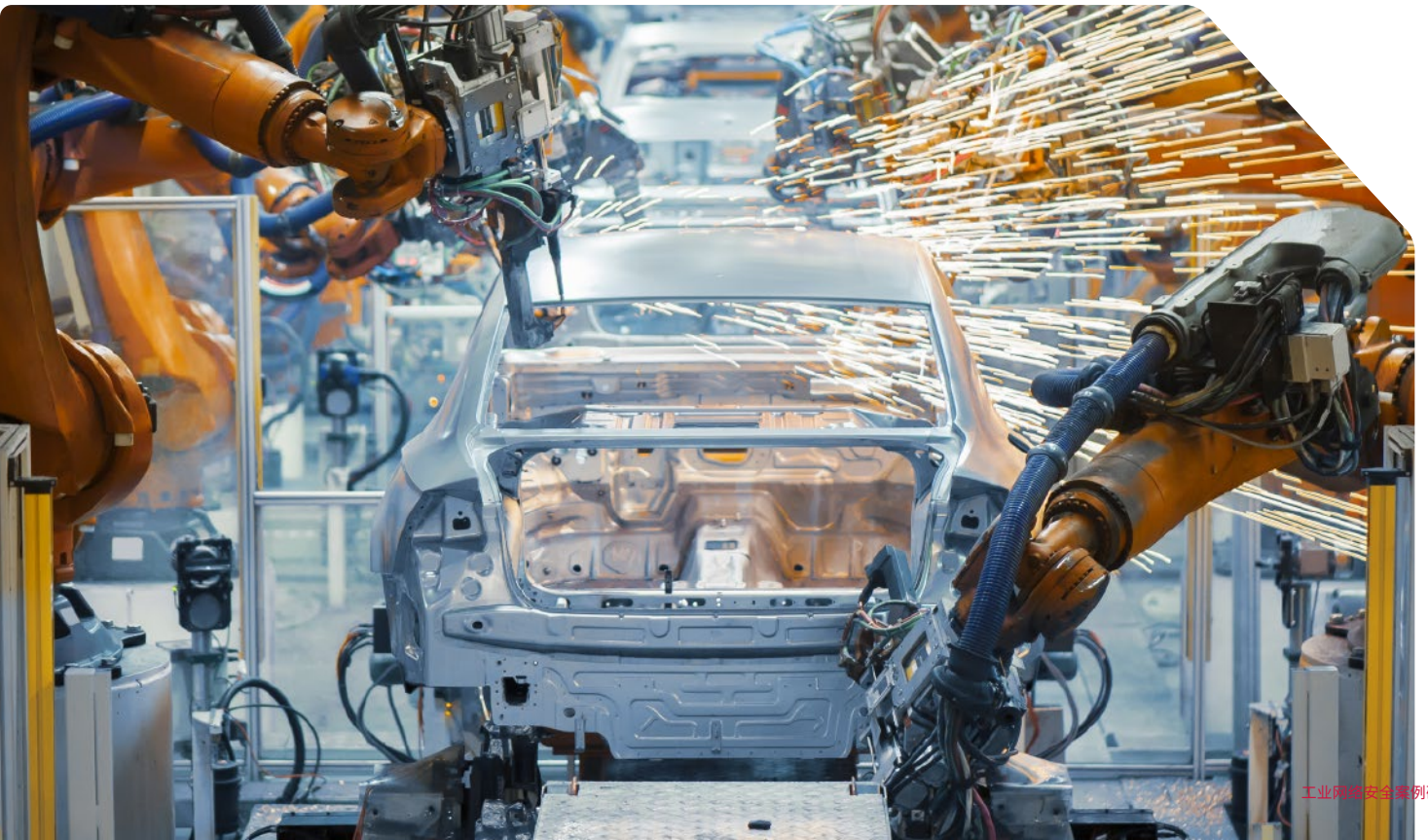
通过渗透测试识别关键漏洞

范围

- 2 周
- 6 个站点

解决方案

- 渗透测试



快消品行业

食品制造商在全球 46 个站点部署统一威胁管理，确保收购的数十家公司具备一致的网络安全水平

一些快消品 (CPG) 公司在新冠疫情期间蓬勃发展（比如杂货、食品和保健品供应商），而另一些则陷入了困境。但是，两者都面临严峻的挑战。网络攻击日益常态化，带来的损失也越来越大，互联 OT 和 IT 系统可能会危及工业控制系统，而公共安全需求一再升级，对敏捷性提出了更高要求。

为了克服这些障碍，一家位列《财富》500 强的消费食品制造商需要清楚了解其 OT 和 IT 网络中存在的网络安全漏洞。更为复杂的是，该制造商在过去 20 年间收购了数十家食品企业，每一家都配备不同的技术和安全生态系统。

因此，该制造商不能集中实时了解全球 46 家制造基地的系统安全性。实现透明化需要标准且基于风险的安全战略以及统一威胁管理能力。

2021 年，快消品公司数据泄露带来的平均损失飙升至 370 万美元，比 2020 年增加了 42.9%（增幅近 43%）

资料来源：IBM SECURITY 平台，2021 年数据泄露成本报告 - 2021 年 7 月

方案部署

通过与公司网络安全负责人协作，以及在其生态圈合作伙伴 Claroty 的协助下，罗克韦尔自动化为该制造商在全球 46 个制造基地设计并部署了集中式威胁检测服务。此举帮助确立了网络活动基线，并针对异常活动提供了持续威胁检测能力，确保在不影响运营的前提下实现网络攻击预警。

现在，一旦系统遭到入侵，定制工作流就会帮助恢复受影响的系统和网络。由于员工培训对于确保安全战略的有效性至关重要，公司还实施了一项旨在培养全企业网络安全卫生文化的计划。

成果

该食品制造商目前已拥有集中且统一的威胁管理系统，能够将可见性从 IT 扩展到 OT 环境，及时检测并解决各类网络威胁，防止演变为入侵事件，从而最大限度降低网络安全风险。员工通过覆盖全企业的培训计划获得了新的网络安全意识。

放眼未来，公司将继续通过收购发展业务，因此便立足于实施一致的网络安全计划。

数字解读

实现集中式威胁检测，最大限度降低全球 OT 和 IT 网络面临的风险

范围

- 全球 46 个站点
- 生态圈合作伙伴：Claroty

解决方案

- 威胁检测服务

食品和饮料行业

食品和饮料制造商改善了网络安全和事件响应能力，将整体设备效率 (OEE) 评分提高了 5%

在经历了一次扰乱计算系统和生产线的恶意软件攻击之后，一家跨国休闲食品公司需要加强网络安全防御并在全球 80 个站点实现网络基础设施现代化。公司在早些时候曾尝试过部署一个整体设备效率 (OEE) 平台，以帮助衡量和缓解安全风险并提高现有应用程序的性能。但由于 OEE 软件与公司的企业控制层以及网络之间存在不兼容问题，这一计划并未成功实施。

公司请求罗克韦尔自动化帮助其实现全球数字资产盘点，以及事件响应能力和首要网络安全能力的现代化升级。

2021 年快消品公司数据泄露带来的总平均损失增加了 43%。

IBM SECURITY 平台，2021 年数据泄露成本报告 - 2021 年 6 月

面临的挑战

快消品 (CPG) 行业的形势一直很艰难。没有人会对过去十年的状况感到陌生：产品和购物偏好发生了翻天覆地的变化，全球供应链受到重创，疫情政策限制了消费群体规模，熟练工严重短缺。

如今，爆炸式增长的网络攻击令行业形势雪上加霜。

方案部署

罗克韦尔自动化与该公司的全球工程设计总监协作，对公司网络进行评估，并帮助确保衡量 OEE 所需的数据与企业网络及应用程序兼容。

罗克韦尔自动化随后对该公司在全球的工厂进行了全面的网络评估，并实施了可互操作工业数据中心 (IDC)，以实现远程监控和数字资产管理。经过深入评估，我们团队制定了一项计划，旨在缓解与 OEE 应用程序之间的网络冲突，并由罗克韦尔自动化支持团队实施全天候远程监控与管理。

成果

随着新的网络基础设施部署到位，该休闲食品制造商很快便见证了数据准确度和标准化全球报告方面的改进。统一基础设施与我们的托管服务相结合，帮助企业缩短停机时间，提高数据准确度，并使用服务级别协议 (SLA) 更快响应网络安全事件。

这些优势叠加在一起，帮助该食品和饮料公司将其整体 OEE 评分提高了 5%。即使 OEE 只提高 1%，也能帮助大型生产线节省大量成本，除此之外，还可作为公司改善 OT 网络安全防御的典型商业案例。

数字解读

改善网络安全，提高 OEE 评分

范围

- 全球 80% 的站点
- 整体设备效率 (OEE) 提高 5%
- 生态圈合作伙伴：
  World Wide Technology

解决方案

- 解决方案
- 网络评估
- 全球资产盘点
- 部署 IDC，实现全天候远程监控与管理
- 事件响应

食品和饮料行业

食品和饮料公司通过全天候托管支持服务简化 OT 网络安全

面临的挑战

许多制造商多年来未能更新传统系统和软件。这可能会增加网络攻击风险，造成运营效率低下，削弱业务成果，并增加数字化转型工作的复杂度。

在着手规划为期多年的现代化项目时，一家跨国食品和饮料制造商就发现自己面临这样的状况。有三大挑战需要解决。另外，公司的主要目标之一是简化关键 OT 系统的管理，以及整合尚未一致实施的新资产与仍在使用的老旧技术。在未实现上述整合的情况下，公司员工缺乏一致管理 OT 系统的技能。

更糟糕的是，新冠疫情刺激了消费者对食品类产品的需求。公司业务负责人担心，他们的技术基础设施无法承受不断增长的通信流，继而导致停工和收入损失。

随着越来越多的员工和第三方选择居家办公，公司在实施安全远程访问方面也需要帮助，力求抵御不断增加的网络安全事件。这些因素交织在一起，形成了一个不稳定、不可靠的技术生态系统，导致了计划外财务损失。该制造商还需要对 OT 数字资产实施一致可靠的管理，确保在面临挑战时生产业务仍可正常运转。

方案部署

该食品和饮料公司请求罗克韦尔自动化帮助部署托管服务，以更好地抵御网络攻击，并营造一个稳定高效的运营环境。

罗克韦尔自动化与该公司合作设计了一套能够管理所有数字基础设施设备的企业 OT 托管支持服务计划。另外还实施了其他解决方案，用以实现对关键应用程序、软件和基础设施的一致部署与支持以及全天候远程监控。

罗克韦尔自动化还帮助该公司部署了 19 个 OT 工业数据中心 (IDC) 和一个持续威胁检测平台，以应对网络安全风险。而且，为了保护居家办公的员工，我们还在北美 40 个站点设计并实施了安全远程访问。

成果

基础设施和配套托管服务已完成现代化升级，使该制造商能够通过全天候威胁监控减少公司和 OT 网络受到的网络安全威胁，同时将停机风险降至最低。技术资产的一致部署和整合帮助提高了系统可靠性，改善了应用程序管理，并延长了工厂正常运行时间。部署安全远程访问功能可以保护员工、第三方合作伙伴和公司运营基础设施免受网络风险影响。

这些举措结合起来，使公司在降低成本的同时提高了运营效率。

数字解读

更新传统系统，获得强大的网络安全保护能力

范围

- 40 个站点
- 19 个 OT 工业数据中心

解决方案

- 为所有数字基础设施设备提供托管支持
- OT 工业数据中心
- 安全远程访问
- 全天候威胁检测

快消品行业

快消品公司经历安全数字化转型，使得平均网络响应时间降低达 90%

看起来势不可挡的新冠疫情颠覆了工作场所的运营方式，改变了消费者的购物习惯，并削弱了全球供应链。更为糟糕的是，网络攻击的频率、严重程度和代价急剧上升。例如，在一项研究中，61% 的制造商报告称 2021 年曾经历过网络攻击，其中有 75% 更是遭遇了系统瘫痪。

疫情大流行还有一个连带后果，就是需要快速跟踪数字化转型工作来应对远程办公等新挑战，以及为满足随之而来的工业网络安全要求对新接入的运营系统和网络采取保护措施。

正如一家跨国食品和饮料制造商所发现的，数字化转型和网络安全不能再被视为两个独立的举措，而必须整体实施。该公司计划推出一项以安全为中心的数字化计划，确保日益数字化的业务系统生成的实时数据充分发挥作用。但首先需要解决多年来积累的技术缺陷。

例如，该食品制造商的传统系统和应用程序与现代云计算及网络安全平台不兼容。各不相同的网络和虚拟基础设施无法容纳关键数据分析和人工智能技术。而且，员工网络安全意识不足和培训计划不到位也导致了安全卫生不良的文化。

2021 年，61% 的工厂经历了安全事件。

资料来源：趋势科技，《工业网络安全现状》，2021 年 5 月

方案部署

该快消品制造商请求罗克韦尔自动化帮助其实现 IT 和 OT 系统的现代化和统一，实施新网络自动监控与管理，以及改进北美 44 个站点的网络安全能力。但是，该制造商并不想利用资本支出 (CapEx) 资金来实现这一目标。

罗克韦尔自动化利用我们的基础设施即服务 (IaaS) 产品创建并部署了一套基于云的现代解决方案。我们的团队与该快消品公司一起设计出 IaaS 网络并部署网络安全能力，包括网络分段、运营系统补丁管理和防病毒解决方案。罗克韦尔自动化生态圈合作伙伴 World Wide Technology 负责为该计划提供硬件。随后将所有网络和计算基础设施都迁移到 OT 托管服务中。

该公司还部署了罗克韦尔自动化的 TechConnectsm 支持与应用程序支持服务，用以改进应用程序和基础设施的全天候服务台支持质量，并派遣现场人员提供驻场支持。虽然服务级别协议 (SLA) 要求在 10 分钟或更短时间内对 IaaS 报警做出响应，但实际响应时间平均仅为 3.5 分钟。

成果

该安全数字化转型解决方案通过实施采用基础设施即服务 (IaaS) 产品的现代化网络基础设施，以及有效的 OT 补丁管理（一种急需解决的复杂安保要求）和病毒防护措施，填补了巨大的网络风险缺口。

凭借罗克韦尔自动化的应用程序支持服务，该公司对关键警报和报警的响应时间加快了 90%，从而缩短了停机时间。用于此计划的资金来自于该公司的运营支出，这使其能够在不动用资本支出 (CapEx) 准备金的情况下为数字化转型提供资金。全球性支持且随时服务的支持模式帮助解决了新数字化运营中的 IT 和网络安全熟练工短缺问题，并为公司未来的规模扩张做好了准备。

数字解读

实施安全数字化转型，响应时间加快 90%

范围

- 44 个北美站点
- 响应时间从 IaaS SLA 规定的 10 分钟缩短至平均 3.5 分钟
- 生态圈合作伙伴：World Wide Technology

解决方案

- 基础设施即服务 (IaaS)
- OT 补丁管理
- 防病毒
- TechConnectsm 支持和应用程序支持

化工行业

化工公司为员工提供对控制系统的安全远程访问权限，以便在新冠疫情期间处理多达 8000 个 I/O 点

面临的挑战

鉴于新冠疫情仍在持续，大量员工选择继续在家办公。生物燃料公司也不例外。

南美的一家乙醇、生物能源和牲畜饲料生产商需要实现对公司 IT 和 OT 网络的安全远程访问。当务之急是与远程供应商一起实施对新建项目的安全访问。该生物燃料公司还需要制定旨在减少差旅的工作指令，同时确保能够审计与工业控制系统 (ICS) 的所有远程交互。

方案部署

该生物燃料公司与罗克韦尔自动化合作，设计和部署了关于复杂电源选项的安全解决方案。

其中新建项目是第一要务。罗克韦尔自动化提供咨询服务，帮助公司了解能够达成项目目标的复杂电源阵列选项。其中一个选择是配备中低压动力设备的智能成套动力 (IPP) 系统，现已集成至公司的分布式控制系统 (DCS) 中。

预计在 2021 至 2026 年间，全球生物燃料需求将增长 28%。

国际能源署，《可再生能源 2021—2026 年分析与预测》，2021 年 12 月

罗克韦尔自动化随后帮助该公司改善了集中式安全信息监控，实施了工业数据中心 (IDC) 解决方案以及针对虚拟环境的全天候远程监控和管理。我们的团队还设计并实施了工业非军事隔离区 (IDMZ)，用于安全隔离公司的业务网络和工业控制系统。

考虑到新冠疫情导致的旅行和社交距离限制，安全远程访问和配置能力也至关重要。这样一来，生物燃料公司就能监控远程操作员与 ICS 之间的交互，并审计与主要供应商（距离现场 1,243 英里以外）的所有远程交互。这种方法也将部署在未来的新建站点中。

成果

使用罗克韦尔自动化的生命周期服务，配合部署 IDMZ 和安全远程访问，该公司完成了其新建项目要求，同时降低了公司和 OT 网络所面临的网络安全风险。该举措还简化了 OT 和 ICS 远程访问会话的控制与监测，提高了系统可靠性，改进了员工效率，并通过全天候远程监控提高了系统支持覆盖范围。

罗克韦尔自动化团队还帮助该生物燃料公司强化了当前和未来应对疫情大流行的员工安全程序。

数字解读

部署新冠疫情期间的安全远程访问

范围

- 2 个站点
- 生态圈合作伙伴：Claroty

解决方案

- 威胁检测服务

罗克韦尔自动化：保障世界根基安全

罗克韦尔自动化提供一系列工业安全解决方案与服务，帮助您管理威胁，提高 OT 和 IT 运营弹性。我们的专家可以设计稳健且安全的网络基础设施，同时通过全天候监控措施抵御威胁并对事件做出快速响应。除了深厚的专业知识和最新的最佳实践知识外，我们还带来了源于 100 多年工业自动化经验的生产运营智慧。

我们的业务据点覆盖全球，能够帮助客户在全球多站点实施一致的网络安全保护措施，同时提供定制后勤服务，满足您对工业自动化行业巨头的所有期望。

入门参考资源

- 深入了解常见 OT 网络安全攻击。观看 Automation Fair® 会议演示：OT 领域的十大网络安全攻击。
- 参加我们的网络安全就绪度评估，接收一份以原始调查对象为基准的定制报告。查看贵组织在行业、公司规模和所在地区方面的对比结果。
- 与罗克韦尔自动化专家对话，了解我们如何帮助您制定合适的 OT 网络安全计划，以保护您的工业运营。

Rockwell Automation

关注我们。

rockwellautomation.com — expanding **human possibility**®

AMERICAS: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
EUROPE/MIDDLE EAST/AFRICA: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
ASIA PACIFIC: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Allen-Bradley 和 expanding human possibility 是罗克韦尔自动化有限公司的商标。
不属于罗克韦尔自动化的商标是其各自所属公司的财产。

出版物 GMSN-AP001A-ZH-P – 2022 年 5 月
© 2022 罗克韦尔自动化有限公司版权所有。保留所有权利。美国印刷。