



应对化工企业网络攻击的挑战

你的化工厂受到网络攻击时，能安全防护吗？——网络攻击在全球范围内持续增加，化工行业也不幸地未能避免被网络攻击。随着越来越多的化工企业开始数字化转型，这也使他们遭受到网络攻击，可能会对他们的运营造成毁灭性的后果。

文 /Ahlam Rais

目 前网络攻击对化工厂带来的直接影响是：长期停产进而造成资金和公司声誉的损失，甚至还可能导致工厂关键性基础设施被破坏，从而引发爆炸，对人的生命安全造成威胁。这些网络攻击背后的动

机通常是为了赚钱，在这种模式中，勒索软件攻击是指黑客通过非法手段获取公司的敏感信息，并威胁公开泄露他们的数据，他们甚至可能窃取公司的知识产权并将其卖给其他公司。在某些情况下，这些黑客也可能是出于政治动机，从而导致对公司资产造成最大的损害，如窃取走宝贵的数据和使工厂运转瘫痪。

对化工企业的网络攻击

化工行业目前也经常遭受到网络攻击。2019年，瀚森专用化学品公司（HEXION）和迈图高新材料集团（Momentive Performance Materials）遭受到网络攻击，这使得他们无法访问某些信息技术（IT）系统和相关数据。不过，这些公司及时采取了行动，控制住了这些“网络安全

本文作者系 PROCESS 德文版编辑。

事件”，并恢复了正常运营。近些年来，可能还有其他化工企业遭受了网络攻击，但由于事关公司声誉，这些事件都被保密得很好。

在这种背景下，保护公司的资产变得极其重要，这就是网络安全的作用所在。根据市场研究公司 Statista 的数据，全球网络安全市场的规模预计将从 2022 年的 2 400 亿美元增长到 2026 年的 3 450 亿美元。专家认为，网络安全市场大幅增长的原因是各行各业的网络攻击数量不断增加，以及数字化的兴起。

数字化转型导致网络安全需求增加

随着越来越多的化工厂向数字化转型，对网络安全的需求肯定会增加。ABB 能源行业全球网络安全业务主管 Tobias Nitzsche 解释说：“数字化转型导致化工厂中系统和设备使用增加，而这些设备和系统有可能被网络犯罪分子利用。”

此外，罗克韦尔自动化 OT 首席架构师 Gert Thoonen 还表示：“数字化转型已成为自动化行业的新趋势，还为企业之间的激烈竞争创造了新的动态环境。而采用这些新技术的企业，将通过提供新产品、新服务和更好的客户体验而占优势。但将企业中的所有资产连接在一起，也会降低企业安全性，使企业更容易被攻击，从而破坏业务连续性。”

西门子数字工业横向管理网络安全副总裁 Michael Metzler 说：“目前，全球各地的化工厂都在经历数字化转型，越来越多的公司将其现场操作机械与公司的 IT 技术结合起来，以提高效率、降低成本并获得竞争优势。然而，

随着以太网和虚拟化等 IT 标准在 OT（操作技术）系统中使用得越来越多，化工厂也会变得更容易受到网络攻击。”

他继续解释道，造成这种情况的一个主要原因是 IT 系统在设计上是开放和互联的，而 OT 系统在设计上通常是封闭和孤立的。这使得网络罪犯更容易通过 IT 系统访问 OT 系统。因此，化工企业在工厂中采用网络安全变得越来越重要。这一整体发展促使全行业标准的制定，如 IEC 62443，该标准涉及自动化和控制系统中的操作技术安全。

制定网络安全战略

在这种情况下，制定一个强有力的网络安全战略变得至关重要，因为它可以在很大程度上为化工厂安全运行护航。罗克韦尔自动化 OT 首席架构师 Gert Thoonen 强调说：“企业需要的是制定明确的网络安全战略，而不是直接照搬 IT 战略，这是企业网络安全防护重要的开始。制定一项成功战略的关键在于提高领导层面对其的认知，并且能够获得跨部门利益相关者的支持。重组 IT 和 OT 部门对于确保统一协调非常重要，因为双方都需有价值的信息来确保整个企业的安全。”

Gert Thoonen 解释说，首席信息官（CIO）和首席运营官（COO）的目标、责任和指标应相互重叠，

这将迫使他们作为一个团队一起来确保基础设施的安全。成立一个由 IT 技术人员、控制工程师、运营商、安全专家、HSE 专家、管理层和 OEM 控制制造商组成的协调联合工作组，分享他们的领域知识和专业技能，以评估和降低化工厂的风险。

在这方面，ABB 能源行业全球网络安全业务主管 Tobias Nitzsche 阐述道：“网络安全战略应该在持续改进的基础上注重价值交付。有效利用现有资源是成功的关键因素，特别是考虑到实际的 OT 网络安全资源短缺。一旦制定了要实现的计划或者战略，下一步就需要制定安全战略。制定安全计划（路线图）的下一步（路线图）将是差距分析，其中可能包括多个主题，例如审查以前的战略、政策、标准、指南、风险评估、审计和监管要求。一个好的网络战略的另一个方面是一个网络安全计划，在这个计划中，你可以衡量绩效的提高”。

当企业谈到在其化工厂采用网络安全系统的想法时，人们经常讨论投资回报率（ROI），这方面也需要注意。

网络安全系统的投资回报率（ROI）

在定义一项投资的盈利能力时，通常会考虑投资回报率。西门子数字工业横向管理网络安全副总



“数字化转型导致化工厂中系统和设备使用增加，而这些设备和系统有可能被网络犯罪分子利用。”

——Tobias Nitzsche
ABB，能源行业全球网络安全业务主管

裁 Michael Metzler 认为，当谈到化工厂的网络安全系统时，投资回报率很难量化，因为很难衡量防止可能永远都不会发生的网络攻击的成本和收益。然而，这并不意味着不应该花费金钱，网络安全是业务运营连续性的一个重要考虑因素，网络攻击的潜在代价可能是巨大的，包括经济损失、声誉损害和信任损失，甚至对人和环境的身体伤害。与网络攻击的影响相比，实施网络安全系统和措施的成本相对较低，因此，化工厂必须对网络安全进行投资。

Gert Thoonen 同意 Michael Metzler 的观点，他表示网络安全不会产生直接的投资回报率，但相关的收益是无形的，可以用公司的效率和有效性来衡量。总之，网络安全有助于更好地管理总拥有成本（TCO）。

Tobias Nitzsche 解释说：“为了更好地理解网络安全投资的投资回报率，公司相关组织应该进行风险评估，了解各种网络安全解决方案的成本和收益，将其与业务影响分析相结合，并建立一个系统来衡量其网络安全工作在一段时间内的有效性。在许多工厂中，这并不总是意味着从头开始，可能已经有现有的 Hazop 研究和 Lopa 分析，可以作为影响分析的有价值的输入。”

如果想降低化工厂遭受网络



“数字化转型已成为自动化行业的新趋势，还为企业之间的激烈竞争创造了新的动态环境。采用这些新技术的敏捷组织将通过提供新产品、新服务和更好的客户体验而占上风。而采用这些新技术的企业，将通过提供新产品、新服务和更好的客户体验而占优势。”

——Gert Thoonen

罗克韦尔自动化，OT 首席架构师

攻击的风险，企业应该采取“深度防御”的方法，包括实施多层次的安全，以保护工厂的网络和系统。Tobias Nitzsche 解释说，这可能包括以下内容。

1. 工厂安全。工厂安全采用各种方法来防止未经授权的人实际访问关键部件，从传统的楼宇进出到通过钥匙卡保护敏感区域。此外，还应包括对工厂全面保护的流程和相关规章制度。从风险分析到适当措施的实施和监测，而且需要一直定期更新。

2. 网络安全。这涉及到保护工厂的网络免受未经授权的访问和攻击。这可能包括防火墙、入侵检测系统和其他安全技术等措施，以保护工厂的网络和系统。为了保护化工厂的自动化网络免受未经授权的陌生访问，网络安全系统会监控所有接口，包括网络安全监控办公室网络和工厂网络之间的所有接口，以及远程维

护访问保护、网络分割、加密通信和零信任原则。

3. 系统完整性。包括确保工厂的系统以安全的方式进行配置和维护，以及正在运行最新的软件和安全更新。还可能包括以下安全控制等措施，以保护工厂的工业控制系统（ICS）和操作技术（OT）。定期进行渗透测试和漏洞评估，以识别和解决漏洞，这对于维护系统的完整性非常重要。自动化系统必须受到保护，以防止外部的访问和操作尝试。系统内、程序代码和知识产权内的通信尤其需要保护。

4. 非技术措施。如为员工提供网络安全培训，制定快速有效应对网络安全事件响应计划，在整个组织内营造网络安全意识文化，并与其他组织和机构合作，共享有关潜在威胁的信息和情报，对于确保化工厂的整体安全也很重要。

结语

网络安全有许多积极的方面，但有一点是可以肯定的：化工企业如果想要保障自己生产运营的安全并在市场上保持竞争力，就应该制定网络安全战略。毕竟，网络攻击随时有可能发生，化工企业一旦遭受网络攻击，损失代价将不可估量。

“目前，全球各地的化工厂都在经历数字化转型，越来越多的公司将其现场操作机械与公司的 IT 技术结合起来，以提高效率、降低成本并获得竞争优势”。

——Michael Metzler

西门子，数字工业横向管理网络安全副总裁

