

制药公司亟需加强网络安全

在敏感的制药环境中发生黑客攻击是每个运营商的噩梦——一旦发生，患者数据、生产安全、声誉，这些都岌岌可危。它甚至可能会造成高达数百万元损失。所以，制药企业万不能对网络安全掉以轻心。

文 / John Allen

近年来，网络攻击的频率和复杂程度都有所增加。根据 Check Point Research 的数据，2020 年至 2021 年间，全球范围内对企业网络的攻击增加了 50%。这些攻击可能会泄露敏感的个人数据，乃至商业机密，使公司陷入财务困境，并损害其声誉。这些威胁对各种组织都有着直接影响，迫使人们更加关注网络安全。

制药行业正成为黑客攻击受害者

与所有行业一样，制药行业也会受到这些问题的影响。默克公司在 2017 年遭遇的 Not Petya 袭击事件给该公司造成了 14 亿美元的损失。这是此类袭击造成破坏性影响的一个突出例子，但问题远不止于此。近年来，该行业在 IT(信息技术)和 OT(操作技术)方面受到的攻击不断增加，这令人担忧。

本文作者系 Radiflow 的制药顾问。

经常用于研发、生产和仓库的工业自动化和控制系统尤其容易受到影响。虽然 IT 在过去一直处于网络威胁的中心，但对 OT 系统的攻击正在增加。它们可能产生破坏性的影响，这警告着人们 OT 安全需要立即得到关注。

OT 系统的网络安全经常被忽视

OT 生态系统面临着一些关键的网络安全挑战。

首先，OT 环境通常有些分散。系统和机器操作通常分布在许多工厂、仓库和研发设施中。这种碎片化，加上近年来应数字化转型要求，在 OT 和网络之间已经建立了更牢固的连接，导致攻击面增加，从而增加了 OT 系统的脆弱性。

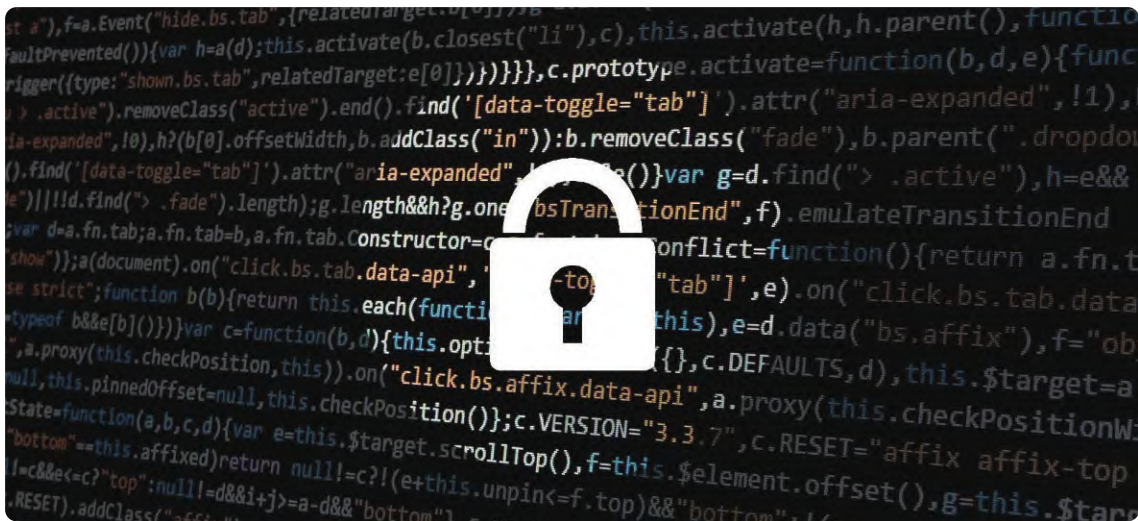
其次，OT 系统中的网络安全通常并不是各公司的首要任务。IT 运营商一般将网络安全放在第一位，其次才考虑系统的可用性和安全性；但 OT 却相反，运营商一般将安全性和正常运行时间



Radiflow 的制药顾问 John Allen 在本文中提供了加强网络安全的建议

放在首位，然后才考虑网络安全。造成这一现象的部分原因可能是 OT 系统由负责确保系统功能和安全的工程师和实验室技术人员维护，而不是由更关注网络威胁的网络安全专家维护。

在如今的环境中，潜在的削弱性网络攻击的威胁正在增加，需要通过定义和实施 OT 网络安全运营模式来重新评估。如果制药公司想避免可能会影响到运营效率、利润，甚至客户安全等方方面面的网络威胁，就必须将 OT 网



网络攻击的威胁正在增加，制药公司有必要考虑将 OT 网络安全作为更高的优先事项

络安全作为公司更高的优先事项。

但也有人认为高度关注实验室和生产设施的网络安全可能会损害公司的整体健康，以及客户和最终消费者的健康——这种想法似乎并不符合情理。当然，员工安全和系统可用性对一家公司的整体成功来说至关重要，无论是在制药行业还是其他领域，因此似乎应将它们列为最优先的事项。但是，需要注意，当前很多公司的 OT 安全规划并没有对潜在的网络威胁给予足够的关注，忽视了实际存在的网络威胁，这可能会给他们带来灾难。

很多公司都低估了黑客攻击的后果。设想一下，如果实验室或生产设施的关键系统出现安全漏洞或故障，后果将是毁灭性的：重要药品和医疗设备的生产将被推迟和减缓，无法再及时送达至需要它们的人手中。为了有效应对无处不在的网络威胁，OT 系统运营商必须拥有能够对整个 OT 网络进行持续检测和监控的工具，从而有效地优先考虑风险，并在需要时迅速采取行动保护整个生态系统。

了解 OT 网络

对于制药行业的 OT 系统运营商来说，成功应对网络风险首先要全面了解 OT 网络，并能够清楚地掌握所有设备的情况。有效的网络管理需要对网络的所有组件和拓扑结构进行全面、不间断的观察，以便无论问题或异常发生在哪里，都能快速检测到。

如果检测到问题，运营商必须有工具来识别威胁网络的内容和人。通过这种方式，他们可以评估风险的严重性，网络是否以及在多大程度上面临风险，以及入侵可能产生的影响。所有这些信息都是必要的，以便正确评估问题并准确地确定优先级。

大多数公司缺乏人力和财力，无法将同样的时间和注意力投入到所有可能的风险中。优先考虑对整个组织构成最大风险的威胁的能力至关重要。这将使公司能够优化其网络安全支出，并提高整个网络安全运营的投资回报率。

风险分析将有所帮助

除了能够应对直接威胁外，全面的网络可见性和有效识别最

大风险的能力还有助于运营商主动解决潜在的网络漏洞，并为未来的预算、风险缓解规划和弥补合规差距提供关键的决策支持。

当发现潜在威胁时，制药行业的 OT 运营商应该拥有能立即采取行动的工具。在这种情况下，建立全面的“如果……便会发生……”场景有助于运营商做出明智、安全的决策。选择方案之后，明确的跟进和报告以及准确、近乎实时的更新，将大大有助于 OT 团队解决风险，更好地了解进展，并知道问题何时得到了控制。

不幸的是，当下的网络威胁格局正在不断演变，攻击变得越来越复杂和频繁。这意味着 OT 运营商需要更新工具、流程和资源，以便对整个 OT 网络的活动进行持续实时监控。此外，他们还需要能够快速检测出可能违规的异常情况。更重要的是，能够对其做出快速反应。

传统的 OT 在当今世界已不再适用。制药公司需要认识到这一点，并立即采取行动，保护自己免受日益增长的网络风险的威胁，确保未来安全。