

药品生产企业如何应对网络威胁？

如今，制药行业不仅要应对生产现场的挑战，还要应对来自于网络的攻击——大型医药制造企业如何保护自己的运营技术（OT）网络免受安全威胁？TX One Networks 表达了自身对于网络攻击的第一手见解。

文 / Alexander Stark

PROCESS-Tip

* 更多信息请登录：
pharm.vogel.com.cn
* 反馈编码：210648



网络攻击对全社会都构成了严重的威胁，特别是对制药等敏感关键技术领域造成的损害更是不可估量

随着网络科技的进步，网络上的违法犯罪活动也越发猖獗，特别是对于敏感、关键行业（如制药行业及其制造过程）而言，所受的损失更为严重，攻击者频繁开发出恶意软件对其进行网络攻击。

网络攻击对全社会都构成了严重的威胁，特别是对制药等敏感的关键技术领域，造成的损害更是不可估量。这些不确定因素带来的威胁性后果包括：业务中断，停产，产品被污染，面临跨

时几个月的重新评估，以及危险材料泄漏和数据泄露（导致配方或成分数据的非自愿披露）。利益相关者应该得到保护，以免受到此类事件潜在致命后果的影响。

OT 面临的主要威胁

医药 OT 网络环境中最大的两个安全挑战是：第一，验证通过空隙法加入的终端设备的安全性。通过这种方法，两个互联网技术（IT）系统在物理上和逻辑上是相互分离的，但仍然允许用户数据的传输。第二，减少第三方技术人员的终端设备为企业网络带来威胁。这是因为当合作伙伴、供

应商或顾问在现场进行 IT 维护时，他们会将可能受到病毒感染的笔记本电脑或 U 盘连接到工业控制系统（ICS）网络或生产设备上。根据最近的一项调查，2020 年有 60% 的受访公司表示“恶意软件从一个员工传播到了另一个员工的工作设备上”。

传统的端点安全解决方案无法解决这些问题，因为它们是针对内部 IT 环境开发的，并不适用于医药行业。为了帮助制药行业的 OT 网络免受安全威胁，OT 安全解决方案领域的领先供应商 TX One Networks，针对大型医药制造企业如何加强生产设施的安全提出了自己的见解。

提高 OT 安全的 6 个技巧

TX One Networks 总结了提高 OT 安全的 6 个技巧。这 6 种实用技巧可以提高操作安全性，保护生产设施不受潜在网络攻击的影响。

安装移动式扫描系统：为了更清楚地了解已投入使用的 IT 系统

本文作者系本刊德文版杂志编辑

的使用状况，需要一套移动 IT 安全解决方案对恶意软件进行扫描。通过对 IT 系统的日常维护，可从设备之间扫描出恶意软件并进行跟踪采集，尽早发现威胁，防止网络病毒隐藏在本地文件中。

例行的“纯日志”网络安全检查：对于敏感的生产设施，企业应部署一个可执行的“纯日志”扫描解决方案，扫描结果只需简单地记录和存档。安全专员和 IT 管理员通常更喜欢能够生成扫描日志的扫描器。不对检测到的威胁立即采取行动的好处在于，他们在操作中可以避免删除关键业务的程序或文件。如果需要的话，企业还可以采取更加谨慎的方式来消除威胁。

检查“端点漏洞”：在设备检查期间收集到的数据可以用来了解生产中的每个终端设备上安装了哪些补丁和应用程序，识别未打补丁的设备、资源或已经过期的操作系统（所谓的“报废操作系统”）。

彻底的即插即扫安全检查：每一台部署在制造工厂现场的终端设备都必须通过检查点，对可能隐藏在设备内部的 IT 安全威胁进行扫描。因此，一个能够在各个终端设备之间进行方便快捷交换的移动扫描解决方案是必不可少的。

集中记录资产信息和扫描结果：从全厂甚至全企业的角度来看，获取到企业的 IT 信息是轻而易举的。为了简化审核流程，制药企业应建立固定的审核程序（或称“审核追踪”）以确保合规性。这样一来，制药企业便能轻松地将安全计划或 IT 状态文档传递给供应链的所有利益相关者（包括医院、药房和其他医疗机构）。

优化安全运营中心：一个理想的 SIEM（安全信息和事件管理）系统在使用时——通过启用集中组织的日志和事件记录——应尽可能地操作便捷，而与公司正在研究的 IT 安全生产设备的制造方式无关。例如，日志应易于导出到 SIEM 系统，如 QRadar 或 Splunk。理想情况下，公司应保持数据完整性并以某种方式进行存储。除此之外，还要满足诸如临床研究中患者安全的要求以及其他法律要求。

当不安全的移动设备被带到生产现场并到达企业的 IT 控制点时，必须对其进行快速而彻底的安全扫描。用于证明合规性和监测生产设备的记录系统应被设计成使用方便且适合日常工作的程序。公司安全理念中的每一个流程都应该尽可能简单、直观。便携式端点安全解决方案可有效保护制药行业的 OT 网络，在应对复杂多样的安全挑战时常常发挥着重要作用。当遇到有量身定制的移动解决方案需求时，这种方法的效果最好。

移动安全解决方案也被称之为便携式安全解决方案，可帮助工业控制系统的所有者和运营商对恶意软件进行扫描，并在独立计算机和空隙式系统中收集与安全相关的信息。这些基于 USB 的解决方案已经包含所需的扫描软件，因此无需在目标系统本身上安装安全软件，可以更加轻松地检测和删除恶意软件。这样一来，制药企业按照自身的需求可以随时进行恶意软件的扫描操作，而不用担心被扫描设备的性能下降。可以说，移动安全解决方案既简化了安全扫描过程，也使得用户能够从证明合规性中受益。 ●



上海意发玛制药设备有限公司

E-PHARMA (SHANGHAI) PHARMACEUTICAL EQUIPMENT CO., LTD



We Are **E-Pharma**,
我们是 **意发玛**,
Sanitary Heat Exchanger
卫生级换热器
Supplier.
提供商。

专业、专注、精益求精
Specialized, Focus, Try for the Best

www.e-pharmatech.net
E-mail: info@e-pharmatech.net
Tel: +86-21-32503721 32503722



广告