精译版

可见性是增强 ICS 安全的关键

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	Look, But Don't Touch: One Key to Better ICS Security		
原文作者	Sara Peters	原文发布日期	2017 年 6 月 26 日
作者简介	Sara Peters 是 Dark Reading 的高级编辑。http://www.darkreading.com/author-bio.asp?author_id=524		
原文发布单位	Dark Reading		
原文出处	http://www.darkreading.com/vulnerabilities---threats/look-but-dont-touch-one-key-to-better-ics-security--/d/d-id/1328987?		
译者	安天技术公益翻译组	校对者	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块		
免责声明	• 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 • 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 • 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 • 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。		

可见性是增强 ICS 安全的关键

Sara Peters

2017 年 6 月 26 日

更好的可见性对于改善工业控制系统（ICS）和关键基础设施的网络安全至关重要，但是这要求 OT（操作技术）和 IT（信息技术）进行融合。

我们应该如何解决工业控制系统的网络安全问题呢？

专家说，更好的可见性对于提高 ICS/SCADA 的安全性至关重要。但是，除非信息安全团队停止用 IT 专家的眼光来看待 ICS 环境，否则他们永远不会获得这种可见性。

专家说，IT 和 OT 的装备、流程和人员有着根本的差异。

GE 石油天然气集团网络安全和风险团队的高级安全总监保罗·布拉格（Paul Brager）说："总的来说，IT 人员不知道如何运行 OT 环境。"

"互联网的成功使得计算机领域的人感到自豪。" ICS-ISAC 主席兼 Unisys 工业控制系统全球总监克里斯·布莱克（Chris Blask）表示。然而，工业工人"知道这个社会如何运作"，比如不能将生活污水混入饮用水。

因此，在网络安全专家担心 ICS 恶意软件攻击国家电网时，OT 工程师们担心的是，他们的发电站和生产线可能不只会被黑客破坏，还面临其他威胁。他们非常了解这一点，因此他们坚持广泛的过程安全管理控制、危害分析、变更管理、应急响应，事件调查规则等等，以便及早和迅速地应对这些威胁。

将任何新事物（新泵、软件补丁、升级、新安全工具）引入操作环境必须要非常慎重，因为任何对可用性或完整性的干扰都有可能导致不可逆转的、代价高昂的甚至危险的物理影响。

最糟糕的结果是持续停电、水坝破裂、核崩溃和公共供水系统污染，除此之外，还会导致经济影响。没有经过充分测试的软件补丁一旦被释放到化工厂的操作环境中，其系统可能会在生产过程发生故障或脱机，即使时间很短，化工厂也会遭受严重的损失。"这可能要报

废价值 10 万美元的产品。”布拉格说。

“任何 CEO 都不会因为要去修复貌似没有损坏的设备（如不受支持的操作系统）而同意停止抽油一周。”OT 安全公司 Claroty 的联合创始人和西门子工业安全服务前全球总监加利纳·安托娃（Galina Antova）解释说。说服他们相信网络安全面临威胁非常困难，更不用说让他们花钱解决了，她说。

企业 IT 环境可以承受比 OT 环境更多的迭代和停机时间。如果 OT 环境是稳定、运行和高效的，那么为什么要做些可能会使它变得不稳定的改变呢？

PAS 首席执行官埃迪·哈比比（Eddie Habibi）解释说，目前运行的许多物理和网络-物理系统已经用了“几代”了。

正如这些专家所说，OT 人员的一般态度是：如果设备没有损坏，就不要改动。因此，信息安全专家面临的挑战是：说服 OT 人员相信有些设备已经损坏了，然后在事态变得更糟之前修复它们。

看到他人看不到的东西

正如布莱克所说，ICS 是“提供对物理过程的可见性的系统”，它们唯一不可见的就是 ICS 系统本身。

布拉格说：“可见性是一个大问题，在面对网络物理系统时，我们通常没有很多的可见性。”当出现问题时，“你无法确定这是网络原因还是人为原因。”

哈比比说，不幸的是，“这些系统不容易被发现”。正如他所解释的，工业环境通常是一个非常复杂的专有系统，通过不同的协议进行通信，需要一定的专业知识才能运行。

布拉格补充说，许多 OT 系统已经不再受支持，供应商可能已经不存在了。其中的一些系统只能通过一个协议通信。

哈比比说：“由于人们不断地增加自动化功能，因此这种情况不断恶化。”

这种 IT-OT“融合”为环境增加了更多的传感器、更多的 I/O 卡、更多的端点、更多的协议、更多的互连和更高的复杂性，使得情况更加糟糕。

“除非你可以直观地看到资产，”布拉格说，“否则很难询问它...但是如果你不知道你有

哪些设备，你就不知道你有多脆弱。”

此外，他指出，大量工业环境通常由具有访问权限的第三方管理。布拉格说，他们应该对此进行记录，包括谁运行什么，在哪里运行。

不过，哈比比表示，呼吁这些第三方承包商和托管服务提供商进行人工记录比“什么都不做更糟糕”。

怎么做

根据布拉格的说法，每当安全团队或公司提出“嗅探”或“积极询问”这些术语时，“这些工厂中的人就会紧张”。

他解释说，对企业 IT 经理来说非常温柔的姿态可能会被操作工程师认为是危险的入侵。工业过程不能容忍有可能引入的新延迟，如果某些机械系统损坏而无法恢复，则需要更换。

布拉格说：“如果你说‘我们要安装一个代理’，他们会说‘不行，你不能安装’”。

这并不能改变必须提高可见性的事实。没有可见性，攻击威胁可能会比一些 OT 团队意识到的更加严重，因为攻击者可能比操作者具有更好的可见性。

因此，ICS 安全团队的目标是，Antova 说，“以被动的方式提高可见性……这是我可以做的，只要不影响工程师的流程，他们将允许我这样做。”她说，这也能用最低投资获得最大的收益。

哈比比也敦促同样的做法。被动地评估环境中的所有组件，然后检查所有组件的漏洞，将该信息提供给操作员，并允许他们采取行动（或不采取行动）。“如果你想修复那些损坏的窗户和门锁，”他说，“那就实施一个非常严格的变更管理流程吧。”

但是，布拉格警告说，要仔细测试产品，因为一些承诺“被动监控”的供应商比他们声称的被动性更被动。

由于 ICS 与安全流程和变更管理有关，因此，OT 和 IT 团队将有机会聚在一起。

布莱克说：“很多事情都归结于礼貌问题。你不做的事情恰恰是安全团队经常做的，如果你因为这个指责别人，那就不要怪别人不再邀请你参加会议了。”