简译版

工业环境中七大安全“漏洞”

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	The Seven Leading Security Gaps in Industrial Environments		
原文作者	Barak Perelman	**原文发布日期**	2018 年 10 月 30 日
作者简介	Barak Perelman 是工业网络安全公司 Indegy 的首席执行官。		
原文发布单位	Security Week		
原文出处	https://www.securityweek.com/seven-leading-security-gaps-industrial-environments		
分享地址	请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块		
译者	安天技术公益翻译组	**校对者**	安天技术公益翻译组
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。		

工业环境中的七大安全“漏洞”

Barak Perelman

2018 年 10 月 30 日

每年 10 月是美国“国家网络安全意识月”（NCSAM）。今年，该活动的关键任务之一是寻求各方合作，以保护关键基础设施免受网络威胁。

显然，运营技术（OT）网络中的安全漏洞正在成为重要的关注点。

例如，卡巴斯基最近的一项研究（PDF）指出，77%的工业环境安全专家认为他们的企业很有可能成为网络安全事件的目标。其中，48%的受访者表示他们没有特定的运营技术/工业控制系统（OT/ICS）事件响应计划，31%的受访者则表示他们的企业在 2017 年经历过一次或多次攻击事件。

借此契机，我们来谈一谈工业环境中的七大安全“漏洞”。

恶意软件从 IT 转向 OT

在过去的几年中，“魔窟”（WannaCry）和 Petya 是最严重的两个恶意软件威胁。它们虽然不是专门针对工业网络的，但确实影响到了工业网络。这些威胁证明，IT 和 OT 网络各自以及它们之间的薄弱安全防御，使 OT 网络不可避免地受到攻击。

WannaCry 导致巨大破坏的主要原因是：它的攻击目标是运行过时 Windows 系统版本（如 Windows XP）的企业，这些系统已经无法再接收安全更新和补丁，存在严重的安全漏洞。

最佳实践：企业既要保护 IT 网络，也要保护 OT 网络。这意味着，他们要及时更新所有操作系统和应用程序、安装强大的杀毒软件，并监控 IT 和 OT 网络的所有威胁。

迷信“物理隔离”

直到最近，工业网络还是通过“物理隔离”（air gap）与其他网络分离开来的。理论上，物理隔离是一种很好的安全措施，能够将工业网络与业务网络分开，从而保护工业网络。然而，在当今以互联网为中心的世界中，IT 和 OT 网络日益混杂，物理隔离已经不复存在，导致 OT 网络更容易受到攻击。

最佳实践：关注基于互联网的威胁，特别是跨越 IT 和 OT 网络的工业物联网（IIoT）设备产生的威胁。

攻击热门 OT 工具

今年 5 月，Tenable Research 公司发布了一份告警，指出施耐德电气（Schneider Electric）的两款应用存在漏洞，这两款应用被美国广泛用于管理石油、天然气等行业的工业流程。

这些漏洞凸显了网络安全供应商和内部安全团队的弱点，这两者都为 IT 部门投入了大量资源，但是忽视了工业环境。

最佳实践：必须对 OT 操作系统及其上安装的所有软件打补丁。如果无法修复关键设备，则必须部署能够检测行为变化的监控工具。

不安全的控制器普遍存在

如今，许多拥有 OT 网络的企业面临着巨大的挑战——在保持运营效率和提高网络安全性之间取得平衡。面临该挑战的原因是，企业将存在漏洞的老旧控制器和较新的、基于互联网的控制器混合使用。

老旧控制器缺乏新技术中常见的关键安全功能，因此容易受到攻击。此外，企业通常不会更新或修复老旧系统，他们更注重运营效率而非网络安全。

最佳实践：保持实时的可见性——及时了解网络的各个方面以及每台设备上的每个操作，查看受信内部人员和未知源执行的所有活动，并确定是否对其授权。

内部威胁

如果因为意外或疏忽而对 OT 网络做了更改（不管是员工还是第三方承包商做的更改），可能会导致与外部攻击一样具有破坏性的后果。

最佳实践：通过告警系统，保持对网络活动和设备完整性的实时可见性——当发生更改时能够及时发现。此外，必须拥有全面的意外险。

心怀不满的员工

如果心怀不满的员工窃取代码、破坏生产线或者在关键配方中“投毒”，其影响可能是

灾难性的。

最佳实践：保持对网络的实时可见性，可能无法阻止心怀不满的员工执行恶意活动，但能够迅速识别威胁。理想情况下，企业应部署分析网络流量的入侵检测系统，并积极进行设备完整性检查，以识别威胁。

缺乏“未雨绸缪”

如今，首席信息安全官（CISO）关注的主要问题之一是业务风险。为了最大限度地降低风险，企业通常采用自上而下的方法，尽可能有效地保护所有技术。但是在 OT 领域，企业很少采用这种坚实的方法——许多企业的 OT 网络并未遭到攻击，因此他们认为无需担心。

最佳实践：OT 人员需要改变这种思维，积极主动地保护 OT 网络的安全，降低网络中所有设备和应用程序的风险。

安天简介

安天是引领威胁检测与防御能力发展的网络安全国家队，始终坚持自主先进能力导向，依托下一代威胁检测引擎等先进技术和工程能力积累，研发了智甲、镇关、探海、捕风、追影、拓痕等系列产品，为客户构建端点防护、边界防护、流量监测、导流捕获、深度分析、应急处置的安全基石。安天致力于为客户建设实战化的态势感知体系，依托全面持续监测能力，建立系统与人员协同作业机制，指挥网内各种防御机制联合响应威胁，实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报有机结合，推动客户整体安全能力建设的叠加演进。安天为网信主管部门、军队、保密、部委行业和关键信息基础设施等高安全需求客户，提供整体安全解决方案，产品与服务为载人航天、探月工程、空间站对接、大飞机首飞、主力舰护航、南极科考等提供了安全保障。

安天是全球基础安全供应链的核心赋能方，全球近百家著名安全厂商、IT 厂商选择安天作为检测能力合作伙伴，安天的威胁检测引擎为全球超过三十万台网络设备和网络安全设备、超过十四亿部智能终端设备提供了安全检测能力。

安天技术实力得到行业管理机构、客户和伙伴的认可，已连续五届蝉联国家级安全应急服务支撑单位。安天是中国应急响应体系中重要的企业节点，在“红色代码”、“口令蠕虫”、“心脏出血”、“破壳”、“魔窟”等重大安全威胁和病毒疫情方面，实现了先发预警和全面应急响应。安天针对“方程式”、“白象”、“海莲花”、“绿斑”等几十个高级网空威胁行为体及其攻击行动，进行持续监测和深度解析，协助客户在“敌情想定”下形成有效防护，为捍卫国家主权、安全和发展利益提供了有力支撑。

2016 年 4 月 19 日，在习近平总书记主持召开的网络安全和信息化工作座谈会上，安天创始人、首席架构师作为网络安全领域的发言代表，向总书记进行了汇报。2016 年 5 月 25 日，习近平总书记在黑龙江调研期间，视察了安天总部，并对安天人说，“你们也是国家队，虽然你们是民营企业”。

安天实验室更多信息请访问： *http://www.antiy.com（中文）*

http://www.antiy.net（英文）

安天企业安全公司更多信息请访问： *http://www.antiy.cn*

安天移动安全公司（AVL TEAM）更多信息请访问： *http://www.avlsec.com*