

简译版

## 工业网络的最新威胁：远程用户

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	Industrial Networks' Newest Threat: Remote Users		
原文作者	戴夫·温斯坦 (Dave Weinstein)	原文发布日期	2020 年 5 月 1 日
作者简介	戴夫·温斯坦是 Claroty 的首席安全官。		
原文发布单位	Dark Reading		
原文出处	<a href="https://www.darkreading.com/endpoint/industrial-networks-newest-threat-remote-users/a/d-id/1337662">https://www.darkreading.com/endpoint/industrial-networks-newest-threat-remote-users/a/d-id/1337662</a>		
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 <a href="https://bbs.antiy.cn">bbs.antiy.cn</a> 安天公益翻译板块		
免责声明	<ul style="list-style-type: none"> <li>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。</li> <li>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。</li> <li>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。</li> <li>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。</li> </ul>		

## 工业网络的最新威胁：远程用户

戴夫·温斯坦

2020 年 5 月 1 日

随着远程办公成为常态，人们需要远程访问其组织的网络，以及服务器、电子邮件和数据才能完成工作。但是随着愈来愈多的员工和组织开展远程办公，远程访问也可能使组织面临安全风险。

当我们特别关注工业网络以及负责维护、运营与保护它们的组织时，就会发现工业网络存在着更大的安全风险。现在，确保这些网络的安全比以往任何时候都更为重要。这些工业网络——电网、制造工厂、石油和天然气以及交通运输网络等——对我们国家的基础设施至关重要。但是由于我们的工作环境现在发生了变化，这些网络正在被来自世界各地的人们（而不仅仅是现场人员）访问和维护。如果这些网络遭到攻击，则可能会损坏城市的电网，或者关闭对制造工厂系统的访问权限，从而造成严重的后果。

此外，Claroty 最近的调查数据显示，63% 的美国安全专家预计，未来五年内美国关键基础设施将遭受重大网络攻击，这表明网络安全专家对其工业网络的安全和保障缺乏信心。此外，有 51% 的美国工业从业者认为，当今的工业网络没有得到适当的保护，需要更多的保护，而 55% 的人则认为美国的关键基础设施容易受到网络攻击。

工业网络面临的风险非常高，而且我们知道远程办公在短时间内不会结束，所以对工业组织来说，加强基础设施的安全越来越重要，保护他们的远程访问点和远程用户则是这样做的关键。

尽管这看起来很容易，但是这些组织仍需要克服各种远程访问挑战。

第一个挑战与员工紧密相关。随着越来越多的员工从家里连接企业网络，远程访问风险对于任何企业来说都是可怕的，而对于那些在关键基础设施中工作的人来说，风险要高得多。

虽然远程访问为无法在办公室办公的员工提供了灵活性，但这也意味着员工可能会连接到不安全的 Wi-Fi 网络或 VPN，而且他们甚至可能没有意识到这一点。如果他们的 Internet 连接不安全，那么浏览器活动、密码和敏感的公司数据可能会被暴露，甚至容易受到恶意活动的攻击。

企业面临的另一个挑战是保护员工的密码安全，因为远程办公人员通过电子邮件、聊天、文本等方式共享密码和登录信息的情况并不少见。如果这些信息被错误的人访问，落入错误的人手中，或者被企业外部的人发现，公司可能会面临隐性成本、数据泄露和声誉受损。

这些挑战为黑客或外来威胁给工业网络造成严重破坏提供了可能性——如今越来越多的人处于远程状态，这种可能性就更大了。想象一下：拥有员工密码（他们在不安全的 Wi-Fi 网络上从员工会话中窃取的密码）的黑客合法地登录该工业组织的网络，并破坏工厂或工厂中的关键流程。这并不是不可能发生的场景。我们最近的调查还显示，56%的人认为黑客攻击将是 2020 年针对工业网络的最普遍的网络攻击类型，其次是勒索软件（21%）和破坏活动（12%）。

除了与员工相关的风险外，还有第三方供应商和承包商带来的风险。许多工业组织使用服务提供商或顾问来帮助监控网络并提供额外的支持或服务，并且随着远程办公的增加，这些工作人员也需要远程访问企业的网络。因为这些供应商没有像全职员工那样直接连接到内部系统，所以他们的访问可能不会受到严格的监管或监控。这意味着，如果恶意行为者劫持了供应商（访问企业网络）的远程会话，那么攻击者的访问可能不会在第一时间被检测到，从而给攻击者提供了巨大的机会来进行破坏。

与第三方供应商相关的另一个问题是，传统的网络访问设置对于系统管理员来说是非常耗时的，因此，在他们的待办事项列表中，并不总是优先考虑这一点。另一方面，由于供应商实际上不是企业的一部分，所以它们可能不像全职员工那样重视安全。

像远程办公一样，当今社会中某些工作外包给第三方的情况也越来越普遍，企业需要更加强调确保企业内部或外部的每个具有远程访问权限的个人都得到广泛的培训，并使用适当的安全协议进行适当的监控。

全世界正在努力尽快实现远程办公，这为所有行业的企业带来了重大的安全挑战，而关键基础设施面临的风险尤其高。为确保企业尽其所能保护远程访问的安全，必须严格控制网络访问并确保监控所有远程会话（无论是内部的还是外部的）。

## 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，始终坚持自主先进的能力导向，依托下一代威胁检测引擎等先进技术和赛博超脑大平台工程能力积累，研发智甲、探海、镇关、捕风、追影、拓痕等系列产品，为客户构建 endpoint 防护、流量监测、边界防护、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的有机结合，协助客户开展深度结合与全面覆盖的体系化网络安全规划与建设，支撑起协同联动的实战化运行，赋能客户筑起可对抗高级威胁的网络安全防线。

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企业、IT 企业选择安天作为检测能力合作伙伴，目前，安天的威胁检测引擎为全球超过八十万台网络设备和网络安全设备、超过十七亿部智能终端设备提供了安全检测能力。安天的移动检测引擎获得国际知名测试机构颁发的 2013 年度权威评测奖项。

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（如 APT 组织）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，通过深度分析高级网空威胁行为体的作业能力，安天建立了以实战化对抗场景为导向的能力体系。

安天被行业管理机构、客户和伙伴广泛认可，已连续六届蝉联国家级安全应急支撑单位，是中国国家信息安全漏洞库六家首批一级支撑单位之一，亦是国家网络与信息安全信息通报机制技术支撑单位，国家信息安全漏洞共享平台成员单位。

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>