简译版

企业需了解物联网供应链风险

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	What Organizations Need to Know About IoT Supply Chain Risk		
原文作者	丹尼尔·多斯·桑托斯（Daniel dos Santos）	**原文发布日期**	2020 年 7 月 20 日
作者简介	丹尼尔·多斯·桑托斯是 Forescout Technologies 的研究经理。		
原文发布单位	Dark Reading		
原文出处	https://www.darkreading.com/iot/what-organizations-need-to-know-about-iot-supply-chain-risk/a/d-id/1338348		
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。		

企业需了解物联网供应链风险

丹尼尔·多斯·桑托斯

2020 年 7 月 20 日

如果企业希望限制诸如 Ripple20 之类的漏洞所带来的风险，需考虑以下因素。

当企业将数十亿台联网设备纳入公司网络中时，他们真的了解这些设备的组件，及其可能带来的风险吗？答案通常是否定的。

这是因为物联网（IoT）和生产（OT）设备的供应链较为复杂。公司可能从其了解并信任的制造商那里购买设备，但是他们可能没有意识到，用于感染这些设备的某些基础软件和组件可能是由另一家制造商制造的。

在最近披露的 Ripple20 事件中，Treck 的 TCP/IP 网络堆栈中发现了 19 个漏洞；而这些网络堆栈被各大供应商用于数百万种常见设备，包括工业控制系统、医疗设备、企业网络设备和打印机等。

实际上，这并非 IoT 和 OT 设备供应链漏洞的唯一案例。这类漏洞已在网络安全界引起了广泛关注。在过去的一年中，人们对设备及其组件的制造商的安全性愈发担忧；而美国政府则以国家安全为由，禁用了多家中国设备制造商。最近，特朗普总统签署了一项行政命令，禁止采购、进口、转让或安装与任何外国对手连接的大功率系统电气设备，并呼吁识别已经投入使用的此类设备。

IoT 和 OT 的庞大规模进一步放大了这些设备的风险。Gartner 预测，到 2021 年，将有 250 亿台联网设备。供应链中某个组件的一个漏洞可能会影响多家制造商的设备。据估计，仅 Ripple20 漏洞就影响了数亿台设备。

如果企业希望限制此类漏洞带来的风险，需考虑以下因素。

识别具有供应链风险的设备

在 IoT、IT 和 OT 设备方面，尽管有一些行业要求提供“软件物料清单”（SBOM），但基本制造商是不会提供的。这意味着，制造商没有义务披露设备的组件。当典型的设备或软件漏洞被披露后，企业可以轻松地使用诸如设备可见性和资产管理之类的工具来查找和修补

其网络上存在漏洞的设备。但是，如果不要求制造商披露内部组件，则很难确定哪些制造商或设备可能会受到诸如 Ripple20 之类供应链漏洞的影响，除非制造商自行予以确认。

对于企业而言，要想应对这一挑战，在制定购买决策时应要求制造商提供相关组件的信息。虽说仅基于安全性做出采购决策是不现实的，但是这些供应链挑战的性质要求企业至少要获取相关信息以进行最佳风险计算。

一种风险 vs 多种设备

供应链风险的特别之处在于，一个漏洞会影响多种设备。例如，Ripple20 会影响 IT 和 OT 网络上的各种设备，包括工业控制系统、医疗设备、企业网络设备和打印机。发现漏洞的公司 JSOF 估计，该漏洞会影响全球多家制造商和数亿台设备。尽管这只是一个例子，但这种现象放大了供应链漏洞的风险。

对于企业而言，这意味着 Ripple20 漏洞带来的风险很可能已经存在于其环境中。尽管受影响的制造商仍在生产设备，但是企业可以识别已知的受影响设备并采取适当的风险缓解措施。

发布补丁的困难

一旦发现此类漏洞，则由软件或组件制造商来发布补丁。但是，设备制造商负责分发补丁，并由最终用户应用补丁。这意味着，补丁需要由一家制造商发行，然后由第二家（或者更多）制造商识别和合并，然后推给最终用户，最终用户必须自己应用该补丁。这是一个复杂的供应链。

所有这些步骤均假定，设备制造商可以实施修复。但是，制造商有可能倒闭或不再支持涉事设备，这意味着必要的安全更新可能无法传递给最终用户。在这种情况下，企业需要通过对网络进行分段来隔离这些设备，或者将这些设备从网络中删除。

应用补丁的挑战

即使解决了所有这些障碍并向最终用户交付补丁，仍然可能无法修复漏洞。发生这种情况的原因有很多，其中包括无法承受停机时间、无法更新设备或无法运行旧版应用程序以及已打补丁的软件等。无论是什么原因，企业都必须通过网络分段之类的安全解决方案来减轻这种风险，这种解决方案可以将漏洞设备局限在网络的某个部分。

企业如何应对供应链风险？

在上文，我们介绍了企业可以采取的保护措施，这些措施与缓解其他类型的网络安全风险时所采取的措施相似：盘点和修复已知的漏洞设备，对网络进行分段以防止通过危险设备的初始访问或横向移动，以及持续监控网络中是否存在感染迹象。

在将任何设备连接到网络之前，企业还应该通过考虑以下问题来评估其制造商：

- 是否使用安全的开发生命周期（包括源代码审查和渗透测试）来减少 IoT 设备中的漏洞数量？测试是否涵盖第三方组件？
- 是否实施诸如地址空间布局随机化（ASLR）和数据执行保护（DEP）等缓解措施，以减少设备中仍然存在的漏洞的影响？
- 是否具有安全更新计划，以便在发现漏洞时进行修复？这些更新是否安全交付？企业是否可以控制何时应用这些更新？
- 企业是否了解制造商的设备中包含哪些软件和硬件组件？
- 企业是否可以溯源制造商及其供应商？（这一点越来越重要，尤其是对于政府机构而言。）

根据这些问题的答案，企业可以做出明智的风险决策，并更有效地监控其 IoT 设备的安全状况。

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，为客户构建端点防护、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