简译版

如何应对 IoT 设备安全问题

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	Where should companies start when it comes to device security?		
原文作者	马克·哈里斯（Mark Harris）	**原文发布日期**	2022 年 3 月 31 日
作者简介	马克·哈里斯是 Finite State 首席产品经理。		
原文发布单位	Help Net Security		
原文出处	https://www.helpnetsecurity.com/2022/03/31/devices-security/		
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		
摘要	虽说设备制造商无法保证其设备是坚不可摧的，但他们在满足客户的产品需求时还是应优先考虑安全性。一方面，这对于保护产品大有帮助。另一方面，通过向客户展示其在风险缓解方面所做的努力，制造商能够获得客户的信任。		
免责声明	本译文不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天集团一律不予承担。		

如何应对 IoT 设备安全问题

马克·哈里斯

2022 年 3 月 31 日

物联网（IoT）市场的安全问题正在演变为业务问题。Ponemon Institute 最近的一项调查显示，59%的嵌入式产品安全决策者认为产品安全问题导致其收入减少了。

如今，联网设备制造商不断增加产量以满足快速增长的行业需求。管理咨询公司 McKinsey 预测，到 2030 年，物联网的市场价值将达到 5.5-12.6 万亿美元之间。因此，IoT 制造商需要一种能够随着不断增长的市场而扩展的安全策略。但是，目前 IoT 设备的安全性远没有其他领域那么成熟。

IoT 设备容易发现和访问，且与物理系统的连接越来越多。因此，它们更容易受到机会主义攻击者和更高明的民族国家攻击者的攻击，这些攻击者试图执行分布式拒绝服务（DDoS）攻击，组装僵尸网络，对关键环境进行网络-物理攻击。

IoT 安全基金会最近发布的一份报告显示，只有 21.6%的公司拥有可检测漏洞披露策略，而另外 78.4%的公司，其策略无法通过阈值测试。

许多设备制造商努力在不牺牲生产力或产生巨额成本的情况下考虑产品的安全性。在 Ponemon 的调查中，大多数受访者表示，“缺乏资源”（62%）和“缺乏专业知识”（60%）是其扩展产品安全工作的最大障碍。这表明，安全性并非他们的行政优先事项，这会对现实世界产生负面影响。在调查中，只有 27%的受访者表示公司领导要求提供产品安全证明；而 94%的受访者认为，最近的供应链攻击事件对其安全优先事项产生了中度或高度影响。

客户也在关注产品的安全性。根据 Ponemon 的研究，76%的受访者表示其客户将设备安全的重要性列为 7 分或以上（总分为 10 分）。确保联网和嵌入式产品的安全性对于保持企业的竞争力至关重要，接下来我们将分析设备制造商应如何大规模地创建安全产品。

确定基线

企业无法保护他们看不到的东西。如果企业不了解嵌入式设备固件中的所有组件（在 Ponemon 的研究中，70%的受访者无法为其设备创建“软件材料清单”[SBOM]），那么其

安全工作就会存在很大的盲点。

确定基线有助于企业了解固件中存在哪些漏洞，并在企业寻求改善设备的安全状况时为其提供一个起点。对于许多制造商而言，渗透测试是一种常见的基线安全策略，但此类测试难以扩展且无法实现自动化。

根据最近的一项研究，如今商业第三方代码比企业内部开发的代码更为常见。相比于针对内部开发的代码发动定制攻击，攻击者更有可能利用广泛使用的组件中的漏洞发动大规模攻击。如果企业想在不与供应商合作的情况下了解设备中的漏洞，可以通过二进制文件分析进行基线安全测试。通过发现组件并识别其代码 ping 的服务器，企业可以了解数据的去向以及设备中运行的软件。

如果不对二进制文件进行基线测试，企业在关键环境中部署的设备中可能会存在重大安全漏洞。

检查凭证和证书

分析固件的配置（包括硬编码凭证），是产品测试中的一个重要步骤。硬编码凭证通常在配置阶段生成，有的企业则是在完成安全测试之后生成。在最糟糕的情况下，机会主义攻击者可以不费吹灰之力，利用这些凭证获得 root 访问权限。

一些产品风险并非来自攻击者，而是源自法律问题。在部署产品前，企业应确保其安全证书是最新的，这一点很重要。如果证书过期且固件不知道需获取新证书，则设备可能会被禁用。

符合合规标准

虽说设备制造商无法保证其设备是坚不可摧的，但他们在满足客户的产品需求时还是应优先考虑安全性。一方面，这对于保护产品大有帮助。另一方面，通过向客户展示其在风险缓解方面所做的努力，制造商能够获得客户的信任。

企业可以通过“自愿遵守标准和指南”为客户提供安全保证。去年 8 月，美国国家标准与技术研究院（NIST）发布了消费者 IoT 设备的基线安全标准，并于 12 月发布了四份文件，提供了更多指导。

还有一个针对汽车、航空、医疗和信息技术等行业的私人监管组织网。这些信息共享和

分析中心（ISAC）能够为其成员提供降低风险和增强弹性恢复能力的工具。

NIST 预计将在 2022 年推出一项标签计划，以应对 IoT 安全问题。目前，制造商可以遵循现有指南，为客户提供一个了解其安全流程的窗口，以便在该标准生效之前让客户安心。

企业采用这些组织发布的指南，其原因各不相同，包括增强产品安全性，提高收入等。通过识别设备中的组件并对其进行测试，制造商可以在追赶产量的同时优先考虑设备的安全性。

安天简介

安天致力于全面提升客户的网络安全防御能力，有效应对安全威胁。通过 20 余年自主研发积累，安天形成了威胁检测引擎、高级威胁对抗、大规模威胁自动化分析等方面的技术领先优势，打造了面向服务器、云、虚拟化、容器和传统办公节点等提供全防御能力覆盖的智甲安全产品家族，满足客户对于包括终端杀毒、终端防护（EPP）、终端检测与响应（EDR）、云工作安全防护（CWPP）等系统安全层面需求；整合强化包括 ATID 威胁情报门户、追影沙箱和捕风蜜罐等产品在内的威胁情报板块产品，有效提升客户情报赋能和自主情报生产能力；基于流量产品探海有效应对客户对于网络威胁检测与响应（NDR）和网络流量分析（NTA）的安全需求，相关产品可以实现交叉联动，统一管理，形成面向从勒索软件到高级威胁（APT）的纵深安全防线。同时打造威胁对抗、威胁猎杀、威胁巡检服务三款主打安全服务，辅以平台支撑、快速到达的轻量级垂直响应服务，以运营模式有效支撑应对综合威胁对抗能力升级。

安天为网信主管部门、军队、部委、保密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，已连续七届蝉联国家级网络安全应急支撑单位。安天参与了 2005 年后历次国家重大政治社会活动的安保工作，获得杰出贡献奖、安保先进集体等荣誉称号；自 2015 年来，安天的产品与服务为包括载人航天、探月工程、空间站对接等历次重大航天飞行任务，以及大飞机首飞、主力舰护航、南极科考等重大任务提供安全保障支撑。

目前，安天的威胁检测引擎为全球超过一百万台网络设备和网络安全设备、超过三十亿部智能终端设备提供了安全检测能力，已经成为“国民级”引擎。

安天已发展成为以哈尔滨为总部基地，建有六地研发中心、两个控股子公司，参与一个国家工程实验室建设，拥有两个省级工程中心和重点实验室、一个博士后创新创业基地和多个高校联合实验室的集团化创新企业，同时在多地设有办事处和应急响应站，为客户提供全面的安全服务与技术支持。

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