保护物联网设备

简译版

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	Securing IoT from the ground up		
原文作者	大卫·诺西博（David Nosibor）	**原文发布日期**	2022 年 2 月 16 日
作者简介	大卫·诺西博是 UL 公司平台安全解决方案主管。		
原文发布单位	Help Net Security		
原文出处	https://www.helpnetsecurity.com/2022/02/16/securing-iot/		
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	在保护 IoT 设备方面，我们面临着三个主要障碍：（1）不断增加的网络安全风险；（2）网络安全专业知识的匮乏；（3）复杂、不断变化的全球监管环境。IoT 生态系统中的每个环节（从芯片到云设备制造商、供应商、系统集成商和其他利益相关者）不仅要降低网络安全风险，还要满足合规性，他们的任务异常艰巨。		
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。		

保护物联网设备

大卫·诺西博

2022 年 2 月 16 日

如今，我们生活在一个高度互联的世界中。目前，全球大约有 100 亿台物联网（IoT）设备，预计到 2030 年这一数字将超过 250 亿台。不同行业使用的 IoT 设备各有不同，包括简单的 IoT 传感器、以消费者为中心的智能家居设备，以及复杂的医疗设备、下一代汽车、工业 IoT 硬件等等。

更大的互联性能够为技术创新者带来更大的可能性，但也会带来更多的网络安全威胁。卡巴斯基实验室的研究显示，在 2021 年上半年，针对 IoT 设备的攻击增加了一倍以上。固件历来是设备安全中最容易被忽视的方面，因此越来越多的攻击者开始针对它们。

去年，微软指出 83%的企业在前两年报告了固件攻击，这一比例高的惊人！

保护 IoT 设备变得更加复杂

在保护 IoT 设备方面，我们面临着三个主要障碍：（1）不断增加的网络安全风险；（2）网络安全专业知识的匮乏；（3）复杂、不断变化的全球监管环境。IoT 生态系统中的每个环节（从芯片到云设备制造商、供应商、系统集成商和其他利益相关者）不仅要降低网络安全风险，还要满足合规性，他们的任务异常艰巨。

以前，企业通常会推出没有足够安全措施的联网设备，这会导致客户面临安全风险。如今，仅仅将优质产品推向市场是不够的，企业必须确保这些产品是安全的，这样才能防御固件攻击，以便在现代威胁环境中安全运行。

许多企业缺乏成熟的安全专业知识，他们正在寻求指导和最佳实践，以便能够迅速采取行动以满足更高的客户和监管要求。当然，企业也可以使用战术工具来修复已识别的漏洞。但是，NIST 的研究表明，这种“任凭安全漏洞不断堆积”的响应式方法无法与主动的安全策略相媲美。

企业应重新考虑网络安全问题

鉴于攻击事件不断发生且呈指数级增长，企业必须迅速采取措施，实现其网络安全措施

的现代化，以便妥善保护自己和客户。

企业不能仅仅做出一个姿态，而是要切实地采取行动。过去，企业通常更加重视上市速度和降低成本，而通常会忽视 IoT 安全问题。如今，企业需要检查 IoT 产品的开发流程及其监管问题，以确保从一开始就将安全性纳入考量。

安全是一项长久的责任

企业应采取主动的安全策略，并在整个产品开发和生命周期管理过程中实施该策略。仅仅发布安全的产品却不予以售后支持已经不够了。企业必须将安全视为任何新产品的核心组成部分，这意味着企业应拥有可持续的安全方法，包括一些售后支持方法。

我们建议开发 IoT 产品的企业采取以下三个措施。

- **满足现代工业标准。**确认企业的产品开发流程符合汽车、医疗、制造和消费行业的特定标准。
- **及时修复漏洞。**在每个固件开发阶段跟踪和修复已知漏洞和零日漏洞，以确保设备是安全的。
- **实现网络安全透明度。**向合作伙伴、利益相关者和最终用户传达产品的安全性，以帮助缓解安全问题。

对于 IoT 开发人员来说，采用现代网络安全方法的优势很多。获得适当保护的企业更有可能成功实施业务战略、降低风险、保护品牌声誉、创造产品差异化和建立市场领导地位。另一方面，缺乏现代网络安全方法的企业则面临着对其品牌、产品和利润的巨大威胁。什么都不做或仅仅遵循过去“足够好”的做法，已不再是现实的选择。

此外，加强 IoT 产品的安全性对于释放互联技术的巨大潜力至关重要。虽然 IoT 设备的数量用了 10 多年才达到 100 亿台，但在下一个十年结束之前，这个数字将会增加一倍以上，从而创建一个庞大的智能数据网络。如果该网络不具备足够的弹性恢复能力，则会有无数的麻烦。现在，企业应采取主动的安全策略，这样才能保护其数据及用户。

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