简译版

5G 时代如何保护物联网生态系统

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	How to Secure Your IoT Ecosystem in the Age of 5G		
原文作者	特蕾莎·拉诺维兹（Theresa Lanowitz）	**原文发布日期**	2020 年 1 月 30 日
作者简介	特蕾莎·拉诺维兹是一位资深的网络安全专家。		
原文发布单位	Dark Reading		
原文出处	https://www.darkreading.com/risk/how-to-secure-your-iot-ecosystem-in-the-age-of-5g/a/d-id/1336879		
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。		

5G 时代如何保护物联网生态系统

特蕾莎·拉诺维兹

2020 年 1 月 30 日

物联网（IoT）正在成为企业和日常生活中必不可少的一部分，影响着从监测仓库里的产品到跟踪您的心率和睡眠模式等各个方面。Gartner 预测，到今年年底，将有 58 亿个企业和汽车 IoT 终端设备投入使用。而现在，随着 5G 的部署和 IoT 设备的大规模应用，新的安全挑战正在出现。

对于计划采用 5G 的企业来说，大量的 IoT 设备会带来更大的攻击面。美国电话电报公司（AT&T）网络安全部门最近的一项调查显示，44%的受访者表示，5G 来临之际，攻击面的扩大是他们为做好业务，而关心的首要问题；39%的受访者则认为与网络连接设备的增长是他们最关心的问题。网络、人和机器的连接点数量的不断增加将为恶意行为者提供新的机会，使目前已知的可控威胁武器化。

虽然 5G 因其内置的安全措施（包括网络切片、更强的传输加密、用户身份保护和更低的窃听风险）在本质上更加安全，可以满足许多业务需求，但企业也应积极主动地调整其安全政策和控制措施。在这个新的 5G 互联世界里，下面四条建议可以帮助组织机构保持网络安全。

采用虚拟化、自动化的安全控制措施

这将有助于组织机构管理扩大的攻击面并降低未来的风险。虚拟化的安全控制措施可以快速部署，并允许组织机构通过自动响应（例如创建防火墙）对新攻击做出及时响应。

实施机器学习和威胁检测

您将需要更好地监控和分析整个网络中急剧增加的网络流量。机器学习和自动威胁检测是必要的，因为人工干预将不能逐一筛选这些 5G 带来的大流量，更不用说对其做出响应了。

考虑零信任方法

在组织机构中的所有设备上对身份认证和授权使用零信任方法，能降低在网络上引入恶

意代码的可能性。通过不断检查登录用户的状态和行为，零信任模型将帮助您的安全团队快速确定登录用户到底是真实的人还是自动化的恶意代码。

采用共享安全模型

IoT 设备还将继续存有漏洞，比如生产中仍然保留的出厂默认密码，因此组织机构将需要承担起防范流氓设备的责任。就像在公共云中一样，5G 共享安全模型将帮助提供商，通过将网络本身用作安全工具来实现基础设施中的安全，而组织机构则需处理端点问题。

在共享安全模型中，企业将负责网络上的设备。在 5G 网络中，网络运营商负责 3GPP 框架和标准中列出的安全要素（即数据加密和无线接入网络），以及网络基础设施本身的安全。而企业将负责网络上的设备，包括移动设备管理，企业在网络上运行的应用程序的认证以及身份和访问管理。

随着连接到 5G 的设备的涌入，采用全面的、多层次的方法将是帮助您保护 IoT 生态系统和其他宝贵资产的关键。每个组织机构的 IT 和安全基础设施的设计都不同，这也意味着每个组织机构的安全需求也将有所不同。例如，一个使用许多工业 IoT 设备来生产汽车的工厂车间，它的安全措施将不同于对生命敏感的设备（如胰岛素泵）的安全措施，后者依赖于补救和响应计划。即使发现有人正在访问数据，组织机构也不会希望禁用这些被访问的设备。

虽然有一些控制措施有助于防止终端设备感染运营商的 4G 网络，但据我们所知，单个设备就能影响到企业的整个网络。2018 年，黑客利用拉斯维加斯一家赌场里的一个智能鱼缸来访问网络，并在整个网络中横向移动，窃取了 10GB 字节的数据。网络中连接的任何东西都可能成为黑客进入您的网络的薄弱环节。检查一下您的 IoT 设备是如何连接到您的传统 IT 网络的，然后再确定如何对其进行分段。这将有助于降低组织机构 IoT 生态系统中的风险。

5G 即将到来，随之而来的是一系列 IoT 设备和新技术。但是各组织机构必须牢牢记住，这也意味着攻击面将显著扩大，并为恶意行为者提供更多的机会。采用多层次的方法，确定设备及其物理环境的互连性，以及在其他防御措施中部署虚拟化和自动化，将有助于降低风险，并使组织机构为其在 5G 世界中实现 IoT 的承诺做好准备。

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，截止到 2019 年 9 月 30 日，安天的威胁检测引擎为全球超过六十万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