减少医疗设备的攻击面

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	How to reduce the attack surface associated with medical devices		
原文作者	Zeljka Zorz	**原文发布日期**	2019 年 9 月 3 日
作者简介	Zeljka Zorz 是 Help Net Security 总编辑。		
原文发布单位	Help Net Security		
原文出处	https://www.helpnetsecurity.com/2019/09/03/medical-devices-attack-surface/		
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。		

减少医疗设备的攻击面

Zeljka Zorz

2019 年 9 月 3 日

随着联网医疗设备的数量不断增长，医疗机构的攻击面也在不断增加。

“目前，医疗系统中的大多数医疗设备在设计时都未考虑到安全性，而且它们还需要数年才能被下一代设备替换（如果有的话）。”医疗设备和医疗物联网（IoMT）安全解决方案提供商 Cynerio 首席执行官兼共同创始人莱昂·勒曼（Leon Lerman）指出。

“我们曾目睹勒索蠕虫‘魔窟’（WannaCry）导致英国 60 多家医院的网络瘫痪。该事件说明：医疗设备的内置漏洞使其容易遭受‘普通’攻击，在这种情况下，攻击者无需执行特别复杂的攻击。”

医疗设备面临的危险

勒曼预测，随着医疗机构对智能医疗设备越来越依赖，针对这些设备的攻击将会更加猛烈。

对于医疗机构来说，勒索软件攻击特别具有破坏性。越来越多的黑客开始以医院为攻击目标，劫持敏感的患者数据并勒索高额赎金。在这种情况下，上述预测很有可能成为现实。劫持敏感的患者数据只是冰山一角，攻击者还会破坏目标医院和诊所的服务，严重威胁患者的健康和生命安全。

“攻击者可以渗透医疗设备，篡改剂量甚至使设备显示错误数据，导致医生做出错误的诊断。他们还可以劫持电子医疗记录，以此索要赎金，导致患者的治疗程序被延误。”他指出。

虽然联网医疗设备能够并且确实提高了住院患者治疗的质量，但也带来了新的漏洞。此外，医疗设备的漏洞取决于其内部运作和临床工作流程，因此患者并不知道他们是否处于危险之中。

主动降低风险

根据自身规模，医院可以将数千或数万台医疗设备连接到他们的网络。每一台联网医疗

设备都是首席信息安全官（CISO）应该担心的潜在目标。

“这些医疗设备的设计并不安全，代表了医院的安全盲点。”勒曼指出。

“在最好的情况下，负责保护医院免受网络威胁的人员，能够识别出 IP 地址，但这个 IP 既可能是核磁共振成像（MRI）机器的，也可能是护士工作站或某台 PC 机的 IP 地址。也就是说，安全人员并不清楚那些 IP 对应哪些设备。在最糟糕的情况下，他们甚至无法检测到 IP 地址。”

他指出，CISO 可以利用现有技术自动将 IP 地址与网络上的设备一一映射，从而避开安全盲点。

一旦他们获得了可见性，并了解了医院网络中的医疗设备，他们就可以采取预防措施来减少 IoMT 生态系统的攻击面，从而控制风险。这些措施包括：对联网医疗设备的自动化可见性、持续的风险评估、异常检测和网络分段。

美国食品药品管理局（FDA）和民权办公室（OCR）已经提出了一些保护医疗设备的安全指令，但并未得到严格执行。

医疗机构可以采取的措施包括：（1）了解企业安全的 IT 专家与熟悉医疗设备的生物医学工程专家密切合作；（2）在采购过程中与医疗设备制造商协商持续支持条款（例如，服务协议应该包含及时提供已知漏洞补丁的条款）。

勒曼说，医疗机构已经开始采取了上述的第一个措施。目前，医疗行业的最新趋势之一是：设立新兴的医疗设备安全工程师（MDSE）职位。

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，安天的威胁检测引擎为全球超过三十万台网络设备和网络安全设备、超过十五亿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