OUCH! | 2018年8月

SANS SECURITY AWARENESS

OUCH!

給大家的安全意识通讯月刊

智能家居设备

什么是智能家居设备?

传统上，在家里只有几个设备可以连接到互联网，比如笔记本电脑、智能手机或游戏机。但时至今日，越来越多的设备都能連到互联网上，从你家的灯泡和扬声器到你的电视，还能把门锁上，甚至乎能連到你的车。很快，几乎所有你家里的设备都能连接到互联网上。这些连接的设备经常被命名为物联网（IoT）或智能家居设备。虽然这些连接设备带给极大的方便，但同时也带出独特的危险。

问题究竟在哪呢?

连接到您的家庭网络的设备越多，出錯便会越多。黑客可以对您的设备进行编程去攻击他人，供应商可以收集大量信息从您的活动里，或者您的设备可能会感染并锁上令你不能使用。许多制造这些设备的公司都没有网络安全方面的经验，并且认为保障安全是一种成本。因此，您所购买的许多设备很少甚至没有内置安全性在内的。例如，某些设备具有众所周知的默认密码，或无法进行设定或更新它们。

我怎样才能保护自己

那么你能做什么呢？我们绝对希望您能安全而可靠地利用可连接的设备。这些设备可以提供绝佳功能，使您的生活变得更简单。此外，随着技术的发展，您可能已别无选择，必须使用智能设备。以下是您可以采取的关键步来保护自己。

只连接什么是您需要的：确保设备安全的最简单方法，便是不将其连接到互联网上。如果您的设备不需联机，便不要将其连接到无线网络上。那么，你真的需要你的烤面包机发送通知到你的手机吗？

你要清楚知道哪些已连接：哪些设备已连接到您的家居网络？不确定，还是记不起来呢？先关闭你的无线网络，然后查看哪些内容不再使用。它可能不会找出所有的，但你会惊讶地发现有多少设备已被忘記。

保持更新: 就像您的计算机和移动设备一样, 保持更新所有设备尤其重要。如果您的设备有自动更新选项, 请先启动它。

密码: 将设备上的密码更改为独特的, 只有你知道的强密码。你很有可能只需要输入它一次。记不起你所有的口令句? 别担心, 我们也一样。考虑一下使用密码管理器, 来安全地存储所有密码。

隐私选项: 如果您的设备允许您配置隐私选项, 选取限制它的信息收集或共享。可选一个简单操作, 便是停用任何信息共享功能。

供应商: 认你识和信任的公司购买设备。查找支持安全性的产品, 例如允许您启用自动更新功能、更改默认密码和修改私隐设置。

用心聆听: 如果那些设备可以不断地倾听语音命令。例如, 您的"Alexa"和"Google"家庭设备, 可以将敏感对话记录下来。当您确定把设备放在你家里的某个位置时, 请必先考虑查看隐私选项这一点。

访客网络: 考虑确立您的智能家居设备必须分开"访客"无线网络, 不要从您的计算机和移动设备上使用的主要无线网络。这样, 如果任何智能设备被感染, 您的主网络上的计算机或移动设备仍然是安全的。

没有理由害怕接触新技术, 但要理解它们所构成的风险。通过采取这些简单的步骤, 可以帮助您创建一个更安全的智能家居。

特邀编辑

Robert M. Lee (@RobertMLee) 是SANS认证的讲师和FOR578的作者 - 网络威胁情报和ICS515 - 事件指挥系统 (ICS) 主动防御和应对能力。Robert也是工业网络安全公司"Dragos"的首席执行官和创始人。

资源

口令句: https://www.sans.org/u/GEB
密码管理器: https://www.sans.org/u/GEG
确保家居网络安全: https://www.sans.org/u/GEL