专家洞察@IBV

为应对全球性安全问题做好准备

在电子行业确保安全的要诀

IBM 商业价值研究院

保护电子行业的安全

虽然来自物联网 (IoT) 的数据增加了业务转型方面的优势，但也存在一个缺点：安全问题。网络漏洞百出，用户缺乏安全意识，使之成为黑客的“乐园”。大多数安全方面的投资都花在企业层面，但这需要作出转变，以确保 IoT 应用的安全，并提供更完善的监管和问责机制。电子行业的企业必须建立安全的环境，支持在网络中安全地收集、使用、共享和存储数据。他们不仅要关注设备和消费者的安全，还要弥补存在于工厂、生态系统以及合作伙伴网络中的漏洞。

做“加法”：了解谁拥有安全“方程”的各个要素

数据中蕴含丰富的洞察，可以帮助企业保持竞争优势，而数据本身也是一种富有价值的商业资产。与其他资产一样，数据也需要受到妥善保护。电子行业的企业需要保护快速增长的数据，但是这个行业中的安全问题相当复杂，因为涉及到众多组织领域。IoT 结合了运营技术 (OT) 和信息技术 (IT)。每个领域都有自身特殊的设计、管理和决策标准。而 OT 的焦点是安全。它结合了用于收集信息的硬件和软件。IT 工作涵盖以人为中心的计算机和信息系统，因此必须确保隐私。问题在于：IoT 安全属于 IT 的责任范围吗？IoT 既涉及 IT 又涵盖 OT，需要确保各种设备和网络的安全和隐私，而这些设备和网络的控制可能比较松散，无法在 OT 较长的时间周期内获得安全保障。

Ponemon Institute 最近的一项调研指出，最应负责移动和 IoT 安全的组织职能部门通常不是 IT 安全团队。[2] 仅有 5% 的受访者表示首席信息安全官应对 IoT 应用负主要管理责任。[3] 相反，受访者认为，产品工程和业务线负责人对解决方案负责，潜台词就是也应负责解决方案的安全问题。[4] 必须调和开发与长期交付支持之间的分界线，确保获得成功。

2016 年的“Dyn 安全入侵”事件利用了数百万台与 IoT 相连的设备，并造成了大规模网络中断，*《纽约时报》*将此次攻击称为“大规模破坏性武器”，这并不夸张。[1]

研究各层面的安全性

有关 IoT 安全的五个无可争辩的事实

1. 设备将在充满敌对因素的环境中运行。IoT 设备通常在无人监督的情况下运行，所以它们必须既能防止数字入侵，又能抵御物理篡改。
2. 软件的安全性会随着时间的推移而逐步降低。设备运行的时间越长，遭到攻击的风险就越大。
3. 共享设置让秘密不复存在。采用默认设置的现象非常普遍，攻击者可以利用这些设置来控制设备，达到不可告人的目的。
4. 除非用户被要求做出决定，删除默认的保护设置，否则弱配置将持续存在。
5. 随着数据的累积，风险会逐渐增加。如果数据没有得到妥善管理、保护和销毁，就可能导致隐私外泄和数据所有权问题。

必须制定跨职能部门的策略和适当的使用准则，这十分必要。随着物理计算机和虚拟世界之间的界线愈加模糊，系统安全性必须既涵盖最小的远程设备，又包括规模最大、最私密的受保护计算系统。IBM 商业价值研究院的报告“提高最高管理层的安全意识”中提到，94% 的高层管理者表示他们的企业可能会在未来两年内遭遇重大网络安全事件。[5] 对于他们来说，问题不在于事件是否会发生，而是什么时候发生。最高层主管必须了解业务将会受到怎样的损害，以及如何减轻此类损害。

随着越来越多的消费者将新设备加入 IT 网络，来自工业级系统的协议经常被改为用来驱动这些家用电器。尽管企业可能有严格的控制措施，但通常并不在消费者层面实施。黑客可能会以篡改的形式发动攻击，包括数据更改、延迟或替换。管理者需要将注意力放在设备层面，因为每个传感器都可视为企业的延伸。无论是简单的传感器、可编程逻辑控制器还是云服务器，所有这些终端设备都可能是复杂网络的一部分。它们也可能是多个网络的一部分，之所以说确定潜在的攻击目标是一项具有挑战性的任务，其原因就在于此。云端是几乎所有电子行业企业的主要运营平台，因此，评估提供运营商级 IoT 安全性的云供应商应该是企业的首要任务。

在电子行业，成千上万的设备通过云计算系统进行通信和存储数据。很快，这些设备有望实现彼此直接通信。您需要检查所有通信流，包括路由流量过程所涉及的设备以及云基础架构中的设备，从而发现潜在的安全漏洞。还需要检查所有专用硬件、共享硬件或者虚拟化硬件。需要经常对整个基础架构进行重新检查，以抵御黑客以及其他“黑暗游戏者”的新手段。

IoT 系统可能深度互联，而所有这些接口都存在风险。例如，如果您与第三方云服务提供商合作，那么您肯定希望安全地将信息传递到这些提供商的系统中，避免受到攻击。设备和数据保护策略中应包含有关 IoT 设备和连接的风险预防以及缓解措施。在网络中移动、收集、分析和存储数据时，必须采取相应的安全措施。

应考虑采用先进的安全技术，例如物理层防克隆功能 (PUF)。在共享系统中，对其他云客户或平台的攻击也可以波及和影响贵公司。

黑客还可能会删除或窃取数据以索要赎金。因此，务必认真思考当前以及今后怎样连接、传输和使用数据。评估篡改和滥用的潜在风险和成本。是否采取了必要措施，保护数据不会遭到勒索软件的威胁？是否采取了必要措施，应对可能会损害企业敏感数据保密性的数据泄露事件？企业最大的弱点在哪里，防御措施是否足够强大？评估遭到入侵的可能性、损害程度，并进行适当的优先次序排列。

Ponemon Institute 的研究表明，丢失的记录越多，数据泄露的成本就越高。[6] 2017 年，丢失记录少于 10,000 条的事件的总成本平均为 190 万美元，丢失记录超过 50,000 条的事件的总成本平均为 630 万美元。[7]

解决道德问题

是否准备好巩固安全基础？

- 如果网络犯罪分子从购买了您 IoT 设备的客户那里盗走了财务信息，您计划怎样应对？
- 想象一下，如果黑客侵入了主题公园游乐设施的控制系统，那会怎样？
- 当 USB 密钥记录器被用来从贵公司的某台医疗设备上的端口窃取个人健康记录和敏感数据时，谁应该对此负责？
- 如果您某个工厂所生产的设备上的 IoT 摄像头被用于录制未经授权的视频，而这些视频会转发或发布到互联网上，将会怎样？
- 如果恶意入侵者能够通过篡改烘干机内部安全防护措施较弱的 IoT 热传感器来烧毁房屋，那会怎样？

法规合规性是另一个令安全战略复杂化的问题。在欧盟，“一般数据保护条例”(GDPR) 将于 2018 年 5 月 25 日生效，所有企业都必须遵守这一影响深远的数据隐私规定。美国也正在积极制定与 IoT 相关的法律法规。[8]

安全措施不应仅限于硬件。每当跟踪个人信息时，都存在隐私问题。有些数据看起来似乎是无关紧要的，比如某人打开冰箱门的次数。但是，如果与其他数据结合，所揭示的个人信息可能比您最初想象的要多很多。收集数据时可能会产生伦理道德方面的问题，这一点同样需要注意。许多国家或地区已经颁布或者正在制订用于保护公民个人身份信息和个人健康信息的准则、标准和规定。这些法规包括欧盟的 GDPR，以及北美的 HIPAA、COPPA 和 PIPEDA。

在电子行业中，随着工业系统与其他包含敏感数据的系统相互连接，隐私风险也随之增加。收集到数据之后，应该怎样使用，在何处使用？过程中是否涉及隐私问题？将会留存哪些数据，留存多久？数据将保存在何处，以何种方式传输？跨设备连接、传送信息并使其相互关联意味着什么？

例如，如果某人的健康追踪系统产生的数据集成到在整个生态系统中共享的设计系统，那么关于此人健康的信息就有可能因为系统的安全漏洞而遭到泄露。如果数据由第三方共享或分发，比如生产附加产品、应用接口或报告的合作伙伴，则可能会产生其他风险。

控制风险

您需要考虑的是一个限度，一旦超越这个度，信息收集就不只是为客户提供协助，而是会成为监视行为或侵犯个人隐私。在何处划定界线？如果一个扬声器始终处于开启状态，它是否可以作为呈堂证供？这类设备会得到与家庭安全系统类似的处理吗？如果用户能在安全问题发生之前就预测到存在的隐患，那将会怎样？尽管这些问题的具体答案取决于企业，但是，制定明确的策略并经常进行检查，将有助于保护企业自身、客户以及行业合作伙伴。

电子产品的安全问题只会越来越复杂。企业中上至 CEO，下至普通员工，都必须了解有关数据、设备、安全和隐私的实践及政策，并负责实施。

以下是关于改善安全和隐私保护方法的一些关键问题：

*您采用怎样的 IT、OT 以及 IoT 策略？*您需要制定有关数据、设备及其所衍生信息的策略。此外，必须检查设备层面的安全性，确保措施足够强有力。关注所有系统和平台，特别是那些作为企业延伸的端点，比如云提供商。

*谁拥有您的数据并与您的客户互动？您对合作伙伴的数据实践的理解程度如何，是否了解他们何时重复使用您客户的数据？*清楚地说明如何收集、使用、共享、验证和保护数据。

*客户的知情程度如何？*制定并分享内容具体、语言平实、面向客户的建议和指导方针。制定明确、具体而且直接的服务条款，确保客户以及用户/消费者能够清楚了解他们的数据将如何被使用。

主题专家

Tim Hahn
IBM 物联网安全杰出工程师，
IBM 发明大师
https://www.linkedin.com/in/hahnt
hahnt@us.ibm.com

Hiroshi Yamamoto
IBM 杰出工程师，全球电子行业首席技术官，IBM 技术学会成员
https://jp.linkedin.com/in/hiroshiyamamotoibm
hiroshiy@jp.ibm.com

关于专家洞察@IBV 报告

专家洞察代表了思想领袖对具有新闻价值的业务和相关技术主题的观点和看法。这些洞察是根据与全球主要的主题专家的对话总结得出。要了解更多信息，请联系 IBM 商业价值研究院：iibv@us.ibm.com。

© Copyright IBM Corporation 2017

New Orchard Road
Armonk, NY 10504
美国出品
2017 年 9 月

IBM、IBM 徽标及 ibm. com 是 International Business Machines Corporation 在全球各地司法管辖的注册商标。其他产品和服务名称可能是 IBM 或其他公司的注册商标。Web 站点 www.ibm.com/legal/copytrade.shtml 上的“Copyright and trademark information”部分中包含了 IBM 商标的最新列表。

本文档是首次发布日期之版本，IBM 可能会随时对其进行更改。IBM 并不一定在开展业务的所有国家或地区提供所有这些产品或服务。

本文档内的信息“按现状”提供，不附有任何种类的（无论是明示的还是默示的）的保证，包括不附有关于适销性、适用于某种特定用途的任何保证以及非侵权的任何保证或条件。IBM 产品根据其提供时所依据协议条款和条件获得保证。

本报告的目的仅为提供通用指南。它并不旨在代替详尽的研究或专业判断依据。由于使用本出版物对任何企业或个人所造成的损失，IBM 概不负责。

本报告中使用的数据可能源自第三方,IBM 并不独立核实、验证或审计此类数据。此类数据使用的结果均为“按现状”提供，IBM 不作出任何明示或默示的声明或保证。

备注和参考资料

1 David E. Sanger and Nicole Perlroth.“A New Era of Internet Attacks Powered by Everyday Devices.”*New York Times*.October 2016. https://www.nytimes.com/2016/10/23/us/politics/a-new-era-of-internet-attacks-powered-by-everyday-devices.html

2 “2017 Study on Mobile and IoT Application Security.”Independently conducted by Ponemon Institute LLC, Sponsored by IBM & Arxan.January 2017.

3 Ibid.

4 Ibid.

5 “Securing the C-suite:Cybersecurity perspectives from the boardroom and C-suite.”March 2016. https://www.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=GBE03738USEN

6 2017 Cost of Data Breach Study Global Overview Benchmark research sponsored by IBM Security Independently conducted by Ponemon Institute LLC.June 2017.

7 Ibid.

8 Mark R. Warner, US Senator from Virginia.“Senators Introduce Bipartisan Legislation to Improve Cybersecurity of “Internet-of- Things” (IoT) Devices.” https://www.warner.senate.gov/public/index.cfm/2017/8/enators-introduce-bipartisan-legislation-to- improve-cybersecurity-of-internet-of-things-iot-devices

GBE03875CNZH-00