五步建立起更好的 IoT 安全基线

1. 别再什么都用 root 权限来运行：默认情况下，管理界面应以较小权限运行，只可执行部分特权操作；2. 反跨站请求伪造令牌应普遍应用：跨站请求伪造（CSRF）是嵌入式设备中最常见的安全缺陷之一；3. 建立漏洞利用缓解机制：抬高了利用内存崩溃漏洞的门槛；4. 身份验证请求：授权机制的缺乏或脆弱，再加上 CSRF，可使恶意网页在无需受害者之前已验证过的情况下，就直接操纵设备；5. 别再用那么多的 HTTP：路由器和智能家居控制器之类设备的 Web 管理界面，通常都是攻陷设备的最大攻击界面，即便 CSRF 缓解措施就位，Web 服务器实现中的漏洞本身，往往就是致命的。

Gartner 未来五年产业预测

1. 预计到 2022 年，企业组织在对业务伙伴进行风险评估时，网络安全等级将变得比信誉等级更为重要。2. 到 2021 年，至少有一家公司将公开承认因恶意软件 / 勒索软件的攻击而造成业务中断，造成的损失将达到 10 亿美元。3. 预计到 2022 年，10% 的企业在安全技术评估流程中将弃用 RFP（请求建议书），而使用更敏捷的流程，包括竞争和战略指引。4. 到 2020 年，大约 60% 参与整合并购的组织会认为网络安全态势是评估核查过程中的一个关键因素。

漏洞管理新趋势：以威胁为中心

漏洞管理的核心一直仰仗由事件响应与安全团队论坛（FIRST）维护通用漏洞评分系统（CVSS），很容易就会被 CVSS 评分误导，陷入数字游戏当中，这些操作往往只能降低纸面上的风险，而不是实际上的。传统漏洞管理方法执行的是渐进式风险降低操作，修复重点要么放在高 CVSS 的严重漏洞上（所谓以漏洞为中心的模式），要么根据资产的价值和暴露面来定（比如面向互联网、第三方访问、含有敏感数据、提供业务关键功能等等；所谓资产为中心的模式）。然而，不幸的是，两种模式往往都落入以最少的补丁封堵最多风险的境地。

Gartner 表示，公司企业应将其漏洞管理操作转向以威胁为中心的模式，实现临近威胁清除，而不是逐步的风险减小。该新模式下，临近威胁的缓解优先级会被拉高。虽然不能预测谁会攻击我们，但至少可以预估谁或什么东西有可能成功实施攻击。

2018 年 IT 安全开支将达 960 亿美元

咨询公司 Gartner 预测，2018 年，全球安全开支将达 960 亿美元，这比 2017 年的 890 亿美元上升了 8%。Gartner 认为，造成安全开支增多的因素包括：监管、买方思维转变、对新兴威胁的重视，以及向数字商业战略的演变。2017 年的安全事件将影响到 2018 年的安全开支，因此，安全测试、IT 外包和安全信息及事件管理（SIEM），将成为基础设施防护及安全服务领域里，增长最快的安全细分市场。

（本栏目刊登文章为缩编，仅代表作者本人观点，与本刊观点无关）