insight.tech
POWERING IoT AND EMBEDDED INNOVATION

确保智能楼宇安全的 7 种方法

Patrick Mannion

连接物联网的智能楼宇面临严重的安全风险。 例如，IBM X-Force Ethical Hacking Team 最近进行了一项白帽子 (white-hat) 演练，发现楼宇控制器通常使用与其网络路由器相同的登录方式。 一旦黑客进入网络，他们就可以快速接管楼宇自动化系统 (BAS)。

更糟糕的是，路由器通常会让管理端口处于打开状态，这为黑客提供了一个易于进入的入口点。 这样的漏洞让黑客可以：

- 关闭冷却系统使服务器过热
- 关闭安全系统或气体传感器
- 停止电梯并关闭照明系统
- 进入 IT 网络并获取企业数据

保护智能楼宇的安全非常困难，因为这些安全风险涉及多个层面：BAS 本身、云连接和远程管理接口。 此外，智能楼宇通常是房地产投资组合的一部分，所以任何安全解决方案都必须能够跨所有地点进行扩展。

根据 IoTium 创始人兼首席执行官 Ron Victor 的观点，获得成功有 7 个关键之处：

1. **使用加密证书**访问 BAS 而不是使用用户名和密码。
2. **消除 VPN 和 APN**（类似于 VPN，用于蜂窝网络），再次避免使用用户名和密码 — 一切都需要使用证书和密钥完成。
3. **不要依赖楼宇中的现有路由器；**而是使用安全网关连接到云。
4. **避免更改防火墙或代理设置，**因为这可能会使 IT 网络易受攻击，并且可能需要冗长的批准过程。
5. **使用同端架构**和在数据源和接收器运行的软件，以避免 DDOS 攻击。
6. **确保数据隔离，**使得每个子系统（照明、HVAC、安全等）都一直与云分离，这样如果恶意软件影响到一个子系统，则不会影响其他子系统。
7. **加密所有流量**以防止未经授权的用户访问数据。

Niagara 4 解决方案

为了说明这些技术，Victor 提到了他在 Niagara 4 楼宇控制框架方面积累的经验。 Niagara 4 是由 Tridium（现属于 Honeywell）开发的管理和控制框架。 它使楼宇系统能够集成到使用 HTML5 界面的统一平台中。 功能包括分析、可视化和自定义仪表板 **（图 1）**。

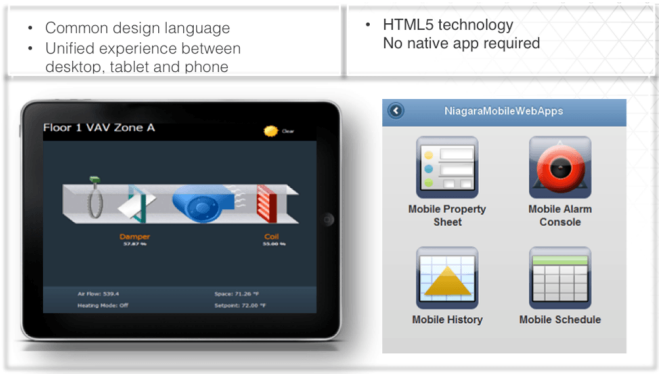

图 1. Niagara 4 提供完整的数据分析、可视化和智能楼宇控制。（来源：Tridium）

IoTium 和 Kodaro 最近开展了合作，将 Niagara 4 引入到戴尔 Edge 网关。 除了其他功能之外，这些网关配备了英特尔® 可信平台模块 (TPM 2.0) 用于安全引导和未使用端口的 BIOS 级封锁。

每个 TPM 都有一个独特的 RSA 加密密钥烧录到其中，支持使用证书和密钥，而不是用户名和密码。“如果您必须连接数以百万计的楼宇，则您无法使用用户名和密码。”Victor 说。“它们很难记住和保存，而且它没有意义，所以您需要摆脱它们的困扰。”

戴尔网关提供了一些对 BAS 有用的其他功能。这些包括连接到任何旧式楼宇生态系统（BACnet、Modbus、CANbus、Z-Wave、6LoWPAN）的功能，以及用于本地分析的高级英特尔凌动® 处理器。

Niagara 4 和戴尔网关的结合满足了智能楼宇的许多关键要求，包括数据采集、处理、分析、可视化以及远程访问和控制。

保护端点安全

一旦 Niagara 移植到网关，下一步就是保护网络，使解决方案可以跨数百个甚至数千个设施扩展。这需要充分了解漏洞，省去上门服务，并避免更改企业代理和防火墙策略的需要。

这正是 IoTium iNodeOS 发挥作用的地方。这种基于 Debian Linux 的操作系统位于网关上，通过省去用户名和密码、管理更新、隔离 IT 和 OT 网络来实现对安全网络的大规模部署。**（图 2）**。

作为托管操作系统，iNodeOS 会自动处理更新和安全补丁，无需命令行输入。“您需要一项能够实时查找漏洞和补丁的全天候服务。”Victor 说。“我们构建它只是因为没有一款操作系统能够在不需要任何命令行界面的情况下完全由云托管。”

保护数据传输安全

在更高一个层次，IoTium 拥有内置防火墙。该防火墙确保 BAS 资产在互联网上不可见，也不会暴露于后门威胁。所有数据都通过安全数据隧道运行，这种数据隧道是一种“同端”方式，需要两端都有授权软件。

此外，IoTium 使用隔离每个子系统的容器化架构。因此，对一个子系统的攻击不会影响其他子系统或更广泛的 IT 网络。通过添加加密功能，确保任何落入坏人之手的数据将无法使用，从而可进一步保护 BAS。

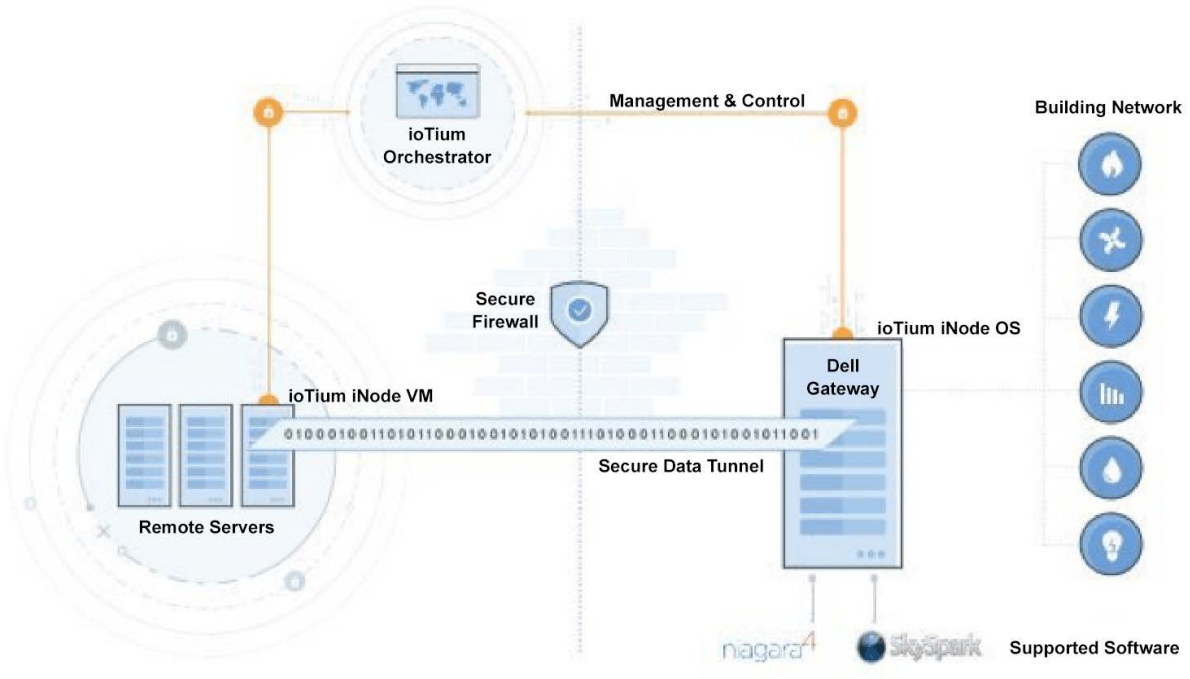

图 2. IoTium 解决方案提供了多层安全。（来源：Kodaro）

insight.tech

避免内部攻击

尽管制定了可以采取的所有技术安全措施，但破坏系统最简单的方式是恶意员工的攻击。“人们认为外面的人会攻击系统，但破坏流量最简单的方式是来自楼宇内部的某个人的报复。”Victor 说。“您必须假定这将会发生，然后保护自己。”

IoTium 的同端架构在这方面可以发挥作用，在该架构中源数据只能与使用相同客户端软件的接收器通信。 如果员工使用自己没有安装合适客户端软件的设备访问网络，则该架构可以防止数据被读取。

迁移到新的物联网部署模式

当然，安全并不是实现扩展唯一需要关注的方面。 正如 IoTium 指出的那样，其零接触配置和一键式应用程序部署可以节省大量时间和费用。

总而言之，很显然，真正的智能楼宇不仅仅是管理 BAS 系统。 智能楼宇必须秉承确保可扩展性和安全性的设计理念。