# Claroty 楼宇管理系统（BMS）

## 为什么楼宇管理系统 (BMS) 的网络安全特别难实现？Claroty 的网络安全解决方案组合如何应对这一挑战？

本项全球性调研对 1,100 名 IT 和 OT 安全专业人员进行了访问，受访者的企业工作职责为运营或以其他方式维护关键基础设施的组件。本项调研探讨了2023年面临的行业挑战、对OT安全计划的影响以及未来的优先事项，其主要发现是：

**他们依靠 Claroty 平台来确保楼宇管理系统 (BMS) 的网络安全，从而支撑其最关键物理设施的功能、适宜性和安全性。**

本文档详细介绍了此类型企业在保护其 BMS 所面临的主要挑战，以及 Claroty 如何帮助客户克服这些挑战，实现和维护有效且高效的 BMS 网络安全。

## BMS 面临的主要网络安全挑战

### 1. BMS 通常是为了工程效率而设计的，没有足够的安全性

大多数 BMS 本质上是不安全的，会产生网络和运营风险。主要关注点和暴露领域包括：

**物理安全问题**

- 对BMS控制台的物理访问控制不佳；缺乏足够的基于角色的访问控制和用户监察。
- BACnet是一种主要协议。BMS通过该协议实现对所有楼宇系统的访问和控制。该协议是明文且未经身份验证的，会增加物理安全风险和与受损相关的其他风险。

**重置密码漏洞**

- BMS一般包含不经常修补的旧技术，因此很容易出现重置密码漏洞。
- 此类漏洞可以使未经身份验证的用户轻松检索和重置设备密码，从而导致BMS底层系统受损。


**网络卫生差**

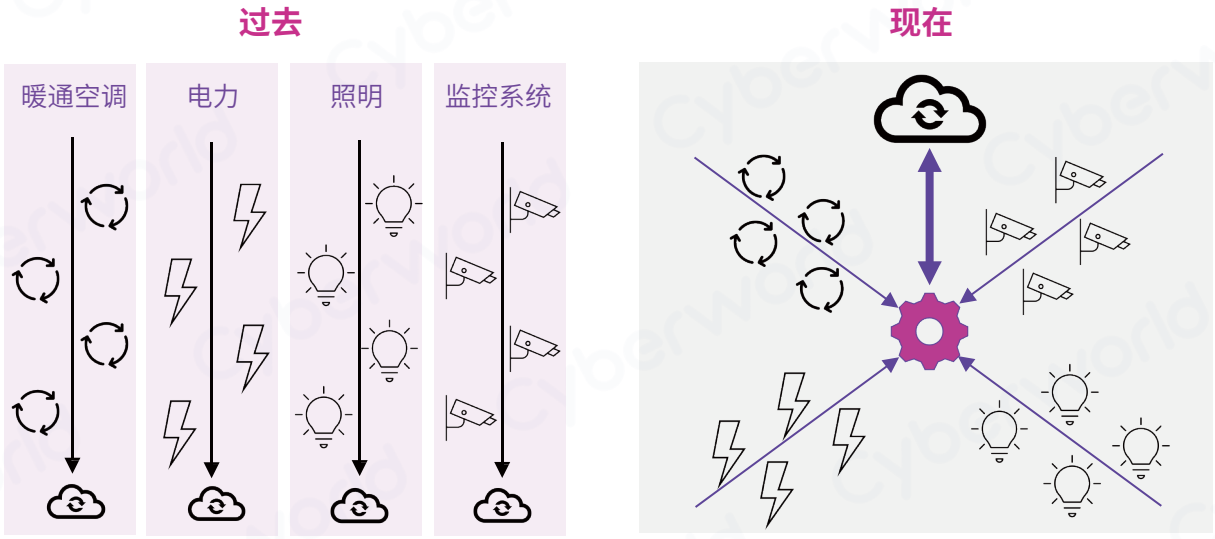
- 将运营效率置于网络安全之上的普遍做法，导致许多BMS技术人员使用弱、默认或共享凭据。
- BMS技术人员通常拥有管理凭据，这种做法会显著增加最关键的系统和设备因凭据盗窃和权限升级攻击而受到损害的风险。

**逻辑连接暴露**

- BMS 经常连接到 IT 网络和互联网，以实现基于云的分析、远程监察和维护等。
- 这种连通性与BMS固有的不安全性相结合，扩大了攻击面，使BMS易于访问，并容易受到各种有针对性和机会性的外部威胁。

## 2. 智能楼宇的兴起正在加剧 BMS 的安全弱点

智能楼宇正在迅速改变现状。在过去，楼宇仅独立包含暖通空调、照明、电力、电梯和安全系统等。但现在，智能楼宇技术使越来越多的楼宇能够通过一个中央控制台（即，楼宇管理系统 BMS）连接、集成和控制所有这些系统。




这种方法的普及得益于其好处，从能源和维护的效率到舒适性和安全性的提高，再到节省成本。然而，这些好处往往掩盖了真正的风险。通过将以前孤立的、在许多情况下本质上不安全的楼宇系统融合到与 IT 共享的异构网络中，智能楼宇技术可以进一步扩大攻击面，并放大 BMS 现有的安全弱点。

## 3. BMS 受损产生的潜在影响很严重

无论攻击类型或媒介如何，BMS 受损产生的影响可能是非常严重的。一些常见的情况包括：

| 类型 | 说明 | 潜在影响 |
|---|---|---|
| **IT 网络攻击的媒介** | • 不安全的楼宇自动化设备可作为攻击者渗透企业 IT 网络的基础。 | • 知识产权、财务信息、个人身份信息、凭据等专有数据的泄露。<br>• IT 连接系统的停机时间。 |
| **附带损害** | • BMS 和 IT 网络之间的不安全连接、以及楼宇自动化设备中的某些类型的漏洞可能会为 IT 攻击（例如勒索软件）蔓延到BMS创建途径。 | • BMS 或连接系统的停机时间。<br>• 依赖于BMS的关键资产，其可用性、完整性和可靠性会受到损害。 |
| **勒索软件 Siegeware** | • Siegeware是一种针对楼宇自动化系统的勒索软件，楼宇自动化设备中的远程可利用漏洞容易受到 Siegeware 的影响。<br>• Siegeware使攻击者完全控制BMS和所有连接的系统，为勒索行动提供便利。 | • BMS 或连接系统的停机时间。<br>• 依赖于BMS的关键资产，其可用性、完整性和可靠性会受到损害。 |
| **内部威胁** | • 基于角色的访问控制不足、使用默认或共享凭据会为技术人员和其他用户提供对BMS的不受限制访问。<br>• 有限的可视化会导致内部恶意人员和无意错误被忽视。 | • BMS 或连接系统的停机时间。<br>• 依赖于BMS的关键资产，其可用性、完整性和可靠性会受到损害。 |

## Claroty 如何应对 BMS 的网络安全挑战

Claroty 通过实施以下控制措施来帮助客户克服 BMS 的网络安全挑战：

| 发现： | 保护： | 检测： | 优化： |
| --- | --- | --- | --- |
| BMS的全部内容、与其连接的所有内容、依赖于它的所有内容 | 针对漏洞、BMS技术人员的危险行为、其他安全弱点 | 可能影响BMS和连接系统的最早威胁指标 | 通过现有工具、人员和流程，从BMS安全性到IT安全性和GRC计划 |
| • 自动发现和编目BMS环境的所有组件，包括所有连接的系统和设备、相关流程、连接的用户会话。<br>• 创建集中式、易于管理、始终保持最新的BMS环境库存。<br>• 对正常情况的明确洞察。<br>• 支持有效BMS安全计划的所有后续和基本方面所需的广泛可视化。 | • 自动识别BMS风险因素：未修补的漏洞、不安全的协议、错误配置、员工网络卫生状况不佳、使用不适当的远程访问工具等。<br>• 持续进行风险和漏洞评估，并提供优先级和缓解指导。<br>• 使用基于角色的访问控制、实时监察和紧急断开机制，确保远程访问安全。<br>• 基于设备通信实现和优化BMS网络分段的能力。 | • 持续监察整个BMS环境，获取已知和未知威胁的最早指标。<br>• 所有警报的可操作上下文，包括完整的根本原因分析和风险评估。<br>• 能够快速检测，并断开远程技术人员和供应商的风险性会话。<br>• 由Claroty著名研究团队支持的弹性威胁检测模型，确保最新的签名和修复指南始终可访问，并内置于BMS防御中。 | • 庞大的集成生态系统和强大的API，能够通过现有和熟悉的工具、基础设施、工作流程实现和维护有效的BMS安全性。<br>• 灵活、可扩展的架构，具有云和本地选项，所有这些都支持多站点部署和各种BMS规范。<br>• 针对风险态势、卫生和整体绩效的可行分析，适合执行人员使用，并揭示BMS安全性对企业范围的影响。 |

## Claroty 平台在 BMS 客户中的常见用例

为 BMS 设备的外部供应商提供安全、无摩擦、高度控制的方法，通过该方法远程访问设备以进行维护。

使 SOC 分析师能够通过现有的 SIEM 和 SOAR 工具，在可操作的上下文中无缝、自信地接收和响应 BMS 警报。

监察数据中心HVAC系统的过程值，以确保快速检测可能对服务器有害的任何温度变化。

识别楼宇自动化设备中的重要漏洞，并实施基于零信任的控制以补偿风险，直到下一个维护窗口可以安全地进行修补为止。

使用自定义警报规则快速查明电力系统、所有连接设备中的维护问题和 EOL 指标。

Cyberworld 广州科明大同科技有限公司 | 中国区总代理
官方网站 www.cyberworld.com.cn
业务电邮 info@cyberworldchina.com
服务专线 400-9988-792