Radiflow

Use Case

OT-Cyber Security: Solutions for Building Management Systems (BMS) and Smart-City Deployments

Building Management Systems (BMS) and Smart-City technologies have become quite more commonplace across the globe. These systems offer the ability to control buildings' internal environments, access control and other security systems and structures, all at the touch of a button!

By integrating an array of different services such as electricity, water supply, HVAC, access control, and fire alarms, BMS systems offer a host of advantages, from cost-effective, single-pane control over all building systems to better handling of security and system failure events and much improved safety.

BMS and Smart City technologies, however, are not without its down side. Integrating previously-disparate (and often inadequately secured) building or city systems poses the risk of hackers accessing their target system through another one.

The Challenge of Securing Building Management Systems

BMS typically consists of devices by multiple vendors, which introduces a host of device- and vendor-specific vulnerabilities into the system. This makes it extremely difficult to obtain real-time visibility of the complete system, which is necessary for threat detection and mitigation. The multitude of multiple vendors in itself exposes the network to increased risk, as each vendor's technicians require remote access to the network for maintenance. This can lead to erroneous or malicious changes to the network.

BMS and Smart City systems also rely heavily on cyber-physical systems (CPS), remotely-controlled automation and operations , and IT/OT connectivity. This results in a maze of system assets which can be very complex to map out and keep track of. It also introduces many possible entry-points which increases system vulnerability.

Smart-City systems face the additional challenge of efficiently sending network data from numerous operational units (e.g. water pumping, air quality monitoring, physical security systems) to the municipal SoC for central threat analysis without overloading or disrupting the municipal LAN.

Securing Building Maintenance and Smart City Systems - Unraveling the Maze

Keeping a building and its occupants secure, as well as mitigating financial loss, certainly presents some challenges, but by approaching the task with a structured and logical framework, it is possible to achieve a high level of threat detection and accurate risk assessment.

1. The first stage involves mapping out the BMS system in its entirety, creating a virtual model which includes both the IT elements and the CPS components, incorporating assets from multiple vendors. This virtual model includes the different interconnections between assets which is important for pinpointing possible weak spots.
2. The virtual model (also called a digital image) can be used for BAS (breach attack simulation) to provide an accurate risk-assessment of the entire network.
3. The BAS results can then be used to offer ROI-driven recommendations for necessary cybersecurity measures. The client's specific needs and budget constraints are taken into consideration, leading to a prioritized list of mitigation possibilities.
4. Ongoing monitoring safeguards the network for the long term, allowing for system updates or new assets to be included so that security is maintained at the highest possible level.

Radiflow Solutions for Building Management Systems

Radiflow's cybersecurity solution suite, designed especially for production (OT) networks, provides BMS operators with the tools to protect, visualize, and safely maintain their systems.

- MAP (VISUALIZE) - Radiflow's iSID, industrial threat detection and monitoring system, generates a visual model of the entire BMS network including assets, connections, protocols, and vulnerabilities.
- KNOW - Radiflow's CIARA industrial risk assessment and management platform uses the iSID data along with MITRE ATT&CK and other resources to thoroughly understand which threat actors and attack tactics are most relevant for testing. By using non-intrusive threat intelligence based breach and attack simulations it is possible to assess the effectiveness of corresponding mitigation measures (IEC62443-compatible).
- ACT - Prepare and implement a security roadmap based on the organization's long-and short-term security preferences (e.g. strengthening a single business unit vs. reducing overall risk) as well as budgetary constraints.
- MONITOR - Detect abnormal behavior indicating breach attempts and changes to various BMS components and continuously monitor the network at the corporate SOC or offsite. Designed especially for OT, Radiflow's solutions support all relevant OT protocols (e.g. BACnet, Profibus) for accurate modeling and anomaly detection (new devices, topology changes, abnormal memory access, and firmware changes) as well as ethernet and serial interfaces for modern and legacy devices.

About

Radiflow develops unique OT cybersecurity tools to protect and ensure organizations' digital resilience. The company closely collaborates with Managed Security Service Providers to oversee the discovery and management of all relevant data security points. Founded in 2009, Radiflow has offices and partners in Europe, USA and APAC. Its field-proven solutions are installed at over 6000 sites around the globe.

Radiflow | For more info: **radiflow.com**