SECURITY MATTERS

Case Study

Rabobank Deploys Building Automation System Security

Rabobank is deploying SilentDefense to improve Building Automation System (BAS) security

Customer Profile

Rabobank is a Dutch multinational banking and financial services company headquartered in Utrecht. Serving approximately 8.4 million clients around the world, it is the second-largest bank in The Netherlands in terms of total assets, and among the world's 25 largest financial institutions in terms of Tier 1 capital. With 420 offices only in The Netherlands, they offer the most finely-meshed banking network in the country.

The Challenge

Nowadays, a building is increasingly a cyber-physical system (CPS) whose physical components (such as HVAC, access control and elevators, escalators and moving walkways) are integrated and controlled through digital infrastructures. Building Automation Systems (BAS) integrate, connect and control the building's different sub-systems to facilitate management operations. In addition, asset inventory is becoming crucial for efficient preventative maintenance and for compliance with the stringent requirements many countries are imposing on Smart Buildings.

BAS vulnerabilities have risen 500% YoY in the last three years and it is becoming increasingly important for owners and managers of critical buildings to address the key issue of Asset Inventory and Cyber Security.

BAS Threat Landscape

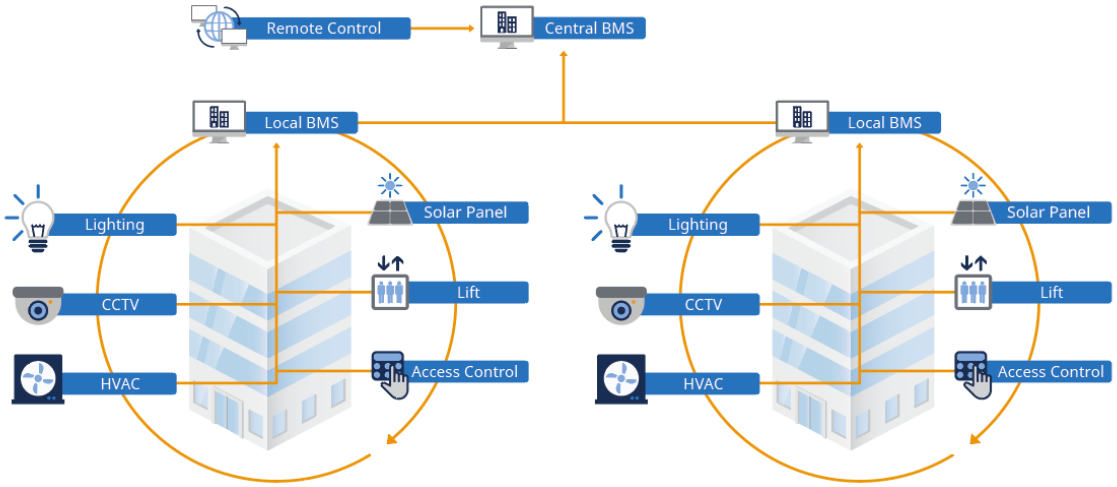
- +500% BAS Cyber Vulnerabilities discovery rate in the last three years
- 75% organizations without a formalized cyber security strategy
- 1,500 access attempts every day on a single smart house exposed on the Internet
- 68,000 open BAS interfaces easily found on the Internet
- 50 billion IOT devices on the network

The Project

Rabobank has launched an initial BAS Cyber Security project to cope with the following challenges:

- Protecting networked BAS/IoT devices
- Inapplicability of IT security solutions to BAS devices
- Limited or no visibility into how devices are operating and whether they are communicating with the outside world

The scope of the OT network to be managed includes several different Building Automation Systems for HVAC, surveillance, access control and lighting. The initial scope covers more than 500 devices. After a defined learning period, a thorough penetration testing will be accomplished to validate the improvement of the bank's security posture. SilentDefense has been deployed to automatically identify and protect each Building Automation System on the network, deliver an accurate asset inventory and capture all the relevant cyber and operational threats without the cost and complexity of software agents on endpoints.



An abstract view of how all assets in different buildings can be monitored from one central point.

Main Results

A complete inventory and network map has been extracted with a detailed view of hundreds of devices, including their current model, firmware and vulnerabilities.

Among the relevant findings SilentDefense detected:

- Unwanted communication links between the IT and OT network caused by firewall misconfiguration.
- Unwanted/unnecessary services and protocols enabled (e.g. file transfer and device discovery services).
- Maintenance operations not adhering to policies (e.g. supplier connecting own laptop to the network).
- Misconfigured devices (e.g. IP cameras with high bandwidth consumption).
- Weak passwords to access IP-cameras. Multiple vulnerable hosts and controllers with outdated firmware.

Customer Value

- Full visibility over BAS network
- Enforcement of compliance with internal network and maintenance policies
- Detection of anomalies and cyber threats to operational continuity
- Improvement of the overall security posture

Other Resources That Might Be Interesting for You

Read our BAS solution brief or watch this animation to learn more about protecting your buildings.

SECURITY MATTERS

SecurityMatters empowers critical infrastructure and manufacturing organizations with the ability to identify, analyze, and respond to industrial threats and flaws, minimizing troubleshooting costs and unexpected downtime. We leverage ICS-specific knowledge and understanding to provide visibility into critical assets and their activity, and detect operational problems and cyber security threats. Our revolutionary network monitoring platform has been successfully deployed by customers worldwide.

www.secmatters.com | info@secmatters.com