CYLANCE CONSULTING

Building Automation Assessment

Identify and Mitigate Risks in Your Smart Building

Benefits

- Identify processes, systems, and technologies involved in integrated buildings and IT systems
- Understand the types of cyberattacks which may be targeted at intelligent buildings
- Identify and evaluate threat sources
- Understand the roles, responsibilities, and capabilities of various stakeholders, including building systems vendors, IT personnel, and system integrators

84% of building automation systems are connected to the Internet, making them targets for cyberattacks.

Source: Survey Suggests Many BAS Could be Vulnerable to Hackers

Today, cybersecurity protection and risk prevention for building automation systems (BAS) and building management systems (BMS) are a necessity. The operational, financial, and reputational impact to a business is tremendous and can include locked-out systems, fire suppression/lighting/HVAC failures, introduction of malicious files into the corporate network, and overall interruption of business and operations. An organization's IT and facilities departments must collaborate to close potential attack avenues.

Cylance® Consulting's Building Automation Assessment helps organizations **identify and remediate vulnerabilities** that pose risk to the IT and OT networks and could impact the function of the smart building.

Service Overview

Cylance Consulting's ICS security experts will work closely with organizations to evaluate the security practices of building automation systems. Multiple systems including HVAC, fire suppression, electronic security systems, and smart lighting controls are analyzed against known and potential vulnerabilities as well as operational dependencies.

The assessment provides context related to the potential business impact of cyberthreats, the vulnerability of the systems to attack, and whether there are any current indicators of compromise. It provides an effective means to identify the highest priority security concerns and recommendations for securing the environment.

Information is collected about the organization's security practices, policies, and procedures through survey responses, staff interviews, tools, company documentation, and site walk downs.

Deliverables

The information obtained from the Building Automation Assessment is used to provide the organization with:

- A risk profile that addresses impact, threat, vulnerability, probability, and countermeasures
- A prioritized road map for remediating security concerns

Cyber-related issues play an increasing role within building networks and it is important to take an active role in managing risk. Contact Cylance Consulting or your technology provider to discuss your needs.

CYLANCE

+1-877-973-3336
proservices@cylance.com
www.cylance.com/consulting

20190129-0578