How Secure Is Your Building Automation System (BAS)?

By 2026, there will be over 56 million new BAS devices. (1)

The number of identified vulnerabilities in BAS has increased over 500% in the past three years. (2)

39.3% of publicly reachable BAS devices are vulnerable (3)

1. Publicly reachable PLCs: Using this path, the malware can enter directly from the Internet and exploit the programmable logic controllers (PLCs) controlling the sensors and actuators at the field level as there is no need to perform any bypass movement from other devices.

2. Publicly reachable access points: Using this path, the malware can enter from the Internet at the management level and move laterally to the PLCs.

3. Publicly reachable devices: Using this path, the malware can enter on BAS devices such as IP cameras or a Wi-Fi router from the Internet and use the entry point to gain access to the internal network, allowing horizontal movement from there to other subsystems.

4. Air gapped network: Using this path, the endpoint must have physical access to the building network (which could be accomplished via the HVAC system) and be more broadly to reach the PLCs.

Potential Attack Paths

Subsystems

Management

Subsystem 2...n

Vulnerable devices include: HAVC, PLCs, Access Control, IP cameras, Protocol Gateways

22,902 devices

Total devices publicly reachable*

9,103 devices

Devices publicly reachable and vulnerable in our research

39.3%*

Conclusion

Building automation systems (BAS) may be as critical as industrial control systems (ICS) in terms of safety and security, yet receive much less attention from the security community.

Enhancing BAS cybersecurity programs with detect, monitor, and act capabilities organizations a thorough understanding of the environment and the control systems, creating robust and effective security architecture, identify attack vectors, and baseline models.

Download the full research report to learn more about the current state of smart building cybersecurity.